The 12th International Workshop on SEquences and Their Applications (SETA)

July 01-05, 2024

Colchester, United Kingdom

PRE-PROCEEDINGS

University of Essex

UNIVERSITAS BERGENSIS

UNIVERSITY OF BERGEN

Preface

This volume contains the pre-proceedings of the 12th international conference on SEquences and Their Applications (SETA) which takes place in Colchester, United Kingdom, July 01-05, 2024. The conference SETA-2024 is co-organized by the University of Essex, Colchester, United Kingdom and University of Bergen, Bergen, Norway.

SEquences and Their Applications is an internationally leading conference, aiming to foster fruitful interactions among sequences, signals, and waveforms designers, mathematicians, coding theorists, cryptographic researchers, and communications practitioners from all over the world. This esteemed conference has been hosted in a variety of international locales: SETA-1998 (Singapore), SETA-2001 (Bergen Norway), SETA-2004 (Seoul, South Korea), SETA-2006 (Beijing China), SETA-2008 (Lexington USA), SETA-2010 (Paris France), SETA-2012 (Waterloo Canada), SETA-2014 (Melbourne, Australia), SETA-2016 (Chengdu, China), SETA-2018 (HongKong China), SETA-2020 online (Bergen Norway).

We are very pleased to have five keynote talks by Pingzhi Fan (IEEE Fellow, IET/CIE/CIC Fellow, Chair Professor) from the Southwest Jiaotong University, China, Sihem Mesnager (Professor of Mathematics) from the University of Paris VIII, University Sorbonne Paris Nord, and CNRS, France, Christos Masouros (IEEE Fellow) from the University College London, United Kingdom, Steven (Qiang) Wang (Professor of Mathematics) from the Carleton University, Canada, and Nam Yul Yu (IEEE Senior Member) from the Gwangju Institute of Science and Technology (GIST), South Korea; and two invited featured talks by Wai Ho Mow (IEEE Senior Member) from the Hong Kong University of Science and Technology, China and Pantelimon Stănică from the Naval Postgraduate School, United States.

This pre-proceedings embraces the abstracts of the invited talks and extended abstracts that have been reviewed by the program committee and accepted for presentations at the conference. All speakers will be invited to submit a full paper, based on their SETA submission, to a special issue of the Springer journal Cryptography and Communication: Discrete Structures, Boolean Functions and Sequences. These papers will be refereed again to ensure that they meet the high standard of this journal. We hope the conference and resulting discussion will inspire submissions to this special issue.

We would like to thank the invited speakers, all authors, the members of the program committee and organization committee for their great contributions to the conference.

We wish you all a pleasant stay in Colchester and an inspiring conference.

Guang Gong, Tor Helleseth, Daniel Katz, Chunlei Li, and Zilong Liu

General Chairs

- Tor Helleseth, University of Bergen, Norway
- Zilong Liu, University of Essex, United Kingdom

Program Chairs

- Guang Gong, University of Waterloo, Canada
- Daniel J. Katz, California State University, United States
- Chunlei Li, University of Bergen, Norway

Technical Program Committee

- Serdar Boztas, RMIT University, Australia
- Lilya Budaghyan, University of Bergen, Norway
- Claude Carlet, University of Paris 8, France
- Chao-Yu Chen, National Cheng Kung University, Taiwan
- Nian Li, Hubei University, China
- Jonathan Jedwab, Simon Fraser University, Canada
- Nikolay S. Kaleyski, University of Bergen, Norway
- Oleksandr Kholosha, Ukrainian Catholic University, Ukraine
- Tetsuya Kojima, National Institute of Technology, Tokyo College, Japan
- Gohar M. Kyureghyan, University of Rostock, Germany
- Subhamoy Maitra, Indian Statistical Institute, Kolkata, India
- Kalikinkar Mandal, University of New Brunswick, Canada
- Takahiro Matsumoto, Kagoshima University, Japan
- Wai Ho Mow, Hong Kong University of Science and Technology, China
- Ferruh Özbudak, Sabanci University, Turkey
- Alexander Pott, Otto-von-Guericke University Magdeburg, Germany
- Udaya Parampalli, University of Melbourne, Australia
- Constanza Riera, Western Norway University of Applied Sciences, Norway
- Sumanta Sarkar, University of Warwick, United Kingdom
- Hong-Yeop Song, Yonsei University, Korea
- Pante Stanica, Naval Postgraduate School, USA
- Arne Winterhof, Austrian Academy of Sciences, Austria
- Zhengchun Zhou, Southwest Jiaotong University, China

Organization Committee

- Wenqiang Yi, University of Essex, United Kingdom
- Dian Li, University of Bergen, Norway
- Palash Sarkar, University of Bergen, Norway

Table of Contents

SETA2024 - Schedule (July 01-05, 2024)

Monday	Tuesday	Thursday	Friday
08:30-09:50 Registration Coffee & Tea	08:30-09:00 Coffee & Tea	08:30-09:00 Coffee & Tea	08:30-09:00 Coffee & Tea
09:50-10:00 Opening	09:00-10:00 Keynote Talk 2 **Pingzhi Fan**	09:00-10:00 Keynote Talk 4 **Christos Masouros**	09:00-10:00 Keynote Talk 5 **Nam Yul Yu**
10:00-11:00 Keynote Talk 1 **Sihem Mesnager**	10:00-10:30 Break	10:00-10:30 Break	10:00-10:30 Break
11:00-11:20 Break	10:30-12:10 **Session 4** 4 papers	10:30-12:10 **Featured Talk** 10:30-11:20 Pantelimon Stănică 11:20-12:10 Wai-Ho Mow	10:30-12:10 **Session 7** 4 papers
11:20-12:10 **Session 1** 2 papers			Closing
12:10-14:00 **Lunch**			
14:00-15:15 **Session 2** 3 Papers	14:00-15:00 Keynote Talk 3 **Steven (Qiang) Wang**	14:00-15:00 Panel Discussion Future Researches on Sequences	Departure
15:15-15:30 Break	15:00-15:30 Break	15:00-15:30 Break	
15:30-17:10 **Session 3** 4 papers	15:30-16:45 **Session 5** 3 papers	15:30-16:45 **Session 6** 3 papers	
		18:30 Banquet at Wivenhoe House	

Session Topics	
Session 1: Autocorrelation of Sequences	**Session 5**: Permutations over Finite Fields
Session 2: DeBruijn Sequences and Linear Complexity	**Session 6**: Randomness of Sequences
Session 3: Crypt. Functions and Algebraic Codes	**Session 7**: Low-Correlation Sequences
Session 4: Complementary Seq. and Arrays	

- Brief introductions of the invited speakers can be found at this link
- The arrangement on Wednesday can be found at this link

SETA2024 Program (Monday)

08:30-9:50	**Registration Break** **Coffee & Tea**		
09:50-10:00	**Conference Opening** Maria Fasli Dean of the Faculty of Science and Health, the University of Essex		
10:00-11:00	Sihem Mesnager Keynote Talk *Chair: Daniel Katz*	On algebraic problems on finite fields and their importance more than ever in the study of S-boxes in block ciphers	abstract
11:00-11:20	**Break**		
	Session 1: Autocorrelation of Sequences (*Chair: Avik Ranjan Adhikary*)		
11:20-11:45	Gangsan Kim	Balanced binary sequences with favorable autocorrelation from cyclic relative difference sets	paper
11:45-12:10	Daniel Katz	Moments of autocorrelation demerit factors	paper
12:10-14:00	**Lunch**		
	Session 2: De Bruijn Sequences and Linear Complexity (*Chair: Chunlei Li*)		
14:00-14:25	Guang Gong	Filtering modified de Bruijn sequences with designated linear complexity	paper
14:25-14:50	Martianus Frederic Ezerman	New successor rules to efficiently produce exponentially many binary de Bruijn sequences	paper
14:50-15:15	Domingo Gomez	On the linear complexity of Shrunken sequences	paper
15:15-15:30	**Coffee & Tea Break**		
	Session 3: Cryptographic Functions and Algebraic Codes (*Chair: Constanza Riera*)		
15:30-15:55	Yongbo Xia	A direct method for calculating the differential spectrum of an APN power mapping	paper
15:55-16:20	Ana Salagean	Bounds for the average degree-k monomial density of Boolean functions	paper
16:20-16:45	Guangkui Xu	Optimal few-weight codes from projective spaces	paper
16:45-17:10	Susanta Samanta	On the Counting of Involutory MDS Matrices	paper

SETA2024 Program (Tuesday)

08:30-09:00	**Coffee & Tea**		
09:00-10:00	Pingzhi Fan Keynote Talk *Chair: Tor Helleseth*	Recent advances in signal design for integrated sensing & communications	abstract
10:00-10:30	**Coffee & Tea Break**		
Session 4: Complementary Sequences and Arrays (*Chair: Qi Zeng*)			
10:30-10:55	Kai Liu	Construction of cross Z-complementary sequence set with large CZC ratio	paper
10:55-11:20	Tao Yu	A construction of optimal Z-complementary code sets on partially m-shift orthogonal complementary codes	paper
11:20-11:45	Dian Li	On average zero-correlation zone of Golay complementary pairs	paper
11:45-12:10	Kai Liu	New constructions of two-dimensional binary Z-complementary array pairs	paper
12:10-14:00	**Lunch**		
14:00-15:00	Steven (Qiang) Wang Keynote Talk *Chair: Ana Salagean*	A survey of compositional inverses of permutation polynomials over finite fields	paper
15:00-15:30	**Coffee & Tea Break**		
Session 5: Permutations over Finite Fields (*Chair: Domingo Gomez*)			
15:30-15:55	Mohit Pal	A proof of a conjecture on trivariate permutations	paper
15:55-16:20	Lucas Krompholz	On the bijectivity of the map χ	paper
16:20-16:45	Steven Wang	An effective approach to enumerate universal cycles for k-permutations	paper
End of Program			

SETA2024 Program (Thursday)

08:30-09:00	**Coffee & Tea**		
09:00-10:00	Christos Masouros Keynote Talk *Chair: Zilong Liu*	Sustainable and multifunctional wireless networks	abstract
10:00-10:30	**Coffee & Tea Break**		
	Featured Talk (*Chair: Chunlei Li*)		
10:30-11:20	Pantelimon Stănică	Threshold implementations and permutations' decompositions: a number theoretical approach	abstract
11:20-12:10	Wai-Ho Mow	Bus coding for low-power on-chip interconnects	abstract
12:10-14:00	**Lunch**		
14:00-15:00	**Panel Discussion**		
15:00-15:30	**Coffee & Tea Break**		
	Session 6: Randomness of Sequences (*Chair: Chaoyun Li)*		
15:30-15:55	Melis Aslan	Observations on NIST SP 800-90B entropy estimators	paper
15:55-16:20	Michael Vielhaber	Two pattern properties of binary sequences invariant under the continued fraction operator K (the Berlekamp-Massey Algorithm)	paper
16:20-16:45	Muhiddin Uğuz	RW-9: A family of random walk tests	paper
End of Program			

SETA2024 Program (Friday)

08:30-09:00	**Coffee & Tea**		
09:00-10:00	Nam Yul Yu Keynote Talk *Chair: Guang Gong*	Pseudorandom sequences for grant-free access in massive machine-type communications	abstract
10:00-10:30	**Coffee & Tea Break**		
Session 7: Low-Correlation Sequences (*Chair: Yongbo Xia*)			
10:30-10:55	Rajen Kumar	Multiple spectrally null constrained complete complementary codes of various lengths over small alphabet	paper
10:55-11:20	Yubo Li	Construction of multiple quasi-complementary sequence sets with low inter-set cross-correlation	paper
11:20-11:45	Qi Zeng	Hierarchical frequency hopping technique for heterogeneous multi-tier networks	paper
11:45-12:10	Avik Ranjan Adhikary	Circular quasi-Florentine rectangles and its application in designing optimal polyphase sequence sets	paper
12:10-12:15	**Conference Closing** Tor Helleseth		
12:15-14:00	**Lunch**		
End of SETA-2024			

Keynote Talk: On algebraic problems on finite fields and their importance more than ever in the study of S-boxes in block ciphers

Sihem Mesnager

LAGA (Laboratory of Analysis, Geometry, and Applications), University of Paris VIII, University Sorbonne Paris Nord, and CNRS, Paris, France

Abstract. Throughout this talk, we will place ourselves in finite fields whose theory originates in the work of the French mathematician Evariste Galois. After briefly presenting some main cryptographic problems in symmetric cryptography in the context of block ciphers and highlighting our main motivations, we focus on some underlying fundamental mathematical problems and discuss some algebraic approaches and ingredients used at the core of the methodologies. We shall also present recent achievements in algebraic equations and address open questions, particularly those aimed at implementing methods to solve equations over finite fields and making them available to theorists, notably cryptographers and sequences designers.

Balanced Binary Sequences with Favourable Autocorrelation from Cyclic Relative Difference Sets

Gangsan Kim Hong-Yeop Song

Department of Electrical and Electronic Engineering
Yonsei University
Seoul, South Korea

{gs.kim,hysong}@yonsei.ac.kr

Abstract

In this paper, we propose a balanced binary sequence of even period $2u$ for some even values of u with 5-level autocorrelation from a cyclic relative difference set with parameters $(u, 2, u-1, \frac{u}{2}-1)$. We further identify its half-period as those having an optimal odd autocorrelation. Various relations of these with some previous constructions are discussed.

1 Introduction

Binary sequences with good autocorrelation properties are advantageous for synchronization in various communication systems [6, 7]. There have been a lot of results on the constructions of sequences (binary, almost binary, ternary, non-binary, polyphase, almost polyphase, etc) for the last half century or more for improved performance of various communications systems. Most of the sequences in this paper are over the binary alphabet $\mathbb{F}_2 = \{0, 1\}$ but the correlation is computed over $\mathbb{C}$ with the correspondence

$$x \in \mathbb{F}_2 = \{0, 1\} \leftrightarrow (-1)^x \in \mathbb{C}.$$

When we are given a binary sequence $\mathbf{s} = \{s(i) \in \mathbb{F}_2 | i = 0, 1, ..., L-1\}$ of length L, we may consider its (usual) periodic expansion for computing its periodic autocorrelation. In that sense, we will use the term 'length' and 'period' of a binary sequence interchangeably. Then, the periodic autocorrelation of $\mathbf{s}$ at shift τ, denoted by $C_{\mathbf{s}}(\tau)$, is given by

$$C_{\mathbf{s}}(\tau) = \sum_{i=0}^{L-1} (-1)^{s(i)+s(i+\tau)}, \tag{1}$$

where $i + \tau$ is computed mod L. There is an alternative way of expanding the sequence $\mathbf{s}$ of length L periodically. Let $\mathbf{s}'$ be a complement of $\mathbf{s}$ defined by

$$s'(i) = s(i) + 1, \quad i = 0, 1, ..., L-1.$$

Then, the alternative periodic expansion, called odd-periodic expansion, is to repeat $\mathbf{s}$ in concatenation with $\mathbf{s}'$ of total length $2L$. The autocorrelation of $\mathbf{s}$ with this type of expansion is called the odd autocorrelation of $\mathbf{s}$. The odd autocorrelation at shift τ with $0 \le \tau < L$, denoted by $C_{\mathbf{s}}^{odd}(\tau)$, is given by

$$C_{\mathbf{s}}^{odd}(\tau) = \sum_{i=0}^{L-\tau-1} (-1)^{s(i)+s(i+\tau)} + \sum_{i=L-\tau}^{L-1} (-1)^{s(i)+s(i+\tau)+1}, \tag{2}$$

where $i+\tau$ is computed mod L. In fact, $C_{\mathbf{s}}(\tau)$ can be said to be an even autocorrelation.

The binary sequence $\mathbf{s}$ of even period L is said to have optimal autocorrelation [7, 9] if

$$C_{\mathbf{s}}(\tau) = \begin{cases} 0 \text{ or } -4 & \text{if } L \equiv 0 \ (mod\ 4) \\ 2 \text{ or } -2 & \text{if } L \equiv 2 \ (mod\ 4). \end{cases}$$

for any $\tau \neq 0$. A lot of binary sequences of even period L above with (non-perfect) optimal autocorrelation have been constructed [4, 5, 15, 19, 21, 26], which would be best possible in terms of its periodic autocorrelation, since the perfect binary sequence is known only for $L = 4$ [7].

Instead of suppressing all the out-of-phase autocorrelation magnitudes, one started to consider having all-zero out-of-phase autocorrelations except for one non-zero value at some $\tau \neq 0$. It is called almost perfect sequences [24] and investigated immediately by many others [10,16–18] and further generalized into some non-binary zero-correlation zone sequences [20,22,23]. We would like to mention that [17,18] established some fundamental relation between cyclic relative difference sets and almost perfect binary sequences, which is very much similar to the relation between cyclic difference sets and binary sequences with two-level autocorrelation. For example, binary NTU sequences [16] are closely related with binary sequences from a cyclic relative difference set [10], which will be mentioned at the very last Remark of this paper. In fact, the main result of this paper is a full generalization of [10].

In search of sequences with better autocorrelation property, on the other hand, almost binary sequences or ternary sequences have been studied a lot [12, 13, 17]. Here, an almost binary sequence is a ternary sequence over $\{0, +1, -1\}$ but the term 0 occurs only once or a few times. Such sequences with 'perfect' autocorrelation have been found, for example, in [13].

Some reviews on the binary and almost binary sequences with good odd autocorrelation follows now. In [14], especially in Section IV. A. 4 there, a binary sequence of even period is said to have an odd optimal autocorrelation if the magnitude of out of phase odd autocorrelation is no larger than 2. The binary sequences with low or optimal odd periodic autocorrelation have also been proposed a lot [12–14, 16, 25].

In this paper, we propose (Theorem 3) a balanced binary sequence of even length $2u$ for some integer u with 5-level autocorrelation from a cyclic relative difference set. The out-of-phase autocorrelation magnitudes are all zero except for three indices at which the value is either $2u$ ($\tau = u$, once) or 4 (at some $\tau \neq 0, u$ twice). We observe the half period of this sequence and found that it has optimal odd autocorrelation (Theorem 4). Furthermore, we explain some of the known constructions for sequences with good (even

or odd) autocorrelation are closely related with two main results of this paper using an relative difference set (RDS).

This paper is organized as follows, Section 2 introduces some preliminaries. Section 3 discusses two main results of this paper. Section 4 explains the relation between our constructions and other known constructions, especially in [12, 16]. Section 5 concludes this paper with a conjecture on the binary sequences of even period with optimal odd autocorrelation.

2 Preliminaries

2.1 Notation

We will fix the following notation throughout the paper.

- $\mathbb{Z}$ is the set of integers and $\mathbb{Z}_L$ is the integers mod L.
- $\mathbb{C}$ is the set of complex numbers and $\mathbb{F}_q$ is the finite field of size q.
- Given a binary sequence $\mathbf{s} = \{s(i) \in \mathbb{F}_2 | i = 0, 1, ..., L-1\}$ of length L, the periodic autocorrelation of $\mathbf{s}$ at shift τ, denoted by $C_{\mathbf{s}}(\tau)$, is given by (1) and the odd autocorrelation $C_{\mathbf{s}}^{odd}(\tau)$ is given by (2), both in the beginning of Introduction.
- For a subset X of $\mathbb{Z}_L$ and an element $\tau \in \mathbb{Z}_L$, we define

$$\Delta_X(\tau) \triangleq |(\tau + X) \cap X|,$$

where $\tau + X = \{\tau + x | x \in X\}$. Note that

$$\Delta_X(\tau) = \Delta_X(-\tau)$$

for any subset X and any τ.

2.2 Relative Difference Set

Definition 1 (Relative Difference Sets [2, 8, 17])**.** Let u,v,k, λ be positive integers. A (u, v, k, λ) relative difference set (RDS) D in the (additive) cyclic group $\mathbb{Z}_{uv}$ relative to its subgroup $(u) = u\mathbb{Z}_{uv}$ is a k-subset $\{d_1, d_2, \ldots, d_k\} \subset \mathbb{Z}_{uv}$, satisfying the following condition:

$$\Delta_D(d) = \begin{cases} \lambda, & d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv} \\ k, & d = 0 \\ 0, & \text{otherwise}, \end{cases} \tag{3}$$

for any $d \in \mathbb{Z}_{uv}$. Throughout this paper, we call this a (u, v, k, λ) RDS without refering to the cyclic group $\mathbb{Z}_{uv}$ and its subgroup $(u) = u\mathbb{Z}_{uv}$.

It is well-known that a (u, k, λ)-cyclic difference set (CDS) in $\mathbb{Z}_u$ is a $(u, v = 1, k, \lambda)$-RDS in $\mathbb{Z}_u$ (relative to its trivial subgroup $\{0\}$). We are mostly interested in the case where

$v = 2$ [2] and $k = u - 1$ so that the parameters become $(u, v = 2, k = u - 1, \lambda = \frac{u}{2} - 1)$, since the existence of a cyclic (u, v, k, λ)-RDS implies the relation

$$k(k-1) = \lambda v(u-1).$$

This set of parameters further implies that u itself must be even. The following provides an equal-size partition of $\mathbb{Z}_{2u}$ so that a binary sequence can be constructed from such RDS D.

Proposition 2. *Let D be a $(u, 2, u-1, \frac{u}{2}-1)$-RDS. Then, $\mathbb{Z}_{2u}$ can be decomposed into the following disjoint union:*

$$\mathbb{Z}_{2u} = D \cup (u + D) \cup \{z\} \cup \{z + u\},$$

for some z.

Proof. By (3), $\Delta_D(u) = 0$. Therefore,

$$D \cap (u + D) = \emptyset.$$

Therefore,

$$|\mathbb{Z}_{2u} \backslash (D \cup (u + D))| = 2u - 2k = 2.$$

Therefore, $\mathbb{Z}_{2u} \backslash (D \cup (u + D))$ is non-empty. Let z be a member. If $z + u \in D$, then $z = z + u + u \in u + D$. If $z + u \in u + D$, then $z \in D$. Therefore, we also have $z + u \in \mathbb{Z}_{2u} \backslash (D \cup (u + D))$. □

3 Binary Sequences with Favourable Autocorrelation from RDS

In this section, we propose a balanced binary sequence $\mathbf{s} = \{s(i) | i \in \mathbb{Z}_{2u}\}$ of length $2u$ with 5-level autocorrelation from a $(u, 2, u-1, \frac{u}{2}-1)$-RDS and discuss its two variations with (somewhat) better correlation property: the first is its half period portion of length u which is still balanced with 4-level optimal odd autocorrelation; the second is its one-bit-changed version so that the result is almost balanced but with 3-level autocorrelation so that it is almost perfect.

Theorem 3 (Main Construction)**.** *Let D be a $(u, v = 2, k = u - 1, \lambda = \frac{u}{2} - 1)$-RDS. Let $z \in \mathbb{Z}_{2u}$ so that $\mathbb{Z}_{2u}$ is partitioned as in Proposition 2:*

$$\mathbb{Z}_{2u} = D \cup (u + D) \cup \{z\} \cup \{z + u\}. \tag{4}$$

Define a binary sequence $\mathbf{s} = \{s(i) \,|\, i = 0, 1, ..., 2u - 1\}$ as follows:

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u + D) \cup \{u + z\}. \end{cases} \tag{5}$$

Then, the periodic (even) autocorrelation of $\mathbf{s}$ becomes:

$$C_{\mathbf{s}}(\tau) = \begin{cases} 2u, & \tau = 0 \\ -2u, & \tau = u \\ 4, & \tau, -\tau \in -z + u + D \\ -4, & \tau, -\tau \in -z + D \\ 0, & \textit{otherwise.} \end{cases} \tag{6}$$

Proof. From the relation (4) and definition of the sequence $\mathbf{s}$ in (5), the autocorrelation of $\mathbf{s}$ at shift τ is calculated as follows:

$$\begin{aligned} C_{\mathbf{s}}(\tau) &= \sum_{i\in\mathbb{Z}_{2u}} (-1)^{s(i)+s(i+\tau)} \\ &= \sum_{i\in D} (-1)^{s(i)+s(i+\tau)} + \sum_{i\in u+D} (-1)^{s(i)+s(i+\tau)} + (-1)^{s(z)+s(z+\tau)} + (-1)^{s(z+u)+s(z+u+\tau)}. \end{aligned} \tag{7}$$

The first sum in (7) can be split into the following three cases: (a) $i \in D$ and $i+\tau \in D$ so that $s(i)+s(i+\tau)=0$, (b) $i \in D$ and $i+\tau \in u+D$ so that $s(i)+s(i+\tau)=1$ and (c) $i \in D$ and $i+\tau \in \{z, u+z\}$ so that $s(i)+s(i+\tau)=s(i+\tau)$ which is 1 if $i+\tau=z$ and 0 if $i+\tau=u+z$. Then the case (a) becomes

$$\sum_{\substack{i\,\in\,D\\ i+\tau\,\in\,D}} (+1) = |D \cap (-\tau + D)| = |\tau + D \cap D| = \Delta_D(\tau).$$

Similarly, the case (b) becomes

$$\sum_{\substack{i\,\in\,D\\ i+\tau\,\in\,u+D}} (-1) = -|D \cap (-\tau + u + D)| = -\Delta_D(u-\tau).$$

Similarly, the second sum can be split into the following three cases: (a) $i \in u+D$ and $i+\tau \in D$ so that $s(i)+s(i+\tau)=1$, (b) $i \in u+D$ and $i+\tau \in u+D$ $s(i)+s(i+\tau)=0$, and (b) $i \in u+D$ and $i+\tau \in \{z, u+z\}$. Then, similar to the first two cases of the first sum, the cases (a) and (b) become:

$$\sum_{\substack{i\,\in\,u+D\\ i+\tau\,\in\,D}} (-1) = -|(u+D) \cap (-\tau + D)| = -\Delta_D(u+\tau)$$

and

$$\sum_{\substack{i\,\in\,u+D\\ i+\tau\,\in\,u+D}} (+1) = |u + D \cap (u - \tau + D)| = \Delta_{u+D}(\tau) = \Delta_D(\tau).$$

Therefore, the autocorrelation of $\mathbf{s}$ at shift τ becomes:

$$\begin{aligned} C_{\mathbf{s}}(\tau) = 2\Delta_D(\tau) &- \Delta_D(u+\tau) - \Delta_D(u-\tau) \\ &+ \sum_{\substack{i\,\in\,D\,\cup\,(u+D)\\ i+\tau\,=\,z,\,z+u}} (-1)^{s(i)+s(i+\tau)} + (-1)^{s(z+\tau)} + (-1)^{s(z+u+\tau)+1} \end{aligned} \tag{8}$$

For the cases of either $\tau = 0$ or $\tau = u$, recall that

$$(D \cup (u+D)) \cap \{z, z+u\} = \emptyset.$$

Therefore, the middle sum in (8) vanishes in this case. When $\tau = 0$, we have

$$C_{\mathbf{s}}(0) = 2\Delta_D(0) + 2(-1)^0 = 2k + 2 = 2u,$$

which is the length of $\mathbf{s}$. Similarly, when $\tau = u$,

$$C_{\mathbf{s}}(u) = -2\Delta_D(0) + 2(-1)^1 = -2k - 2 = -2u.$$

Now, consider the case when $\tau \neq 0, u$. Then, the first line of $C_{\mathbf{s}}(u)$ in (8) becomes

$$2\Delta_D(\tau) - \Delta_D(u+\tau) - \Delta_D(u-\tau) = 0,$$

since $\Delta_D(\tau) = \Delta_D(u \pm \tau) = \lambda = \frac{u}{2} - 1$. Now, the middle sum in (8) becomes the sum of only two terms

$$\begin{aligned}\sum_{\substack{i \in D \cup (u+D) \\ i+\tau = z, z+u}} (-1)^{s(i)+s(i+\tau)} &= (-1)^{s(z-\tau)+s(z)} + (-1)^{s(z+u-\tau)+s(z+u)} \\ &= (-1)^{s(z-\tau)} + (-1)^{s(z+u-\tau)+1},\end{aligned}$$

since, in this case,

$$\{z-\tau, z+u-\tau\} \subset (D \cup (u+D)),$$

and hence, there are only two terms corresponding to $i = z - \tau$ and $i = z + u - \tau$. Therefore, (8) finally becomes

$$C_{\mathbf{s}}(\tau) = (-1)^{s(z-\tau)} + (-1)^{s(z+u-\tau)+1} + (-1)^{s(z+\tau)} + (-1)^{s(z+u+\tau)+1}.$$

Therefore, finally, when $\tau \neq 0, u$,

$$C_{\mathbf{s}}(\tau) = \begin{cases} -4, & z-\tau, z+\tau \in D \\ 4, & z-\tau, z+\tau \in u+D \\ 0, & \text{otherwise.} \end{cases}$$

This proves the theorem. □

The binary sequence $\mathbf{s} = \{s(i) \mid i = 0, 1, ..., 2u-1\}$ constructed from above theorem is balanced since

$$|D \cup \{z\}| = |(u+D) \cup \{u+z\}|.$$

Note that $(u+D) \cup \{u+z\}$ can be represented also as $u + (D \cup \{z\})$. This explains its some special periodic property. When it is (cyclically) shifted by half the period, then the result is a complement of the original sequence. Therefore, its half period portion of length u is expanded odd-periodically, the result is the same as the (even) periodic expansion of the original sequence $\mathbf{s}$ of length $2u$. The proof of the following is straightforward from Theorem 3 and the discussions so far.

Theorem 4. *Let* $\mathbf{s}$ *be the binary sequence of period* $2u$ *constructed from Theorem 3 with some* $(u, 2, u-1, \frac{u}{2}-1)$*-RDS and an integer* z *satisfying the relation* (4)*. Define the binary sequence* $\mathbf{t}$ *of period* u *as follows, for* $i = 0, 1, ..., u-1$*,*

$$t(i) = s(i).$$

Then the odd autocorrelation of $\mathbf{t}$ *at shift* τ *with* $0 \leq \tau < u$ *becomes:*

$$C_{\mathbf{t}}^{odd}(\tau) = \begin{cases} u, & \tau = 0 \\ 2, & \tau, -\tau \in -z + u + D \\ -2, & \tau, -\tau \in -z + D \\ 0, & otherwise. \end{cases}$$

Remark 5. The binary sequence $\mathbf{t}$ constructed from Theorem 4 is optimal in the sense of minimizing the maximum magnitude of out of phase odd autocorrelation described in Section IV. A. 4 of [14], as mentioned in Introduction.

4 The relation between our construction and other known construction

In this section, we discuss the relation between our construction in Theorems 3 and 4 from an RDS of parameters $(u, 2, u-1, \frac{u}{2}-1)$ and other previous constructions, for example, those in [12, 16] which were given without mentioning any RDS structure. In fact, an example of an RDS can be constructed by using some finite field structures [8], and the construction of a binary sequence can be stated without mentioning any RDS structures and by simply using a subset D of the integers mod uv. The sequences in [12, 14, 16] are in fact constructed in this way without mentioning any RDS structures.

First, we will give a brief explanation of those from [12] and [14]. We use the following additional notations in this section.

- q is an odd prime power.
- $\mathbb{F}_{q^2}$ is the finite field with q^2 elements.
- α is a primitive element of $\mathbb{F}_{q^2}$.
- $\beta \triangleq \alpha^{q+1}$ is a primitive element of $\mathbb{F}_q$.
- For any non-zero $b \in \mathbb{F}_q$, we use, for $0 \leq j < q-1$,

$$\log_\beta(b) = j \quad \text{if and only if} \quad b = \beta^j.$$

- $\mathrm{Tr}(a) \in \mathbb{F}_q$ is the trace of $a \in \mathbb{F}_{q^2}$ defined by

$$\mathrm{Tr}(a) = a + a^q.$$

A construction of some binary sequences with optimal odd autocorrelation is given in [14], where the binary sequence is obtained from a ternary $\{0, \pm 1\}$ odd perfect sequence by replacing 0 with one of $\{+1, -1\}$. Here, an odd perfect sequence is defined as those having all the out-of-phase odd autocorrelation values equal to zero. The resulting binary sequence is not odd perfect, but has optimal odd autocorrelation as those from Theorem 4. In fact, it is also given in [12] as follows:

Definition 6 (Modified Krengel Sequences [12, 14])**.** The binary sequence $\mathbf{x} = \{x(i) \,|\, i = 0, 1, ..., q\}$ of length $(q+1)$ is defined as

$$x(i) = \begin{cases} 1, & \log_\beta(\mathrm{Tr}(\alpha^i)) \text{ is odd} \\ 0, & \mathrm{Tr}(\alpha^i) = 0 \text{ or else } \log_\beta(\mathrm{Tr}(\alpha^i)) \text{ is even.} \end{cases}$$

We just note the values of i above so that $x(i) = 0$ except for the case $\mathrm{Tr}(\alpha^i) = 0$. It is not difficult to observe that the set of these values of i forms an RDS of parameters $(q+1, 2, q, \frac{q-1}{2})$ [8] in the structure of $\mathbb{F}_q$ and its extension $\mathbb{F}_{q^2}$. That is, claim that

$$D \triangleq \{i \in \mathbb{Z}_{2(q+1)} \,|\, \log_\beta(\mathrm{Tr}(\alpha^i)) \text{ is even}\}. \tag{9}$$

is a $(q+1, 2, q, \frac{q-1}{2})$-RDS in $\mathbb{Z}_{2(q+1)}$ relative to its subgroup $(q+1)\mathbb{Z}_{2(q+1)}$. For the proof, see Cor. 5.1.1 in [8] or Sec. 2.2 in [17].

Remark 7. The modified Krengel sequence $\mathbf{x}$ of length $q+1$ is the same as those constructed from Theorem 4 with the RDS D in (9).

Nogami, Tada and Uehara [16] proposed some binary sequences as in the following definition for some specific parameters.

Definition 8 (Binary NTU Sequences [16])**.** The binary sequence $\mathbf{y} = \{y(i) \,|\, i = 0, 1, ..., 2(q+1)-1\}$ of length $2(q+1)$ is defined in [16] as

$$y(i) = \begin{cases} 1, & \log_\beta(\mathrm{Tr}(\alpha^i)) \text{ is odd} \\ 0, & \mathrm{Tr}(\alpha^i) = 0 \text{ or else } \log_\beta(\mathrm{Tr}(\alpha^i)) \text{ is even.} \end{cases}$$

We call this sequence the binary NTU sequence.

It is interesting that the only difference between this sequence and the modified Krengel sequence is the range of i which defines the sequence. It can be also seen that only one term is changed from the construction in Theorem 3 at index $u+z$ so that the result is no longer balanced (we may call this almost balanced) but with better autocorrelation property which is only 3-level. In fact, this binary sequence has been defined to be the almost perfect sequences [18,24] and Pott and Bradley proved [18] that they are equivalent to some $(u, 2, u-1, \lambda)$-RDS in $\mathbb{Z}_{2u}$ relative to its subgroup $u\mathbb{Z}_{2u}$.

Remark 9. These are all equivalent to an almost perfect binary sequence of period $2(q+1)$:

1. A cyclic relative difference set with parameter $(q+1, 2, q, (q-1)/2)$ in $\mathbb{Z}_{2u}$ relative to its subgroup $u\mathbb{Z}_{2u}$.
2. Binary NTU sequence of length $2(q+1)$.
3. Modified binary sequence of length $2u$ obtained by chaning one term at index $z+u$ from those constructed in Theorem 3 with $u = q+1$.

5 Concluding Remarks

We propose a construction of a balanced binary sequence of even period with 5-level autocorrelation in Theorem 3 from an RDS of parameters $(u, 2, u-1, \frac{u}{2}-1)$, which is slightly different from the almost perfect binary sequences from this RDS as mentioned in Remark 9. We further identify its half-period in Theorem 4 as those having optimal odd autocorrelation. All of the sequences of our constructions are derived from any $(u, v = 2, k = u-1, \lambda = \frac{u}{2}-1)$-RDS when $u = q+1$ for an odd prime power q [8, 17].

We find out that the binary sequence of period with optimal odd autocorrelation derived from [12, 14] can be constructed from Theorem 4 with the $(u = q+1, 2, q, \frac{q-1}{2})$-RDS constructed from [8, 17].

All the known parameters of a $(u, v = 2, k = u-1, \lambda)$-RDS are $(u = q+1, v = 2, k = q, \lambda = \frac{q-1}{2})$ for some odd prime power q. There exist several non-equivalence classes of $(u = q+1, v = 2, k = q, \lambda = \frac{q-1}{2})$-RDS [1, 3, 11, 17]. Indeed, our construction in Theorem 4 give some binary sequences of period $q+1$ with optimal odd autocorrelation. We conjecture that it is the only way of getting a binary sequence of period $q+1$ with optimal odd autocorrelation for some odd prime power q.

Acknowledgements

This work was supported by the National Research Foundation of Korea (NRF) Grant by the Korea Government through Ministry of Sciences and ICT (MSIT) under Grant RS-2023-002090000.

References

[1] K. T. Arasu, J. F. Dillon, K. H. Leung and S. L. Ma. Cyclic relative difference sets with classical parameters. *J. Comb. Theory, Ser. A* 94(1): 118–126, 2001.

[2] K. T. Arasu, D. Jungnickel, S. L. Ma, and A. Pott. Relative difference sets with $n = 2$. *Discret. Math.* 147: 1–17, 1995.

[3] D. B. Chandler and Q. Xiang. Cyclic relative difference sets and their p-ranks. *Designs Codes Cryptogr.* 30(3): 325–343, 2003.

[4] C. Ding, T. Helleseth, and H. Martinsen. New families of binary sequences with optimal three-valued autocorrelation. *IEEE Trans. Inf. Theory* 47(1): 428–433, 2001.

[5] C. Ding, T. Helleseth, and K. Y. Lam. Several classes of binary sequences with three-level autocorrelation. *IEEE Trans. Inf. Theory* 45(7): 2601–2606, 2001.

[6] S. W. Golomb. *Shift register sequences*, CA, Holden-Day, San Francisco, 1967; 2nd edition, Aegean Park Press, Laguna Hills, CA, 1982; 3rd edition, World Scientific, Hackensack, NJ, 2017.

[7] S. W. Golomb and G. Gong. *Signal design for good correlation: for wireless communications, cryptography, and radar*, New York, NY, USA: Cambridge University Press, 2005.

[8] J. Elliott and A. Butson. Relative difference sets. *Ill. J. Math.* 10(3): 517–531, 1966.

[9] T. Helleseth and K. Yang. On binary sequences of period $n = p^m - 1$ with optimal autocorrelation. *in Proc. 2001 Sequences and their Applications(SETA)*: 209–217, 2002.

[10] G. Kim and H.-Y. Song. Some properties of NTU sequences. *IEICE Proceedings Series* 55(We-AM-Poster. 7), 2018.

[11] S. H. Kim, J. S. No, H. Chung and T. Helleseth. New cyclic relative difference sets constructed from d-homogeneous functions with difference-balanced property. *IEEE Trans. Inf. Theory* 51(3): 1155–1163, 2005.

[12] E. I. Krengel. Almost-perfect and odd-perfect ternary sequences. *in Proc. 2024 Sequences and Their Applications(SETA)*: 197–207, 2004.

[13] H. D. Luke and H. D. Schotten. Odd-perfect, almost binary correlation sequences. *IEEE trans. Aerosp. Electron. Systems* 31(1): 495–498, 1995.

[14] H. D. Luke, H. D. Schotten and H. Hadinejad-Mahram. Binary and quadriphase sequences with optimal autocorrelation properties: A survey. *IEEE Trans. Inf. Theory* 49(12): 3271–3282, 2003.

[15] J.-S. No, H. Chung, H.-Y. Song, K. Yang, J. D. Lee, and T. Helleseth. New construction for binary sequences of period $p^m - 1$ with optimal autocorrelation using $(z+1)^d + az^d + b$. *IEEE Trans. Inf. Theory* 47(4): 1638–1644, 2001.

[16] Y. Nogami, K. Tada, and S. Uehara. A geometric sequence binarized with Legendre symbol over odd characteristic field and its properties. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* E.97-A(12): 2336–2342, 2014.

[17] A. Pott. *Finite geometry and character theory*, Springer, 1995.

[18] A. Pott and P. Bradley. Existence and nonexistence of almost-perfect autocorrelation sequences. *IEEE Trans. Inf. Theory* 41(1): 301–304, 1995.

[19] V. M. Sidelnikov. Some k-valued pseudo-random sequences and nearly equidistant codes. *Probl. Inf. Transm.* 5: 12–16, 1969.

[20] X. H. Tang, P. Z. Fan, and S. Matsufuji. Lower bounds on correlation of spreading sequence set with low or zero correlation zone. *Electron. Lett.* 36: 551–552, 2000.

[21] H. Tang and G. Gong. New constructions of binary sequences with optimal autocorrelation value / magnitude. *IEEE Trans. Inf. Theory* 56(3): 1278–1286, 2010.

[22] A. Z. Tirkel, E. Krengel, and T. Hall. Sequences with large ZCZ. *in Proc. The 8-th IEEE International Symposium on Spread Spectrum Techniques and Applications(ISSSTA)*: 270–274, 2004.

[23] H. Torii, M. Nakamura, and N. Suehiro. A new class of zero-correlation zone sequences. *IEEE Trans. Inf. Theory* 50(3): 559–565, 2004.

[24] J. Wolfmann. Almost perfect autocorrelation sequences. *IEEE Trans. Inf. Theory* 38(4): 1412–1418, 1992.

[25] Y. Yang and X. Tang. Generic construction of binary sequences of period $2N$ with optimal odd correlation magnitude based on quaternary sequences of odd period N. *IEEE Trans. Inf. Theory* 64(1): 384–392, 2018.

[26] N. Y. Yu and G. Gong. New binary sequences with optimal autocorrelation magnitude. *IEEE Trans. Inf. Theory* 54(10): 4771–4779, 2008.

Moments of Autocorrelation Demerit Factors of Binary Sequences

Daniel J. Katz* Miriam E. Ramirez*

Department of Mathematics
California State University, Northridge
Northridge, California, United States

daniel.katz@csun.edu

miriam.ramirez@csun.edu

Abstract

Sequences with low aperiodic autocorrelation are used in communications and remote sensing for synchronization and ranging. The autocorrelation demerit factor of a sequence is the sum of the squared magnitudes of its autocorrelation values at every nonzero shift when we normalize the sequence to have unit Euclidean length. The merit factor, introduced by Golay, is the reciprocal of the demerit factor. We consider the uniform probability measure on the 2^ℓ binary sequences of length ℓ and investigate the distribution of the demerit factors of these sequences. Sarwate and Jedwab have respectively calculated the mean and variance of this distribution. We develop new combinatorial techniques to calculate the pth central moment of the demerit factor for binary sequences of length ℓ. These techniques prove that for $p \geq 2$ and $\ell \geq 4$, all the central moments are strictly positive. For any given p, one may use the technique to obtain an exact formula for the pth central moment of the demerit factor as a function of the length ℓ. Jedwab's formula for variance is confirmed by our technique with a short calculation, and we go beyond previous results by also deriving an exact formula for the skewness. A computer-assisted application of our method also obtains exact formulas for the kurtosis, which we report here, as well as the fifth central moment.

1 Introduction

A *sequence* is a doubly infinite list $f = (\ldots, f_{-1}, f_0, f_1, f_2, \ldots)$ of complex numbers in which only finitely many of the terms are nonzero. We adopt this definition because we are thinking of our sequences aperiodically. If ℓ is a nonnegative integer, then a

*This paper is based upon work of both authors supported in part by the National Science Foundation under Grants 1500856 and 1815487, and by work of Daniel J. Katz supported in part by the National Science Foundation under Grant 2206454.

binary sequence of length ℓ is an $f = (\ldots, f_{-1}, f_0, f_1, f_2, \ldots)$ in which $f_j \in \{-1, 1\}$ for $j \in \{0, 1, \ldots, \ell - 1\}$ and $f_j = 0$ otherwise. Binary sequences are used to modulate signals in telecommunications and remote sensing [7, 8, 13]. Some applications, such as ranging, require very accurate timing. For these applications, it is important that the sequence not resemble any time-delayed version of itself.

Our measure of resemblance is aperiodic autocorrelation. If f is a sequence and $s \in \mathbb{Z}$, then the *aperiodic autocorrelation of* f *at shift* s is

$$C_f(s) = \sum_{j \in \mathbb{Z}} f_{j+s}\overline{f_j}.$$

Since $f_k = 0$ for all but finitely many k, this sum is always defined and is nonzero for only finitely many s. Note that $C_f(0)$ is the squared Euclidean norm of f. For applications, we want $|C_f(s)|$ to be small compared to $C_f(0)$ for every nonzero $s \in \mathbb{Z}$; this distinction is what ensures proper timing.

There are two main measures for evaluating how low the autocorrelation of a sequence f is at nonzero shifts. One measure is the *peak sidelobe level*, which is the maximum of $|C_f(s)|$ over all nonzero $s \in \mathbb{Z}$; this can be regarded as an l^∞ measure. Another important measure is the *demerit factor*, which is an l^2 measure of smallness of autocorrelation. The *(autocorrelation) demerit factor* of a nonzero sequence f is

$$\mathrm{ADF}(f) = \frac{\sum_{\substack{s \in \mathbb{Z} \\ s \neq 0}} |C_f(s)|^2}{C_f(0)^2} = -1 + \frac{\sum_{s \in \mathbb{Z}} |C_f(s)|^2}{C_f(0)^2}, \tag{1}$$

which is the sum of the squared magnitudes of all autocorrelation values at nonzero shifts for the sequence that one obtains from f by normalizing it to have unit Euclidean norm. The *(autocorrelation) merit factor* is the reciprocal of the autocorrelation demerit factor; it was introduced by Golay in [5, p. 450] as the "factor" for a sequence and then as the "merit factor" in [6, p. 460], while "demerit factor" appears later in the work of Sarwate [12, p. 102].

Sequences with low demerit factor (equivalently, high merit factor) are highly desirable for communications and ranging applications. For each given length ℓ, we would like to understand the distribution of the demerit factors of binary sequences of length ℓ, which always have $C_f(0) = \ell$, so the denominator of the last fraction in (1) is always ℓ^2. Thus, it is often convenient to study the numerator of the last fraction in (1), which is the sum of the squares of all the autocorrelation values, so we define

$$\mathrm{SSAC}(f) = \sum_{s \in \mathbb{Z}} |C_f(s)|^2,$$

so that for a binary sequence of length ℓ we have

$$\mathrm{ADF}(f) = -1 + \frac{\mathrm{SSAC}(f)}{\ell^2}. \tag{2}$$

For this entire paper, $\mathrm{Seq}(\ell)$ denotes the set of 2^ℓ binary sequences of length ℓ with the uniform probability distribution, and the expected value of a random variable v with

respect to this distribution is denoted by $\mathbb{E}_f^\ell v(f) = \mathbf{E}_{f\in\mathrm{Seq}(\ell)}(v(f))$. The pth central moment of the random variable $v(f)$ as f ranges over the binary sequences of length ℓ is denoted

$$\mu_{p,f}^\ell v(f) = \mathbb{E}_f^\ell \left(v(f) - \mathbb{E}_f^\ell v(f)\right)^p, \tag{3}$$

and the pth standardized moment is denoted by

$$\tilde{\mu}_{p,f}^\ell v(f) = \frac{\mu_{p,f}^\ell v(f)}{\left(\mu_{2,f}^\ell v(f)\right)^{p/2}}.$$

Sarwate [12, eq. (13)] found the mean of the demerit factor for binary sequences of a given length.

Theorem 1 (Sarwate, 1984)**.** *If ℓ is a positive integer, then $\mathbb{E}_f^\ell \mathrm{ADF}(f) = 1 - 1/\ell$.*

Borwein and Lockhart [3, pp. 1469–1470] showed that the variance of the demerit factor for binary sequences of length ℓ tends to 0 as ℓ tends to infinity. Jedwab [9, Theorem 1] gives an exact formula for the variance of the demerit factor for binary sequences of length ℓ. We present a formula involving a quasi-polynomial divided by the fourth power of the length that is equivalent to Jedwab's formula for the variance.

Theorem 2 (Jedwab, 2019)**.** *If ℓ is a positive integer, then*

$$\mu_{2,f}^\ell \mathrm{ADF}(f) = \begin{cases} \frac{16\ell^3-60\ell^2+56\ell}{3\ell^4} & \text{if } \ell \text{ is even,} \\ \frac{16\ell^3-60\ell^2+56\ell-12}{3\ell^4} & \text{if } \ell \text{ is odd.} \end{cases}$$

When one compares the calculation of the variance by Jedwab with that of the mean by Sarwate, one finds the first instance of a general principle: for each p, the determination of the $(p+1)$th moment is always considerably more difficult than that of the pth moment. Jedwab follows the method of Aupetit et al. [1], which involves many multiple summations and is therefore somewhat difficult to execute precisely: Jedwab had to correct the calculation of Aupetit et al. to get the right formula.

In this paper, we devise a new combinatorial method for calculating the moments of the distribution of the demerit factor of binary sequences of length ℓ. For any given p, one may use the technique to obtain an exact formula for the pth central moment of the demerit factor as a function of the length ℓ. For $p = 2$, this entails a short calculation that yields Jedwab's formula for variance. To demonstrate that one can go further, we also use our formula for $p = 3$ to derive an exact formula for the third central moment of $\mathrm{SSAC}(f)$ as a quasi-polynomial function of sequence length, from which we determine the third central moment and third standardized moment (skewness) of $\mathrm{ADF}(f)$.

Theorem 3. *If ℓ is a positive integer, then*

$$\mu_{3,f}^\ell \mathrm{ADF}(f) = \begin{cases} \frac{160\ell^4-1296\ell^3+3296\ell^2-2496\ell}{\ell^6} & \text{if } \ell \equiv 0 \bmod 4, \\ \frac{160\ell^4-1296\ell^3+3296\ell^2-2736\ell+576}{\ell^6} & \text{if } \ell \equiv \pm 1 \bmod 4, \\ \frac{160\ell^4-1296\ell^3+3296\ell^2-2496\ell-384}{\ell^6} & \text{if } \ell \equiv 2 \bmod 4, \end{cases}$$

and

$$\tilde{\mu}^{\ell}_{3,f}\,\mathrm{ADF}(f) = \begin{cases} \frac{6\sqrt{3}(10\ell^4-81\ell^3+206\ell^2-156\ell)}{(4\ell^3-15\ell^2+14\ell)^{3/2}} & \text{if } \ell \equiv 0 \bmod 4, \\ \frac{6\sqrt{3}(10\ell^4-81\ell^3+206\ell^2-171\ell+36)}{(4\ell^3-15\ell^2+14\ell-3)^{3/2}} & \text{if } \ell \equiv \pm 1 \bmod 4, \\ \frac{6\sqrt{3}(10\ell^4-81\ell^3+206\ell^2-156\ell-24)}{(4\ell^3-15\ell^2+14\ell)^{3/2}} & \text{if } \ell \equiv 2 \bmod 4. \end{cases}$$

We also report in Theorem 20 a computer-assisted determination of the fourth central moment of $\mathrm{SSAC}(f)$ as a quasi-polynomial function of sequence length, from which we obtain the fourth central moment and fourth standardized moment (kurtosis) of $\mathrm{ADF}(f)$ (see Corollaries 21 and 22).

Theorem 4. *If ℓ is a positive integer, then $\mu^{\ell}_{4,f}\,\mathrm{ADF}(f)$ is a quasi-polynomial function of ℓ of degree 6 and period 120 divided by the polynomial ℓ^8 (see Corollary 21 for the precise function), while $\tilde{\mu}^{\ell}_{4,f}\,\mathrm{ADF}(f)$ is a quasi-polynomial function of ℓ of degree 6 and period 120 divided by a quasi-polynomial function of ℓ of degree 6 and period 2 (see Corollary 22 for the precise function).*

Our computer program was also able to find the fifth central moment of ADF as a quasi-polynomial function of ℓ of degree 7 and period 55440 divided by the polynomial ℓ^{10}. Our methods also shed light on interesting aspects of the distribution of demerit factors. For instance, we show that our general theory implies that the odd central moments are always nonnegative, and we can also determine precisely when central moments are zero.

Theorem 5. *Let ℓ and p be positive integers. Then $\mu^{\ell}_{p,f}\,\mathrm{ADF}(f)$ is nonnegative. Moreover, if (i) $p = 1$, (ii) p is odd with $p > 1$ and $\ell \leq 3$, or (iii) p is even and $\ell \leq 2$, then $\mu^{\ell}_{p,f}\,\mathrm{ADF}(f)$ is zero; otherwise it is strictly positive.*

Our method can be developed further to prove that the pth central moment of SSAC for sequences of length ℓ is always a quasi-polynomial function of ℓ with rational coefficients. Further developments of our method also show that in the limit as $\ell \to \infty$, all the standardized moments of the autocorrelation demerit factor tend to those of the standard normal distribution. The additional theoretical tools used to obtain these results are introduced and explored in [10].

The rest of this paper is organized as follows. Section 2 has preliminary conventions and definitions. Section 3 exhibits an exact formula for the central moments of SSAC (cf. Proposition 11). Section 4 describes a group action that yields an easier formula (cf. Proposition 17), and Section 5 discusses an algorithm to assist in the use of this formula. Section 6 discusses the proof of Theorem 5. Section 7 is a brief exposition about how we apply our theory to compute the variance, thus confirming Jedwab's result in Theorem 2. Section 8 follows with a discussion of the exact calculation of skewness reported in Theorem 3. Section 9 then reports on our computer-assisted determination of the kurtosis in reported in Theorem 4.

2 Notation and definitions

In this section, we give the basic conventions, notations, and definitions, mostly concerning particular kinds of partitions and functions, which are used in Section 3 to obtain an exact formula for the central moments (cf. Proposition 11).

We use the convention that $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{Z}_+ = \{1, 2, 3, \ldots\}$. If $\ell \in \mathbb{N}$, we write $[\ell]$ to mean $\{0, 1, \ldots, \ell - 1\}$. If S and T are sets, then T^S denotes the set of all functions from S into T.

A partition of a set A is a collection of nonempty, disjoint subsets of A whose union is A. If $\mathcal{P}$ is a partition of A, then $\mathcal{P}$ induces an equivalence relation on A that is written $a_1 \equiv a_2 \pmod{\mathcal{P}}$, which means that there is some class $P \in \mathcal{P}$ such that $a_1, a_2 \in P$.

Our calculation of the pth central moment of the demerit factor of binary sequences of a given length depends on partitions of $[p] \times [2] \times [2]$.

Definition 6 (**Part(p)**)**.** If p is a nonnegative integer, $\mathrm{Part}(p)$ is the set of all partitions of $[p] \times [2] \times [2]$.

To influence the calculation, a partition must have certain properties. We define the first of these.

Definition 7 (Globally even, locally odd (GELO) partition)**.** Let $p \in \mathbb{N}$. Then $\mathcal{P} \in \mathrm{Part}(p)$ is said to be *globally even, locally odd* (abbreviated *GELO*) if $|P|$ is even for every $P \in \mathcal{P}$ and for every $e \in [p]$ there is some $Q \in \mathcal{P}$ such that $|(\{e\} \times [2] \times [2]) \cap Q|$ is odd.

A certain kind of function, which we shall call an *assignment*, plays a critical role in our probability calculations.

Definition 8 (Assignment)**.** Let $p \in \mathbb{N}$. An *assignment for* $[p]$ is a function from $[p] \times [2] \times [2]$ into $\mathbb{N}$, i.e., an element of $\mathbb{N}^{[p]\times[2]\times[2]}$. The following are notations for the set of all assignments for $[p]$ and some of its important subsets:

- $\mathrm{As}([p]) = \mathbb{N}^{[p]\times[2]\times[2]}$, the set of all assignments for $[p]$,
- $\mathrm{As}([p], \ell) = \{\tau \in \mathrm{As}([p]) : \tau([p] \times [2] \times [2]) \subseteq [\ell]\}$,
- $\mathrm{As}([p], =) = \{\tau \in \mathrm{As}([p]) : \tau(e, 0, 0) + \tau(e, 0, 1) = \tau(e, 1, 0) + \tau(e, 1, 1)$ for every $e \in [p]\}$, and
- $\mathrm{As}([p], =, \ell) = \mathrm{As}([p], =) \cap \mathrm{As}([p], \ell)$.

Furthermore, if $\mathcal{P} \in \mathrm{Part}(p)$, then

- $\mathrm{As}(\mathcal{P}) = \{\tau \in \mathrm{As}([p]) : \tau(\beta) = \tau(\gamma)$ iff $\beta \equiv \gamma \bmod \mathcal{P}\}$,
- $\mathrm{As}(\mathcal{P}, \ell) = \mathrm{As}(\mathcal{P}) \cap \mathrm{As}([p], \ell)$,
- $\mathrm{As}(\mathcal{P}, =) = \mathrm{As}(\mathcal{P}) \cap \mathrm{As}([p], =)$, and
- $\mathrm{As}(\mathcal{P}, =, \ell) = \mathrm{As}(\mathcal{P}) \cap \mathrm{As}([p], =) \cap \mathrm{As}([p], \ell)$.

We now define another kind of partition that is significant in our calculation of moments.

Definition 9 (Satisfiable partition)**.** Let $p \in \mathbb{N}$. A partition $\mathcal{P}$ of $[p] \times [2] \times [2]$ is said to be *satisfiable* if $\mathrm{As}(\mathcal{P}, =)$ is nonempty. (Equivalently, there is some $\ell \in \mathbb{N}$ such that $\mathrm{As}(\mathcal{P}, =, \ell)$ is nonempty.) We denote the set of satisfiable partitions of $[p] \times [2] \times [2]$ as $\mathrm{Sat}(p)$.

When we calculate the moments of the distribution of demerit factors, it turns out that every nonzero term in our calculation corresponds to some partition combining the attributes of both Definitions 7 and 9, so we name such partitions accordingly.

Definition 10 (Contributory partition)**.** Let $p \in \mathbb{N}$. Then a partition $\mathcal{P}$ of $[p] \times [2] \times [2]$ is said to be *contributory* if it is globally even, locally odd and satisfiable. We denote the set of contributory partitions of $[p] \times [2] \times [2]$ as $\mathrm{Con}(p)$. That is, $\mathrm{Con}(p) = \mathrm{GELO}(p) \cap \mathrm{Sat}(p)$.

3 Moments from partitions

In this section, we exhibit an exact formula for central moments of $\mathrm{SSAC}(f)$, the sum of the squares of the autocorrelation values for a sequence f, where the moments are computed with f ranging over the set $\mathrm{Seq}(\ell)$ of all binary sequences of a given length ℓ (equipped with uniform probability measure). Recall from the Introduction that we use $\mathbb{E}_f^\ell v(f) = \mathbf{E}_{f \in \mathrm{Seq}(\ell)}(v(f))$ to denote the expected value of a random variable v depending on f as f ranges over $\mathrm{Seq}(\ell)$. Also, recall from (3) that the pth central moment of the random variable $v(f)$ as f ranges over $\mathrm{Seq}(\ell)$ is denoted

$$\mu_{p,f}^\ell v(f) = \mathbb{E}_f^\ell \left(v(f) - \mathbb{E}_f^\ell v(f) \right)^p .$$

Since (2) shows that the demerit factor of a binary sequence f of length ℓ is $\mathrm{ADF}(f) = -1 + \mathrm{SSAC}(f)/\ell^2$, it is easy to determine the pth central moment of the demerit factor from that of SSAC. Proposition 11 provides a way of calculating central moments of the sum of squares of the autocorrelation in terms of contributory partitions and assignments.

Proposition 11. *For $p, \ell \in \mathbb{N}$, we have*

$$\mu_{p,f}^\ell \mathrm{SSAC}(f) = \sum_{\mathcal{P} \in \mathrm{Con}(p)} |\mathrm{As}(\mathcal{P}, =, \ell)|.$$

The proof of this proposition is too long to include here, but it is a combinatorial proof involving a binomial-type expansion of a product of multiple summations. See [11, Sec. 3] for details.

4 Moments from isomorphism classes of partitions

In this section, we exhibit a new formula (in Proposition 17 below) that makes the moment calculations much easier than those performed using Proposition 11. The exact formula

for central moments in Proposition 11 typically involves many similar partitions $\mathcal{P}$ that produce the same value for $|\operatorname{As}(\mathcal{P}, =, \ell)|$, so we devise an equivalence relation (via a group action) to organize these partitions into classes.

We first describe the group in our action. If $p \in \mathbb{N}$, then we use S_p to denote the group of all permutations of $[p]$. The group in our action is the following wreath product of wreath products: $\mathcal{W}^{(p)} = (S_2 \operatorname{Wr}_{[2]} S_2) \operatorname{Wr}_{[p]} S_p$. Each element $\pi \in \mathcal{W}^{(p)}$ permutes $[p] \times [2] \times [2]$ in a certain way; see [11, Notation 4.1] for details. If $\pi \in \mathcal{W}^{(p)}$ and $P \subseteq [p] \times [2] \times [2]$ and $\mathcal{Q}$ is a set of subsets of $[p] \times [2] \times [2]$, then we let π act on P by setting $\pi(P) = \{\pi(e, s, v) : (e, s, v) \in P\}$ and we let π act on $\mathcal{Q}$ by setting $\pi(\mathcal{Q}) = \{\pi(Q) : Q \in \mathcal{Q}\}$. This gives an action of π on $\operatorname{Part}(p)$. If τ is an assignment from $\operatorname{As}([p])$, we define $\pi^*(\tau) = \tau \circ \pi$, so that $\mathcal{W}^{(p)}$ acts on $\operatorname{As}([p])$ by $\tau \mapsto \pi^*(\tau)$. Then we have the following result concerning the assignment counts of interest in Proposition 11.

Lemma 12. *Let $p, \ell \in \mathbb{N}$ and suppose that $\pi \in \mathcal{W}^{(p)}$ and $\mathcal{P} \in \operatorname{Part}(p)$. Then we have $\pi^*(\operatorname{As}(\pi(\mathcal{P}), =, \ell)) = \operatorname{As}(\mathcal{P}, =, \ell)$.*

This shows that partitions within the same orbit of the action of our group $\mathcal{W}^{(p)}$ make the same contribution to the summation in Proposition 11.

Definition 13 (Isomorphic partitions, isomorphism class)**.** Let $p \in \mathbb{N}$ and $\mathcal{P}, \mathcal{Q} \in \operatorname{Part}(p)$. Then we say that $\mathcal{P}$ and $\mathcal{Q}$ are *isomorphic* and write $\mathcal{P} \cong \mathcal{Q}$ to mean that there exists $\pi \in \mathcal{W}^{(p)}$ such that $\mathcal{Q} = \pi(\mathcal{P})$. The *isomorphism class* of $\mathcal{P}$ is the set of all partitions that are isomorphic to $\mathcal{P}$.

Since $\mathcal{W}^{(p)}$ is a group, the isomorphism relation is clearly an equivalence relation. It turns out that all partitions isomorphic to a contributory partition are also contributory.

Lemma 14. *Let $p, \ell \in \mathbb{N}$. If $\mathcal{P}, \mathcal{Q} \in \operatorname{Part}(p)$ with $\mathcal{P} \cong \mathcal{Q}$, then $\mathcal{P} \in \operatorname{Con}(p)$ if and only if $\mathcal{Q} \in \operatorname{Con}(p)$, and furthermore $|\operatorname{As}(\mathcal{P}, =, \ell)| = |\operatorname{As}(\mathcal{Q}, =, \ell)|$.*

This last result shows that each orbit in $\operatorname{Part}(p)$ under the action of $\mathcal{W}^{(p)}$ either contains only contributory partitions or no contributory partitions at all. Since we are primarily interested in the contributory partitions and their equivalence classes, we make a name for the set of all such classes.

Definition 15 (**Isom(p)**)**.** Let $p \in \mathbb{N}$. We use $\operatorname{Isom}(p)$ to denote the set of isomorphism classes of partitions in $\operatorname{Con}(p)$.

In view of Lemma 14, it is helpful to have a notation for the common value of $|\operatorname{As}(\mathcal{P}, =, \ell)|$ for all partitions $\mathcal{P}$ in an isomorphism class of contributory partitions.

Definition 16 (**Sols($\mathfrak{P}, \ell$)**)**.** Let $p, \ell \in \mathbb{N}$. If $\mathfrak{P}$ is any subset of $\operatorname{Part}(p)$ such that all partitions in $\mathfrak{P}$ are isomorphic to each other, we let $\operatorname{Sols}(\mathfrak{P}, \ell)$ be the common value (by Lemma 14) of $|\operatorname{As}(\mathcal{P}, =, \ell)|$ for $\mathcal{P} \in \mathfrak{P}$.

We most commonly use this definition when $\mathfrak{P} \in \operatorname{Isom}(p)$. Now our formula in Proposition 11 for central moments of the sum of squares of autocorrelation can be made much less unwieldy by grouping terms according to isomorphisms classes.

Proposition 17. *If $p, \ell \in \mathbb{N}$, then*

$$\mu^{\ell}_{p,f}\,\mathrm{SSAC}(f) = \sum_{\mathfrak{P}\in\mathrm{Isom}(p)} |\mathfrak{P}|\,\mathrm{Sols}(\mathfrak{P},\ell).$$

5 Finding contributory partitions

In order to use Proposition 17 to compute the pth central moment of SSAC, we need to find all the isomorphism classes of contributory partitions of $[p] \times [2] \times [2]$. It turns out that a matrix algorithm can be devised to make this search straightforward. This is described in detail in [11, Procedure 5.13].

6 Positivity of moments

Proposition 11 gives the pth central moment of SSAC as a sum of cardinalities, which means that all the central moments are nonnegative. In fact, the pth central moment for $p \geq 2$ is strictly positive for almost all lengths of binary sequences, with the exceptions noted in Theorem 5 of the Introduction. The proof of this amounts to showing that there does exist at least one partition $\mathcal{P} \in \mathrm{Con}(p)$ for all $p \geq 2$ and that the number $|\,\mathrm{As}(\mathcal{P}, =, \ell)|$ of associated assignments is strictly positive for ℓ sufficiently large. See [11, Section 6] for details.

7 Explicit calculation of variance

The calculation of the variance of SSAC (and then of ADF) is detailed in [11, Section 7]. Since we use Proposition 17, the first challenge is finding all the isomorphism classes contributory partitions. We present the results of the search here; see [11, Example 5.14] for details.

Lemma 18. *There are precisely two equivalence classes, $\mathfrak{C}_1$ and $\mathfrak{C}_2$, in* Isom(2)*, which are represented respectively by partitions*

$$\mathcal{P}_1 = \Big\{\{(0,0,0),(0,0,1),(1,0,0),(1,0,1)\},\{(0,1,0),(1,1,0)\},\{(0,1,1),(1,1,1)\}\Big\} \text{ and}$$
$$\mathcal{P}_2 = \Big\{\{(0,0,0),(1,0,0)\},\{(0,0,1),(1,0,1)\},\{(0,1,0),(1,1,0)\},\{(0,1,1),(1,1,1)\}\Big\}.$$

To apply Proposition 17, we now need to find $|\mathfrak{P}|$ and $\mathrm{Sols}(\mathfrak{P})$ for each isomorphism class $\mathfrak{P}$. We compute these in [11, Example 4.6 and Lemma 7.1] to obtain the variance of SSAC, and then use (2) to obtain the variance of ADF, which is reported Theorem 2 of the Introduction.

8 Explicit calculation of skewness

The calculation of the skewness of SSAC (and then of ADF) is detailed in [11, Section 8]. Since we use Proposition 17, the first challenge is finding all the isomorphism classes contributory partitions. We present the results of the search here; see [11, Lemma 8.1] for details.

Lemma 19. *There are precisely eight equivalence classes,* $\mathfrak{C}_1, \ldots, \mathfrak{C}_8$*, in* Isom(3)*, which are represented respectively by partitions*

$$\mathcal{P}_1 = \Big\{\big\{(0,0,0),(0,0,1),(1,1,0),(2,0,0)\big\},\big\{(1,0,0),(1,0,1),(0,1,0),(2,0,1)\big\},\big\{(0,1,1),(2,1,0)\big\},\big\{(1,1,1),(2,1,1)\big\}\Big\};$$

$$\mathcal{P}_2 = \Big\{\big\{(0,0,0),(0,0,1),(1,0,0),(1,0,1)\big\},\big\{(0,1,0),(2,0,0)\big\},\big\{(0,1,1),(2,0,1)\big\},\big\{(1,1,0),(2,1,0)\big\},\big\{(1,1,1),(2,1,1)\big\}\Big\};$$

$$\mathcal{P}_3 = \Big\{\big\{(0,0,0),(0,0,1),(1,1,0),(2,1,0)\big\},\big\{(1,0,0),(1,0,1)\big\},\big\{(2,0,0),(2,0,1)\big\},\big\{(0,1,0),(1,1,1)\big\},\big\{(0,1,1),(2,1,1)\big\}\Big\};$$

$$\mathcal{P}_4 = \Big\{\big\{(0,0,0),(0,0,1),(1,0,0),(2,0,0)\big\},\big\{(0,1,0),(1,1,0)\big\},\big\{(0,1,1),(2,1,0)\big\},\big\{(1,0,1),(2,1,1)\big\},\big\{(1,1,1),(2,0,1)\big\}\Big\};$$

$$\mathcal{P}_5 = \Big\{\big\{(0,0,0),(0,0,1)\big\},\big\{(1,0,0),(1,0,1)\big\},\big\{(2,0,0),(2,0,1)\big\},\big\{(1,1,0),(2,1,1)\big\},\big\{(2,1,0),(0,1,1)\big\},\big\{(0,1,0),(1,1,1)\big\}\Big\};$$

$$\mathcal{P}_6 = \Big\{\big\{(0,0,0),(0,0,1)\big\},\big\{(1,0,0),(1,0,1)\big\},\big\{(0,1,0),(2,0,0)\big\},\big\{(0,1,1),(2,1,0)\big\},\big\{(1,1,0),(2,0,1)\big\},\big\{(1,1,1),(2,1,1)\big\}\Big\};$$

$$\mathcal{P}_7 = \Big\{\big\{(0,0,0),(1,1,0)\big\},\big\{(0,0,1),(1,1,1)\big\},\big\{(1,0,0),(2,1,0)\big\},\big\{(1,0,1),(2,1,1)\big\},\big\{(2,0,0),(0,1,0)\big\},\big\{(2,0,1),(0,1,1)\big\}\Big\};\text{ and}$$

$$\mathcal{P}_8 = \Big\{\big\{(0,0,0),(1,1,1)\big\},\big\{(0,1,0),(1,0,1)\big\},\big\{(1,0,0),(2,1,1)\big\},\big\{(1,1,0),(2,0,1)\big\},\big\{(2,0,0),(0,1,1)\big\},\big\{(2,1,0),(0,0,1)\big\}\Big\}.$$

To apply Proposition 17, we now need to find $|\mathfrak{P}|$ and $\mathrm{Sols}(\mathfrak{P})$ for each isomorphism class $\mathfrak{P}$. We compute these in [11, Lemmas 8.2–8.3] to obtain the third central moment of SSAC, and then use (2) to obtain the third central moment of ADF, which is reported Theorem 3 of the Introduction. Dividing the third central moment of ADF by the 3/2 power of the variance produces the skewness, which is also reported in Theorem 3 of the Introduction.

9 Computer-assisted calculation of kurtosis and fifth moment

A computer program was used to find the fourth central moment of SSAC. The program first finds representatives for each isomorphism class $\mathfrak{C}$ in Isom(4). This is done by the matrix algorithm alluded to in Section 5, and the program finds 97 isomorphism classes. For each class $\mathfrak{C}$ in Isom(4), the program determines $|\mathfrak{C}|$ using an orbit-stabilizer technique and determines $\mathrm{Sols}(\mathfrak{C}, \ell)$ using Ehrhart theory and inclusion-exclusion, since finding $\mathrm{Sols}(\mathfrak{C}, \ell)$ requires one to count the number of integer solutions of a homogeneous linear system that lie in a hypercube as a function of the size of the hypercube (see [2, Ch. 3]) and to then deduct the number of solutions whose coordinates do not have distinct values. The program uses these calculations to compute the sum in Proposition 17 with $p = 4$, and thereby determines the fourth central moment of SSAC. The result is given below as Theorem 20. The program was written in C++ and employing the GNU Multiple Precision Arithmetic Library (GMP) [4], and obtained the fourth central moment of SSAC in about 5 seconds on a personal computer. The same program also obtained the second a third moments of SSAC, and its results agree with our hand calculations in Sections 7 and 8. With a few hours of computation time, the program was also able to find that Isom(5) has 2581 isomorphism classes and then to compute an exact formula for the fifth central moment of SSAC as a quasi-polynomial of degree 7 and period 55440.

Theorem 20. *For $\ell \in \mathbb{N}$, the quantity $\mu^{\ell}_{4,f}\,\mathrm{SSAC}(f)$ is a quasi-polynomial function of ℓ of degree* 6 *and period* 120 *given by*

$$\mu^{\ell}_{4,f}\,\mathrm{SSAC}(f) = \frac{1}{45}\sum_{j=0}^{6} a_j(\ell)\ell^j,$$

where for every ℓ we have $a_6(\ell) = 3840$; $a_5(\ell) = 501120$; $a_4(\ell) = -6786480$;

$$a_3(\ell) = \begin{cases} \textit{27078080} & \textit{if } \ell \equiv 0 \pmod 2, \\ \textit{27072320} & \textit{if } \ell \equiv 1 \pmod 2; \end{cases}$$

$$a_2(\ell) = \begin{cases} \textit{-17638464} & \textit{if } \ell \equiv 0 \pmod 2, \\ \textit{-18213024} & \textit{if } \ell \equiv 1 \pmod 2; \end{cases}$$

$$a_1(\ell) = \begin{cases} \textit{-69561600} & \textit{if } \ell \equiv 0 \pmod{12}, \\ \textit{-71342400} & \textit{if } \ell \equiv \pm 1, \pm 5 \pmod{12}, \\ \textit{-75982080} & \textit{if } \ell \equiv \pm 2 \pmod{12}, \\ \textit{-68516160} & \textit{if } \ell \equiv \pm 3 \pmod{12}, \\ \textit{-72387840} & \textit{if } \ell \equiv \pm 4 \pmod{12}, \\ \textit{-73155840} & \textit{if } \ell \equiv 6 \pmod{12}; \end{cases}$$

and $a_0(\ell)$ is a function of period 120 *whose values are given on Table 1.*

Since $\mathrm{ADF}(f) = -1 + \mathrm{SSAC}(f)/\ell^2$, we can divide this result by ℓ^8 to obtain the fourth central moment of the demerit factor.

Table 1: Values of $a_0(\ell)$ as a function of $\ell \pmod{120}$

$\ell \pmod{120}$	$a_0(\ell)$	$\ell \pmod{120}$	$a_0(\ell)$	$\ell \pmod{120}$	$a_0(\ell)$
0	0	21, 69	53732304	51, 99	57464784
1, 49	68764624	22, 58, 82, 118	100980736	53, 77	76964816
2, 38, 62, 98	98195456	23, 47	79591376	55	60110800
3, 27	63657936	24, 96	12386304	56, 104	43065344
4, 76	48062464	25	56378320	60	2211840
5	58385360	28, 52	54255616	61, 109	69870544
6, 54, 66, 114	61323264	29, 101	70771664	63, 87	62552016
7, 103	78690256	30, 90	48936960	65	57279440
8, 32	49258496	31, 79	72497104	68, 92	51470336
9, 81	52626384	33, 57	58819536	71, 119	73398224
10, 70	82401280	34, 46, 94, 106	94787584	73, 97	74957776
11, 59	74504144	35	62117840	75	45078480
12, 108	20791296	36, 84	14598144	80	30679040
13, 37	76063696	39, 111	56358864	83, 107	80697296
14, 26, 74, 86	92002304	40	33464320	85	57484240
15	43972560	41, 89	69665744	88, 112	52043776
16, 64	45850624	43, 67	79796176	93, 117	59925456
17, 113	75858896	44, 116	45277184	95	61011920
18, 42, 78, 102	67516416	45	41346000	100	35676160
19, 91	73603024	48, 72	18579456	105	40240080
20	32890880	50, 110	79616000	115	61216720

Corollary 21. *If $\ell \in \mathbb{Z}_+$, then*

$$\mu_{4,f}^{\ell}\,\mathrm{ADF}(f) = \frac{\mu_{4,f}^{\ell}\,\mathrm{SSAC}(f)}{\ell^8},$$

where $\mu_{4,f}^{\ell}\,\mathrm{SSAC}(f)$ is the quasi-polynomial function of degree 6 and period 120 described in Theorem 20.

We can normalize the fourth central moment using the variance from Theorem 2 to obtain the kurtosis of $\mathrm{SSAC}(f)$, which is the same as the kurtosis of $\mathrm{ADF}(f) = -1 + \mathrm{SSAC}(f)/\ell^2$.

Corollary 22. *If $\ell \in \mathbb{Z}_+$, then*

$$\tilde{\mu}_{4,f}^{\ell}\,\mathrm{ADF}(f) = \tilde{\mu}_{4,f}^{\ell}\,\mathrm{SSAC}(f) = \frac{\mu_{4,f}^{\ell}\,\mathrm{SSAC}(f)}{\left(\mu_{2,f}^{\ell}\,\mathrm{SSAC}(f)\right)^2},$$

where $\mu_{4,f}^{\ell}\,\mathrm{SSAC}(f)$ is the quasi-polynomial function of degree 6 and period 120 described in Theorem 20 and $\mu_{2,f}^{\ell}\,\mathrm{SSAC}(f)$ is the quasi-polynomial function of degree 3 and period 2 described in Theorem 2.

Acknowledgements

The authors thank Bernardo Ábrego and Silvia Fernández-Merchant for helpful discussions and suggestions.

References

[1] S. Aupetit, P. Liardet, and M. Slimane. Evolutionary search for binary strings with low aperiodic auto-correlations. In P. Liardet, P. Collet, C. Fonlupt, E. Lutton, and M. Schoenauer, editors, *Artificial Evolution*, volume 2936 of *Lecture Notes in Computer Science*, pages 39–50, 2004.

[2] M. Beck and S. Robins. *Computing the continuous discretely*. Undergraduate Texts in Mathematics. Springer, New York, second edition, 2015.

[3] P. Borwein and R. Lockhart. The expected L_p norm of random polynomials. *Proc. Amer. Math. Soc.*, 129(5):1463–1472, 2001.

[4] Free Software Foundation, Inc. *GNU MP version* `6.2.1`, 2020. Available at `https://gmplib.org/`.

[5] M. J. E. Golay. A class of finite binary sequences with alternate autocorrelation values equal to zero. *IEEE Trans. Inform. Theory*, 18:449–450, 1972.

[6] M. J. E. Golay. Hybrid low autocorrelation sequences. *IEEE Trans. Inform. Theory*, 21:460–462, 1975.

[7] S. W. Golomb. *Shift register sequences*. With portions co-authored by Lloyd R. Welch, Richard M. Goldstein, and Alfred W. Hales. Holden-Day, Inc., San Francisco, Calif.-Cambridge-Amsterdam, 1967.

[8] S. W. Golomb and G. Gong. *Signal design for good correlation*. Cambridge University Press, Cambridge, 2005.

[9] J. Jedwab. The mean and variance of the reciprocal merit factor of four classes of binary sequences. arXiv:1911.11246, 2024.

[10] D. J. Katz and M. E. Ramirez. Limiting moments of autocorrelation demerit factors of binary sequences. arXiv:2307.14566, 2023.

[11] D. J. Katz and M. E. Ramirez. Moments of autocorrelation demerit factors of binary sequences. arXiv:2307.14281, 2024.

[12] D. V. Sarwate. Mean-square correlation of shift-register sequences. *Communications, Radar and Signal Processing, IEE Proceedings F*, 131(2):101–106, 1984.

[13] M. R. Schroeder. *Number theory in science and communication*, volume 7 of *Springer Series in Information Sciences*. Springer-Verlag, Berlin, fourth edition, 2006.

A Direct Method for Calculating the Differential Spectrum of an APN Power Mapping

Yongbo Xia*, Furong Bao*, Shaoping Chen†, and Tor Helleseth ‡

Abstract

Let n be a positive integer, p be an odd prime, $d = \frac{p^n+1}{4} + \frac{p^n-1}{2}$ if $p^n \equiv 3 \pmod 8$ and $d = \frac{p^n+1}{4}$ if $p^n \equiv 7 \pmod 8$. When $p^n > 7$, the power mapping x^d from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ was proved to be almost perfect nonlinear by Helleseth, Rong and Sandberg in IEEE Trans. Inform. Theory, 45(2): 475-485, 1999. By establishing a system of linear equations related to the differential spectrum, Tan and Yan completely determined the differential spectrum of this power mapping in Des. Codes Cryptogr., 91(8): 2755-2768, 2023. In this paper, we directly characterize the conditions on $b \in \mathbb{F}_{p^n}$ under which the differential equation $(x+1)^d - x^d = b$ has exactly i solution(s) for $i = 0, 1, 2$, respectively. Then, using the theory of elliptic curves, the number of those b's in each case is determined and thus the differential spectrum of x^d is obtained. Our method releases more information about the differential equation of x^d, which can be used to describe the DDT of this APN power function.

Keywords Differential spectrum, power mapping, almost perfect nonlinear, elliptic curve.
MSC (2020) 94A60, 11T71, 11T06, 05-08

1 Introduction

Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements and $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$, where p is a prime integer and n is a positive integer. Let $F(x)$ be a mapping from $\mathbb{F}_{p^n}$ to itself. The *derivative function* of $F(x)$ at an element $a \in \mathbb{F}_{p^n}$, denoted by $\mathbb{D}_a F$, is given by

$$\mathbb{D}_a F(x) = F(x+a) - F(x).$$

For any a, $b \in \mathbb{F}_{p^n}$, the equation $\mathbb{D}_a F(x) = b$ is called the *differential equation* of $F(x)$ with input difference a and output difference b. Let $\delta_F(a,b) = |\{x \in \mathbb{F}_{p^n} \mid \mathbb{D}_a F(x) = b\}|$,

*Y. Xia and F. Bao are with the Department of Mathematics and Statistics, South-Central University for Nationalities, Wuhan 430074, China (xia@mail.scuec.edu.cn). Y. Xia is also with the Hubei Key Laboratory of Intelligent Wireless Communications, South-Central University for Nationalities, Wuhan 430074, China.

†S. Chen is with the Hubei Key Laboratory of Intelligent Wireless Communications, South-Central University for Nationalities, Wuhan 430074, China (spchen@scuec.edu.cn).

‡T. Helleseth is with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway (tor.helleseth@uib.no).

where $|S|$ denotes the cardinality of the set S. The *differential distribution table (DDT)* of $F(x)$ is the two-dimensional table defined by

$$(\delta_F(a,b))_{a\in\mathbb{F}_{p^n},\, b\in\mathbb{F}_{p^n}}.$$

The *differential uniformity* of $F(x)$ is defined as

$$\delta(F)=\max\{\delta_F(a,b)\mid a\in\mathbb{F}_{p^n}^*,\ b\in\mathbb{F}_{p^n}\}.$$

The function $F(x)$ is said to be differentially δ-uniform if $\delta(F)=\delta$. In particular, $F(x)$ is called a perfect nonlinear (PN) function if $\delta(F)=1$, and an almost perfect nonlinear (APN) function if $\delta(F)=2$.

Differential uniformity is an important concept in cryptography introduced by Nyberg [8], which can be used to quantify the security of the block cipher with respect to the differential attack if $F(x)$ used in the S-box. The lower the differential uniformity of $F(x)$ is, the stronger it is to resist the differential attack. Power functions with low differential uniformity have been extensively studied due to their strong resistance to differential attacks and low implementation cost.

For a power mapping $F(x)=x^d$, it is readily seen that $\delta_F(a,b)=\delta_F(1,b/a^d)$ for all $a\in\mathbb{F}_{p^n}^*$ and $b\in\mathbb{F}_{p^n}$. The *differential spectrum* of $F(x)=x^d$ is defined as $[\omega_0,\omega_1,...,\omega_\delta]$ with

$$\omega_i=|\{b\mid \delta_F(1,b)=i, b\in\mathbb{F}_{p^n}\}|.$$

Compared to the differential uniformity, the differential spectrum of a power mapping reflects more information about its differential property [1, 2, 3, 4]. The whole differential spectrum and even the form of the DDT play important roles when the resistance against several variants of differential cryptanalysis is quantified. According to the definition, the differential spectrum of a power mapping $F(x)$ with $\delta(F)=\delta$ satisfies the following identities:

$$\sum_{i=0}^{\delta}\omega_i=p^n \text{ and } \sum_{i=0}^{\delta}i\omega_i=p^n. \tag{1}$$

It is an interesting topic to completely determine the differential spectra of power mappings with low differential uniformity. However, this problem typically involves solving nonlinear equations and is generally challenging. More explanations about this topic can be found in [9, 10] and references therein.

Let p be an odd prime, n be a positive integer and

$$d=\begin{cases}\frac{p^n+1}{4}+\frac{p^n-1}{2}, & \text{if } p^n\equiv 3 \pmod 8,\\ \frac{p^n+1}{4}, & \text{if } p^n\equiv 7 \pmod 8.\end{cases} \tag{2}$$

It was proved that $F(x)=x^d$ is an APN function over $\mathbb{F}_{p^n}$ when $p^n>7$ [6]. Notice that when $p^n=7$ or $p^n=3$, we have $d=2$ and the function x^d is a PN function. For the case $p=3$, the APN mapping $F(x)=x^d$ is a special case of the power mapping investigated in [5], for which the differential spectrum has been determined. For $p>3$, utilizing the

theory of elliptic curves, Tan and Yan in [10] determined the number of solutions, denoted by M, to the following equation system

$$\begin{cases} x_1 - x_2 + x_3 - x_4 = 0, \\ x_1^d - x_2^d + x_3^d - x_4^d = 0, \end{cases}$$

which yields the identity $\sum_{i=0}^{2} i^2\omega_i = \omega_1 + 4\omega_2 = (M - p^{2n})/(p^n - 1)$. Combining this identity and those in (1), they obtained a system of linear equations and derived the differential spectrum $[\omega_0, \omega_1, \omega_2]$ of $F(x) = x^d$. This commonly-used method can provide the differential spectra of certain power functions, nevertheless, it does not provide further insight into solving the differential equation. Accordingly, it gives little information about the DDTs.

In this paper, by directly investigating the differential equation $\mathbb{D}_1F(x) = (x+1)^d - x^d = b$ of $F(x) = x^d$, we propose an efficient method to solve it. Then, we characterize the conditions on b under which the differential equation $\mathbb{D}_1F(x) = b$ has exactly zero solution, one solution, and two solutions, respectively. By counting the number of those b's in all cases, we obtain the differential spectrum of $F(x) = x^d$. In this way we release more information about the solutions of the differential equation $\mathbb{D}_1F(x) = b$, which can be used to describe the form of the DDT of this APN power function.

2 Main results and their proofs

In this section, we will investigate the differential equation of the APN function $F(x) = x^d$ with d in (2), and then derive the differential spectrum of $F(x)$. The techniques for investigating the differential equation mainly come from [6, Theorem 4], but additional discussions are required. In the case $p > 3$, the differential spectrum will be expressed in terms of some quadratic character sums. When dealing with the quadratic character sums appeared in this case, we use the theory of elliptic curves and some techniques that are similar to those in [10].

Now we begin to deal with the differential equation of $F(x) = x^d$. Recall that the positive integer d given in (2) has the following two properties:
(i) $\gcd(d, p^n - 1) = 2$, and thus d is even;
(ii) $2d \equiv \frac{p^n+1}{2} \pmod{p^n - 1}$.
In the sequel our discussions are always under the condition that $p^n > 3$. The differential equation $\mathbb{D}_1F(x) = b$ of $F(x) = x^d$ is given by

$$\mathbb{D}_1F(x) = (x+1)^d - x^d = b. \tag{3}$$

For convenience, let $N(b)$ denote the number of its solutions in $\mathbb{F}_{p^n}$. If $b = 0$, since $\gcd(d, p^n - 1) = 2$ the differential equation $\mathbb{D}_1F(x) = 0$ has only one solution $x = -\frac{1}{2}$. This shows that $N(0) = 1$. Hence, in the sequel we will investigate the differential equation $\mathbb{D}_1F(x) = b$ for $b \in \mathbb{F}_{p^n}^*$.

From (3) we see that when $x = 0$, $b = 1$; when $x = -1$, $b = -1$. This implies that for each $b \in \{\pm 1\}$, the differential equation $\mathbb{D}_1F(x) = b$ has exactly one solution

in $\{0,-1\}$. In order to determine $N(1)$ (resp. $N(-1)$), we shall determine how many solutions $\mathbb{D}_1F(x)=1$ (resp. $\mathbb{D}_1F(x)=-1$) has in $\mathbb{F}_{p^n}\setminus\{0,-1\}$. Moreover, for each $b\neq\pm1$, the solutions of $\mathbb{D}_1F(x)=b$ (if they exist) must belong to $\mathbb{F}_{p^n}\setminus\{0,-1\}$. Thus, in what follows we only need to investigate the differential equation $\mathbb{D}_1F(x)=b$ under that conditions that $x\in\mathbb{F}_{p^n}\setminus\{0,-1\}$ and $b\neq0$. Set

$$v_x=x^d \text{ and } v_{x+1}=(x+1)^d.$$

Then, $v_x^2=x^{\frac{p^n+1}{2}}=\chi(x)x$ and $v_{x+1}^2=\chi(x+1)(x+1)$ since $2d\equiv\frac{p^n+1}{2} \pmod{p^n-1}$, where $\chi(x)=x^{\frac{p^n-1}{2}}$ is the quadratic character of $x\in\mathbb{F}_{p^n}$ [7]. Note that the expression $v_x^2=\chi(x)x$ implies that x is uniquely determined by v_x and $\chi(x)$.

Lemma 1 *With the notation introduced above, let $v_x=x^d$ and $v_{x+1}=(x+1)^d$. When $x\notin\{0,-1\}$, for each $b\neq0$, the differential equation (3) is equivalent to the following equation system*

$$\begin{cases}\left(\chi(x+1)\chi(x)-1\right)v_x^2-2bv_x+\chi(x+1)-b^2=0,\\ \chi(v_x+b)=1.\end{cases}\tag{4}$$

Proof: If $x\in\mathbb{F}_{p^n}\setminus\{0,-1\}$ satisfies (3), then we have

$$v_{x+1}=v_x+b.\tag{5}$$

Squaring both sides of (5) yields

$$v_{x+1}^2=v_x^2+2bv_x+b^2.\tag{6}$$

Substituting $v_x^2=\chi(x)x$ and $v_{x+1}^2=\chi(x+1)(x+1)$ into the above equation, we have

$$(\chi(x+1)-\chi(x))x+\chi(x+1)-b^2-2bv_x=0,\tag{7}$$

which can be rewritten as

$$\left(\chi(x+1)\chi(x)-1\right)\chi(x)x+\chi(x+1)-b^2-2bv_x=0.\tag{8}$$

Furthermore, substituting $x=\chi(x)v_x^2$ into (8), we get the first equation of (4). The second equation $\chi(v_x+b)=1$ is obvious due to (5) and $v_{x+1}=(x+1)^d$.

Conversely, let $x\in\mathbb{F}_{p^n}\setminus\{0,-1\}$ be a solution of (4). Reversing the process from (6) to (8), we can deduce that

$$-v_{x+1}=v_x+b \text{ or } v_{x+1}=v_x+b.$$

If v_x+b is square, then x will satisfy the differential equation $v_{x+1}=v_x+b$ since -1 is a nonsquare and v_{x+1} is a square. □

Given $b\neq0$, the differential equation $D_1F(x)=b$ is transformed to the equation system (4), where the first equation can be regarded as a quadratic equation in variable v_x. We have the following method of finding its solutions in $\mathbb{F}_{p^n}\setminus\{0,-1\}$:

- *Step 1:* Pose a restriction on $(\chi(x), \chi(x+1))$, which ranges over the set

$$\{(1,1),\ (1,-1),\ (-1,1),\ (-1,-1)\};$$

- *Step 2:* For each given $(\chi(x), \chi(x+1)) = (\epsilon_1, \epsilon_2)$, solve the first equation in (4) in variable v_x, where $\epsilon_i \in \{\pm 1\}$, $i = 1, 2$;

- *Step 3:* If the solution v_x satisfies

$$\chi(v_x) = 1 \text{ and } \chi(v_x + b) = 1, \tag{9}$$

then $x = v_x^2\chi(x) = v_x^2\epsilon_1$ is a solution of (4).

- *Step 4:* Repeat the steps 2 and 3 until (ϵ_1, ϵ_2) takes all possible values. Collecting all the x's obtained in the Step 3, we get the solutions of (4) in $\mathbb{F}_{p^n} \setminus \{0, -1\}$.

To validate the above method, we need to verify that each x obtained in Step 3 must be a solution to the equation (4). More precisely, we need to show that for each given (ϵ_1, ϵ_2), the x obtained in Step 3 (if it exists) satisfies $\chi(x) = \epsilon_1$, $\chi(x+1) = \epsilon_2$ and $x^d = v_x$ (here v_x is the solution of the quadratic equation $(\epsilon_2\epsilon_1 - 1)v_x^2 - 2bv_x + \epsilon_2 - b^2 = 0$ for each given (ϵ_1, ϵ_2)). It is obvious that the x satisfies $\chi(x) = \epsilon_1$ since $x = v_x^2\epsilon_1$. Furthermore, by $v_x^2 = x\epsilon_1$, we get $x^d\epsilon_1^d = x^d = v_x^{2d} = \chi(v_x)v_x$. With the condition $\chi(v_x) = 1$, we can conclude that the x obtained in Step 3 satisfies $v_x = x^d$. Next we verify that satisfies $\chi(x+1) = \epsilon_2$. Note that

$$(\epsilon_2\epsilon_1 - 1)v_x^2 - 2bv_x + \epsilon_2 - b^2 = \epsilon_2(v_x^2\epsilon_1 + 1) - (v_x + b)^2 = 0,$$

which implies

$$\epsilon_2(v_x^2\epsilon_1 + 1) = (v_x + b)^2.$$

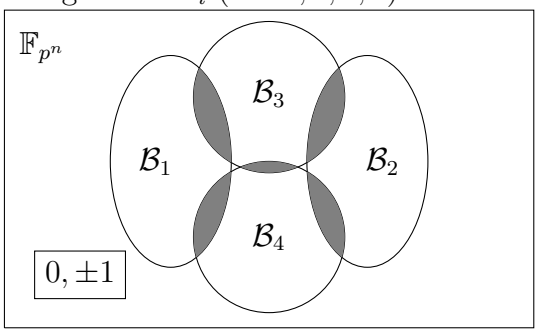
Then, it follows that $\chi\left(\epsilon_2(v_x^2\epsilon_1 + 1)\right) = 1$. Since $x = v_x^2\epsilon_1$, we have $\chi(x+1) = \epsilon_2$. Due to the condition $\chi(v_x + b) = 1$ in (9), the obtained x also satisfies the second equation of (4). Therefore, the method described above is valid, and according to Lemma 1, it provides an efficient approach to deal with the differential equation $\mathbb{D}_1F(x) = b$ in (3).

For the sake of brevity, we introduce the following sets

$$\begin{cases} \mathcal{B}_1 := \{b \in \mathbb{F}_{p^n}^* \mid \chi\left(\frac{1-b^2}{2b}\right) = \chi\left(\frac{1+b^2}{2b}\right) = 1\}, \\ \mathcal{B}_2 := \{b \in \mathbb{F}_{p^n}^* \mid \chi\left(\frac{-1-b^2}{2b}\right) = \chi\left(\frac{-1+b^2}{2b}\right) = 1\}, \\ \mathcal{B}_3 := \{b \in \mathbb{F}_{p^n}^* \mid \chi\left(\frac{-1-b^2}{2}\right) = \chi(-2-b^2) = 1\}, \\ \mathcal{B}_4 := \{b \in \mathbb{F}_{p^n}^* \mid \chi\left(\frac{1-b^2}{2}\right) = \chi(2-b^2) = 1\}, \end{cases} \tag{10}$$

where $p^n > 3$. Generally, these sets have the following relations as illustrated in Figure 1:
(i) $\{0, \pm 1\} \cap \cup_{i=1}^4 \mathcal{B}_i = \emptyset$;
(ii) $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$;

Figure 1: Diagram of $\mathcal{B}_i$ $(i = 1, 2, 3, 4)$ and their relations



(iii) $\mathcal{B}_i \cap \mathcal{B}_3 \cap \mathcal{B}_4 = \emptyset$, $i = 1, 2$.

It is easy to verify the properties (i) and (ii). The reason for the property (iii) is given as follows. For $b \in \mathcal{B}_1 \cup \mathcal{B}_2$, we have

$$\chi\left(\frac{1-b^2}{2b}\right)\chi\left(\frac{1+b^2}{2b}\right) = \chi\left(\frac{1-b^2}{2}\right)\chi\left(\frac{1+b^2}{2}\right) = 1,$$

while for $b \in \mathcal{B}_3 \cap \mathcal{B}_4$, we have

$$\chi\left(\frac{1-b^2}{2}\right)\chi\left(\frac{1+b^2}{2}\right) = -1.$$

Thus, the intersection is empty.

Set

$$\begin{cases} \mathcal{C}_1 := \{x \in \mathbb{F}_{p^n}^* \mid (\chi(x), \chi(x+1)) = (1, 1)\}, \\ \mathcal{C}_2 := \{x \in \mathbb{F}_{p^n}^* \mid (\chi(x), \chi(x+1)) = (-1, -1)\}, \\ \mathcal{C}_3 := \{x \in \mathbb{F}_{p^n}^* \mid (\chi(x), \chi(x+1)) = (1, -1)\}, \\ \mathcal{C}_4 := \{x \in \mathbb{F}_{p^n}^* \mid (\chi(x), \chi(x+1)) = (-1, 1)\}. \end{cases}$$

Then, $\mathcal{C}_i$, $i = 1, 2, 3, 4$, are pairwise disjoint and $\cup_{i=1}^4 \mathcal{C}_i = \mathbb{F}_{p^n} \setminus \{0, -1\}$. With these preparations, we give the following proposition.

Proposition 1 *With the notation introduced above, let d be the positive integer defined in (2) with $p^n > 3$, and $F(x) = x^d$ be the power mapping over $\mathbb{F}_{p^n}$. Then, when $b \neq 0$, the differential equation $(x+1)^d - x^d = b$ has at most one solution in $\mathcal{C}_i$, and it has exactly one solution in $\mathcal{C}_i$ if and only if $b \in \mathcal{B}_i$, $i = 1, 2, 3, 4$.*

Proof: By Lemma 1, for each $b \neq 0$, we only need to consider the number of solutions of (4) in $\mathbb{F}_{p^n} \setminus \{0, -1\}$. We distinguish four cases.

Case 1: $x \in \mathcal{C}_1$, i.e., $(\chi(x), \chi(x+1)) = (1, 1)$. Then (4) becomes

$$\begin{cases} v_x = \frac{1-b^2}{2b}, \\ \chi\left(\frac{1+b^2}{2b}\right) = 1. \end{cases}$$

According to (9), this case contributes one solution if and only if $b \in \mathcal{B}_1$.

Case 2: $x \in \mathcal{C}_2$, i.e., $(\chi(x), \chi(x+1)) = (-1, -1)$. In this case, (4) can be rewritten as

$$\begin{cases} v_x = \frac{-1-b^2}{2b}, \\ \chi\left(\frac{-1+b^2}{2b}\right) = 1. \end{cases}$$

Similarly, this case contributes one solution if and only if $b \in \mathcal{B}_2$.

Case 3: $x \in \mathcal{C}_3$, i.e., $(\chi(x), \chi(x+1)) = (1, -1)$. In this case, (4) becomes

$$\begin{cases} v_x^2 + bv_x + \frac{1+b^2}{2} = 0, \\ \chi(v_x + b) = 1. \end{cases} \tag{11}$$

The first equation in (11) is a quadratic equation in variable v_x and its discriminant is equal to $-2 - b^2$. If $\chi(-2 - b^2) = 1$, (11) is equivalent to the following two equation systems:

$$\begin{cases} v_{x_1} = \frac{-b+\sqrt{-2-b^2}}{2}, \\ \chi(v_{x_1} + b) = \chi\left(\frac{b+\sqrt{-2-b^2}}{2}\right) = 1, \end{cases} \tag{12}$$

or

$$\begin{cases} v_{x_2} = \frac{-b-\sqrt{-2-b^2}}{2}, \\ \chi(v_{x_2} + b) = \chi\left(\frac{b-\sqrt{-2-b^2}}{2}\right) = 1. \end{cases} \tag{13}$$

Note that $v_{x_i}(v_{x_i}+b) = \frac{-1-b^2}{2}$, $i = 1, 2$. To make sure (12) or (13) contributes one solution to (4), it is necessary to have $\chi\left(\frac{-1-b^2}{2}\right) = 1$, which further implies that $\chi(v_{x_1}v_{x_2}) = \chi\left(\frac{1+b^2}{2}\right) = -1$. So one and only one of v_{x_1} and v_{x_2} is square. Therefore, we can conclude that when $b \in \mathcal{B}_3$, one and only one of (12) and (13) contributes one solution to (4).

Note that if $-2 - b^2 = 0$, the first equation in (4) has only one solution v_x, and this solution satisfies $v_x(v_x + b) = \frac{-b^2}{4}$, which is a nonsquare. Thus, the condition in (9) does not hold. So (4) has no solution in this case.

The above discussions show that when $x \in \mathcal{C}_3$, (4) has at most one solution, and it has exactly one solution if and only if $b \in \mathcal{B}_3$.

Case 4: $x \in \mathcal{C}_4$, i.e., $(\chi(x), \chi(x+1)) = (-1, 1)$. In this case, (4) becomes

$$\begin{cases} v_x^2 + bv_x + \frac{-1+b^2}{2} = 0, \\ \chi(v_x + b) = 1. \end{cases} \tag{14}$$

The first equation in (14) is also a quadratic equation in variable v_x and the discriminant is equal to $2 - b^2$. If $\chi(2 - b^2) = 1$, it has two solutions, denoted by $v_{x_1} = \frac{-b+\sqrt{2-b^2}}{2}$ and $v_{x_2} = \frac{-b-\sqrt{2-b^2}}{2}$, which satisfy $v_{x_i}(v_{x_i} + b) = \frac{1-b^2}{2}$, $i = 1, 2$. To make sure that (14) can have solutions, it is necessary to have $\chi\left(\frac{1-b^2}{2}\right) = 1$, which leads to that $\chi\left(\frac{-1+b^2}{2}\right) = \chi(v_{x_1}v_{x_2}) = -1$. This means that one and only one of v_{x_1} and v_{x_2} is square. Therefore,

when $b \in \mathcal{B}_4$, (14) can contribute one and only one solution to (4). Moreover, if $2-b^2=0$, we have $v_x(v_x+b) = \frac{-b^2}{4}$, which is a nonsquare. Due to (9), we know that under this condition (14) has no solution. Therefore, we can conclude that this case can contribute exactly one solution if and only if $b \in \mathcal{B}_4$.

Based on the results obtained in Cases 1-4, we get the the desired result. □

According to Proposition 1 and its proof, we can characterize the conditions on b for which the differential equation $(x+1)^d - x^d = b$ has no solution, exactly one solution and two solutions, respectively.

Proposition 2 *With the same notation as in Proposition 1, for each $b \in \mathbb{F}_{p^n}$, let $p^n > 3$ and $N(b)$ denote the number of solutions $x \in \mathbb{F}_{p^n}$ to the differential equation $\mathbb{D}_1 F(x) = (x+1)^d - x^d = b$. Then,*

$$N(b) = \begin{cases} 0, & \text{if } b \in \mathbb{F}_{p^n} \setminus (\{0, \pm 1\} \cup \mathcal{B}), \\ 1, & \text{if } b \in \{0, \pm 1\} \cup \mathcal{B} \setminus \widetilde{\mathcal{B}}, \\ 2, & \text{if } b \in \widetilde{\mathcal{B}}, \end{cases} \tag{15}$$

where $\mathcal{B} = \cup_{i=1}^4 \mathcal{B}_i$, and $\widetilde{\mathcal{B}} = (\mathcal{B}_1 \cap \mathcal{B}_3) \cup (\mathcal{B}_1 \cap \mathcal{B}_4) \cup (\mathcal{B}_2 \cap \mathcal{B}_3) \cup (\mathcal{B}_2 \cap \mathcal{B}_4) \cup (\mathcal{B}_3 \cap \mathcal{B}_4)$, which corresponds to the gray areas shown in Figure 1.

Proof: Recall that $x=0$ (resp. $x=-1$) is a solution of $\mathbb{D}_1 F(x) = 1$ (resp. $\mathbb{D}_1 F(x) = -1$). Due to Proposition 1 and the fact $\pm 1 \notin \mathcal{B}$, we know that for each $b \in \{\pm 1\}$, the differential equation $\mathbb{D}_1 F(x) = b$ has no solution in $\cup_{i=1}^4 \mathcal{C}_i = \mathbb{F}_{p^n} \setminus \{0, -1\}$ and thus $N(\pm 1) = 1$. Together with the fact $N(0) = 1$, we have $N(b) = 1$ for $b \in \{0, \pm 1\}$. On the other hand, for each $b \notin \{\pm 1\}$, the differential equation $\mathbb{D}_1 F(x) = b$ has no solution in $\{0, -1\}$ and its solutions in $\mathbb{F}_{p^n}$ are exactly those in $\mathbb{F}_{p^n} \setminus \{0, -1\}$. Thus, according to Proposition 1, we conclude that $N(b) \geq 1$ if $b \in \mathcal{B}$, and $N(b) = 0$ if $b \notin \{0, \pm 1\} \cup \mathcal{B}$.

Furthermore, note that the properties (ii) and (iii) about the sets $\mathcal{B}_i$ $(i = 1, 2, 3, 4)$ imply that the differential equation cannot have solutions in $\mathcal{C}_1$ and $\mathcal{C}_2$ simultaneously, and cannot have solutions simultaneously in any three sets of $\mathcal{C}_i$, $i = 1, 2, 3, 4$, either. Thus, for each $b \in \mathcal{B}$, $N(b) \leq 2$. Moreover, according to Proposition 1 and its proof, $N(b) = 2$ if and only if b belongs to the intersection of any two sets of $\mathcal{B}_i$, $i = 1, 2, 3, 4$. Thus $N(b) = 2$ if and only if $b \in \widetilde{\mathcal{B}}$. Removing the elements in $\widetilde{\mathcal{B}}$ from the set $\mathcal{B}$ and adding the elements of $\{0, \pm 1\}$, we can get the elements b such that $N(b) = 1$. The relationships between the sets mentioned above can be easily observed with the help of Figure 1. □

Proposition 2 has characterized the sets of elements b for $N(b) = 0$, 1 and 2 , respectively. Next we need to calculate the cardinalities of the sets in Proposition 2, thereby determining the differential spectrum of $F(x) = x^d$. The sets $\mathcal{B}_i$, $i = 1, 2, 3, 4$, are defined in terms of quadratic characters. Hence we use quadratic character sums to calculate the cardinalities of the sets in (15) in Propositions 2. Many quadratic character sums involved can be reduced to a simpler form in the case $p = 3$. Thus, we deal with the cases $p > 3$ and $p = 3$ separately. We first consider the case $p > 3$.

When $p > 3$, for simplicity, we will express the relevant quadratic character sums in terms of the following three quadratic character sums:

$$\Gamma_{p,n}^{(1)} = \sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x-1)(x-3)\right), \tag{16}$$

$$\Gamma_{p,n}^{(2)} = \sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x-1)(x+2)\right), \tag{17}$$

and

$$\Gamma_{p,n}^{(3)} = \sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x-1)(x+3)\right). \tag{18}$$

These three quadratic character sums can be evaluated by the theory of elliptic curves, and the details have been described in [9] and [10]. The following two lemmas evaluate the quadratic character sums derived from Propositions 2, some of which are expressed in terms of $\Gamma_{p,n}^{(i)}$, $i = 1, 2, 3$.

Lemma 2 *Let $p > 3$, and $p^n \equiv 3 \pmod 8$ or $p^n \equiv 7 \pmod 8$. Then, we have 24 identities in Table 1, where $\Gamma_{p,n}^{(1)}$, $\Gamma_{p,n}^{(2)}$ and $\Gamma_{p,n}^{(3)}$ are defined in* (16), (17) and (18), respectively.

Table 1: Some identities about quadratic character sums

1)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x^2-1)\right) = 0$	2)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x^2+1)\right) = 0$
3)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(1-2x)(2-2x)\right) = 0$	4)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(1+x)(2-2x)\right) = 0$
5)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x+1)(x-1)(x+3)(3x+1)\right) = 0$	6)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(2x+1)(2x-2)\right) = \chi(2)\Gamma_{p,n}^{(1)}$
7)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x+1)(3x+1)\right) = \Gamma_{p,n}^{(2)}$	8)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(2x-2)(6x-2)\right) = -\Gamma_{p,n}^{(2)}$
9)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(2x-2)(6-2x)\right) = \Gamma_{p,n}^{(2)}$	10)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x-1)(3x+1)\right) = -\Gamma_{p,n}^{(3)}$
11)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x+1)(6x-2)\right) = \chi(2)\Gamma_{p,n}^{(3)}$	12)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x+1)(6-2x)\right) = \chi(2)\Gamma_{p,n}^{(3)}$
13)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(3x+1)(x+3)\right) = -\Gamma_{p,n}^{(3)}$	14)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+2x^2)\right) = 1$
15)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+x^2)\right) = \chi(2) + \chi(2)\Gamma_{p,n}^{(1)}$	16)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2-x^2)\right) = -\chi(2)$
17)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2+2x^2)(2-x^2)\right) = \chi(2) - \chi(2)\Gamma_{p,n}^{(1)}$	18)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2+2x^2)(2+x^2)\right) = -\chi(2)$
19)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-x^2)(2+x^2)\right) = 1$	20)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+2x^2)(2+x^2)\right) = 1 + \Gamma_{p,n}^{(2)} - \Gamma_{p,n}^{(3)}$
21)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+2x^2)(2-x^2)\right) = -1 + \Gamma_{p,n}^{(2)} + \Gamma_{p,n}^{(3)}$	22)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-x^2)(2+x^2)(2+2x^2)\right) = \chi(2) + \chi(2)\Gamma_{p,n}^{(3)} - \Gamma_{p,n}^{(2)}$
23)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-x^2)(2+x^2)(2-2x^2)\right) = -\chi(2) + \chi(2)\Gamma_{p,n}^{(3)} + \Gamma_{p,n}^{(2)}$	24)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+2x^2)(2+x^2)(2-x^2)\right) = -1 - \Gamma_{p,n}^{(3)}$

Proof: See Appendix A. □

The conditions that $p^n \equiv 3 \pmod 8$ or $p^n \equiv 7 \pmod 8$ are equivalent to n being odd and $p \equiv 3 \pmod 8$ or $p \equiv 7 \pmod 8$. Note that the element 2 is a nonsquare in $\mathbb{F}_p$ if $p \equiv 3 \pmod 8$ and a square in $\mathbb{F}_p$ if $p \equiv 7 \pmod 8$, and -1 is a nonsquare when $p^n \equiv 3 \pmod 4$. Therefore, the element 2 is a square in $\mathbb{F}_{p^n}$ if $p^n \equiv 7 \pmod 8$, and a nonsquare if $p^n \equiv 3 \pmod 8$; -2 is a nonsquare in $\mathbb{F}_{p^n}$ if $p^n \equiv 7 \pmod 8$, and a square if $p^n \equiv 3 \pmod 8$. In order to present our main results, we need to define the following three sets

$$\mathcal{A}_1 = \begin{cases} \{\pm 1, \pm\sqrt{-2}\}, & \text{if } p^n \equiv 3 \pmod 8, \\ \{\pm 1\}, & \text{if } p^n \equiv 7 \pmod 8, \end{cases} \tag{19}$$

$$\mathcal{A}_2 = \begin{cases} \{\pm 1\}, & \text{if } p^n \equiv 3 \pmod 8, \\ \{\pm 1, \pm\sqrt{2}\}, & \text{if } p^n \equiv 7 \pmod 8, \end{cases} \tag{20}$$

and

$$\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2. \tag{21}$$

Lemma 3 *With the notation introduced above, let $p > 3$, and $p^n \equiv 3 \pmod 8$ or $p^n \equiv 7 \pmod 8$, then we have*

$$\sum_{x \in \mathbb{F}_{p^n} \setminus \mathcal{A}_1} \big((1-\chi(2-2x^2))(1-\chi(2+2x^2))(1-\chi(2+x^2))\big) = p^n+1+\chi(2)\Gamma_{p,n}^{(1)}-\Gamma_{p,n}^{(2)}+\Gamma_{p,n}^{(3)},$$

$$\sum_{x \in \mathbb{F}_{p^n} \setminus \mathcal{A}_2} \big((1+\chi(2-2x^2))(1+\chi(2+2x^2))(1+\chi(2-x^2))\big) = p^n-7-\chi(2)\Gamma_{p,n}^{(1)}+\Gamma_{p,n}^{(2)}+\Gamma_{p,n}^{(3)},$$

and

$$\sum_{x \in \mathbb{F}_{p^n} \setminus \mathcal{A}} \big((1+\chi(2-2x^2))(1-\chi(2+2x^2))(1+\chi(2-x^2))(1-\chi(2+x^2))\big) = p^n+1-2\Gamma_{p,n}^{(2)}-3\Gamma_{p,n}^{(3)},$$

where $\Gamma_{p,n}^{(1)}$, $\Gamma_{p,n}^{(2)}$ and $\Gamma_{p,n}^{(3)}$ are defined in (16), (17) and (18), respectively.

Proof: See Appendix B. □

Keeping the notation introduced above, we have the following main theorem.

Theorem 1 *Let d be defined in (2) and $F(x) = x^d$ be the power mapping over $\mathbb{F}_{p^n}$. When $p > 3$ and $p^n > 7$, the differential spectrum of $F(x) = x^d$ is given by*

$$[\,\omega_0, \omega_1, \omega_2\,] = [\,\frac{5p^n-27-2\Gamma_{p,n}^{(2)}+\Gamma_{p,n}^{(3)}}{16}, \frac{3p^n+27+2\Gamma_{p,n}^{(2)}-\Gamma_{p,n}^{(3)}}{8}, \frac{5p^n-27-2\Gamma_{p,n}^{(2)}+\Gamma_{p,n}^{(3)}}{16}\,],$$

where $\Gamma_{p,n}^{(2)}$ and $\Gamma_{p,n}^{(3)}$ are given in (17) and (18).

Proof: Determining the differential spectrum of $F(x) = x^d$ requires calculating the cardinalities of the sets in (15). We start with calculating the cardinality of $\widetilde{\mathcal{B}}$, which is exactly the component ω_2 in the differential spectrum of $F(x)$. According to (10), we have

$$\begin{aligned}
|\mathcal{B}_1 \cap \mathcal{B}_3| &= |\{b \in \mathbb{F}_{p^n}^* \mid \chi\left(\tfrac{1-b^2}{2b}\right) = 1, \chi\left(\tfrac{1+b^2}{2b}\right) = 1, \chi\left(\tfrac{-1-b^2}{2}\right) = 1, \chi(-2-b^2) = 1\}| \\
&= |\{b \in \mathbb{F}_{p^n}^* \mid \chi(2-2b^2) = -1, \chi(2+2b^2) = -1, \chi(2+b^2) = -1, \chi(b) = -1\}|, \\
|\mathcal{B}_1 \cap \mathcal{B}_4| &= |\{b \in \mathbb{F}_{p^n}^* \mid \chi(2-2b^2) = 1, \chi(2+2b^2) = 1, \chi(2-b^2) = 1, \chi(b) = 1\}|, \\
|\mathcal{B}_2 \cap \mathcal{B}_3| &= |\{b \in \mathbb{F}_{p^n}^* \mid \chi(2-2b^2) = -1, \chi(2+2b^2) = -1, \chi(2+b^2) = -1, \chi(b) = 1\}|, \\
|\mathcal{B}_2 \cap \mathcal{B}_4| &= |\{b \in \mathbb{F}_{p^n}^* \mid \chi(2-2b^2) = 1, \chi(2+2b^2) = 1, \chi(2-b^2) = 1, \chi(b) = -1\}|,
\end{aligned}$$

and

$$|\mathcal{B}_3 \cap \mathcal{B}_4| = |\{b \in \mathbb{F}_{p^n}^* \mid \chi(2-2b^2)=1,\, \chi(2+2b^2)=-1,\, \chi(2-b^2)=1,\, \chi(2+b^2)=-1\}|.$$

Note that the sets $\mathcal{B}_1 \cap \mathcal{B}_3$, $\mathcal{B}_1 \cap \mathcal{B}_4$, $\mathcal{B}_2 \cap \mathcal{B}_3$, $\mathcal{B}_2 \cap \mathcal{B}_4$ and $\mathcal{B}_3 \cap \mathcal{B}_4$ are pairwise disjoint, see Figure 1. Denote the cardinality of $\mathcal{B}_i \cap \mathcal{B}_j$ by $N_{i,j}$, where $i \neq j$. It can be seen that $N_{1,3} = N_{2,3}$ since $b \in \mathcal{B}_1 \cap \mathcal{B}_3$ if and only if $-b \in \mathcal{B}_2 \cap \mathcal{B}_3$. Similarly, $N_{1,4} = N_{2,4}$ since $b \in \mathcal{B}_1 \cap \mathcal{B}_4$ if and only if $-b \in \mathcal{B}_2 \cap \mathcal{B}_4$. Moreover, we have

$$\begin{aligned}
8(N_{1,3}+N_{2,3}) &= \sum_{x \in \mathbb{F}_{p^n}^* \setminus \mathcal{A}_1} \left((1-\chi(2-2x^2))(1-\chi(2+2x^2))(1-\chi(2+x^2))\right), \\
8(N_{1,4}+N_{2,4}) &= \sum_{x \in \mathbb{F}_{p^n}^* \setminus \mathcal{A}_2} \left((1+\chi(2-2x^2))(1+\chi(2+2x^2))(1+\chi(2-x^2))\right),
\end{aligned}$$

and

$$16N_{3,4} = \sum_{x \in \mathbb{F}_{p^n}^* \setminus \mathcal{A}} \left((1+\chi(2-2x^2))(1-\chi(2+2x^2))(1+\chi(2-x^2))(1-\chi(2+x^2))\right),$$

where $\mathcal{A}_1$, $\mathcal{A}_2$ and $\mathcal{A}$ being defined in (19), (20) and (21), respectively. By Lemma 3, we obtain

$$\begin{aligned}
N_{1,3}+N_{2,3} &= \frac{p^n+1+\chi(2)\Gamma_{p,n}^{(1)}-\Gamma_{p,n}^{(2)}+\Gamma_{p,n}^{(3)}-(1-\chi(2))^3}{8}, \\
N_{1,4}+N_{2,4} &= \frac{p^n-7-\chi(2)\Gamma_{p,n}^{(1)}+\Gamma_{p,n}^{(2)}+\Gamma_{p,n}^{(3)}-(1+\chi(2))^3}{8}, \\
N_{3,4} &= \frac{p^n+1-2\Gamma_{p,n}^{(2)}-3\Gamma_{p,n}^{(3)}}{16}.
\end{aligned}$$

Then we obtain

$$\omega_2 = |\widetilde{\mathcal{B}}| = N_{1,3}+N_{1,4}+N_{2,3}+N_{2,4}+N_{3,4} = \frac{5p^n-27-2\Gamma_{p,n}^{(2)}+\Gamma_{p,n}^{(3)}}{16}. \tag{22}$$

Next we determine the component ω_1 in the differential spectrum of $F(x)$. Based on the properties of $\mathcal{B}_i$, $i=1,2,3,4$, which are illustrated in Figure 1, we have

$$|\{0,\pm 1\} \cup \mathcal{B} \setminus \widetilde{\mathcal{B}}| = 3 + \sum_{i=1}^{4} |\mathcal{B}_i| - 2|\widetilde{\mathcal{B}}|. \tag{23}$$

According to the definition of $\mathcal{B}_i$ in (10), $i=1,2,3,4$, we can calculate their cardinalities as follows.

$$\begin{aligned}
4|\mathcal{B}_1| &= \sum_{x \in \mathbb{F}_{p^n} \setminus \{0,\pm 1\}} \left(1+\chi(2x(1+x^2))\right)\left(1+\chi(2x(1-x^2))\right) \\
&= p^n - 4 + \sum_{x \in \mathbb{F}_{p^n}} \chi(2x(1+x^2)) + \sum_{x \in \mathbb{F}_{p^n}} \chi(2x(1-x^2)) + \sum_{x \in \mathbb{F}_{p^n}} \chi\left((1-x^2)(1+x^2)\right) \\
&= p^n - 3,
\end{aligned}$$

where we use the identities 1), 2) and 14) in Table 1. Similarly, we have

$$\begin{aligned}4|\mathcal{B}_2| &= \sum_{x\in\mathbb{F}_{p^n}\setminus\{0,\pm1\}} \big(1-\chi(2x(1+x^2))\big)\big(1-\chi(2x(1-x^2))\big)\\ &= p^n-3.\end{aligned}$$

Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be the sets defined in (19) and (20), respectively. Then

$$\begin{aligned}4|\mathcal{B}_3| &= \sum_{\mathbb{F}_{p^n}^*\setminus\mathcal{A}_1} \big((1-\chi(2+2x^2)\big)\big(1-\chi(2+x^2)\big)\\ &= \sum_{x\in\mathbb{F}_{p^n}} \big(1-\chi(2+2x^2)\big)\big(1-\chi(2+x^2)\big)-(1-\chi(2))^2\\ &= p^n+\chi(2)+1+\sum_{x\in\mathbb{F}_{p^n}}\chi\big((2+2x^2)(2+x^2)\big)-(1-\chi(2))^2\\ &= p^n+1-(1-\chi(2))^2,\end{aligned}$$

where we use the identity 18) in Table 1. Similarly,

$$\begin{aligned}4|\mathcal{B}_4| &= \sum_{x\in\Omega_1=\mathbb{F}_{p^n}^*\setminus\mathcal{A}_2} \big((1+\chi(2-2x^2))(1+\chi(2-x^2))\big)\\ &= \sum_{x\in\mathbb{F}_{p^n}} \big((1+\chi(2-2x^2))(1+\chi(2-x^2))\big)-(1+\chi(2))^2-4\\ &= p^n-3-(1+\chi(2))^2.\end{aligned}$$

Therefore, we get

$$\sum_{i=1}^{4}|\mathcal{B}_i| = p^n-3. \tag{24}$$

Substituting (24) and (22) into (23), we obtain

$$\omega_1 = \frac{3p^n+27+2\Gamma_{p,n}^{(2)}-\Gamma_{p,n}^{(3)}}{8}.$$

Finally, we determine the component ω_0 in the differential spectrum of $F(x)$. According to (15), (24) and (22), we get

$$\omega_0 = p^n-3-|\mathcal{B}| = p^n-3-\sum_{i=1}^{4}|\mathcal{B}_i|+|\widetilde{\mathcal{B}}| = \frac{5p^n-27-2\Gamma_{p,n}^{(2)}+\Gamma_{p,n}^{(3)}}{16}.$$

The proof is finished. □

Remark 1 *After we determined the component ω_2 in (22), we actually can utilize the identities (1) to derive ω_1 and ω_0. Here we don't use these identities since we want to give a direct calculation via determining the sizes of the corresponding sets. The reason*

why we can do this lies in that we successfully characterize the conditions on b under which the differential equation $\mathbb{D}_1F(x) = b$ has exactly i solution(s) in $\mathbb{F}_{p^n}$, $i = 0, 1, 2$. This characterization reveals more essential information about the differential equation $\mathbb{D}_1F(x) = b$ and can be used to describe the form of the DDT of $F(x) = x^d$.

Remark 2 *When the power function $F(x) = x^d$ in this theorem is APN, we must have $\omega_2 = \frac{5p^n-27-2\Gamma^{(2)}_{p,n}+\Gamma^{(3)}_{p,n}}{16} > 0$. According to the Weil bound in [7, Theorem 5.41], when $p > 3$ we have $-2\sqrt{p^n} \le \Gamma^{(2)}_{p,n}, \Gamma^{(3)}_{p,n} \le 2\sqrt{p^n}$. Thus,*

$$5p^n - 27 - 2\Gamma^{(2)}_{p,n} + \Gamma^{(3)}_{p,n} \ge 5p^n - 6\sqrt{p^n} - 27.$$

To make sure $\omega_2 > 0$, it suffices that $5p^n - 6\sqrt{p^n} - 27 > 0$, which implies $p^n > 9$. When p is odd and n is odd, $p^n > 9$ is equivalent to that $p^n > 7$. This explains again why we need the condition $p^n > 7$ when x^d is APN.

Remark 3 *When $p^n = 7$, by Magma, we get $\Gamma^{(2)}_{p,n} = 4$ and $\Gamma^{(3)}_{p,n} = 0$. Using the the formulas in Theorem 1, we get $\omega_2 = 0$, $\omega_1 = 7$ and $\omega_0 = 0$, which coincides with the fact that x^d is the PN function x^2 when $p^n = 7$. This shows that the formulas of the differential spectrum in this theorem also hold for $p^n = 7$.*

Remark 4 *Note that*

$$\Gamma^{(2)}_{p,n} = \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-x(-x-1)(-x+2)\right) = -\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x+1)(x-2)\right)$$

and

$$\Gamma^{(3)}_{p,n} = \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-x(-x-1)(-x+3)\right) = -\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x+1)(x-3)\right).$$

Therefore, Theorem 1 agrees with Theorem 3 in [10].

Next we give the differential spectrum of $F(x) = x^d$ in the case $p = 3$.

Theorem 2 *Let $p = 3$, $n \ge 3$ and $F(x) = x^d$ be the power mapping over $\mathbb{F}_{p^n}$ with d being defined by (2). The differential spectrum of $F(x) = x^d$ is given by*

$$[\,\omega_0, \omega_1, \omega_2\,] = [\,\frac{p^n-3}{2},\, 3,\, \frac{p^n-3}{2}\,].$$

Proof: With the same notation in Proposition 2, when $p = 3$, besides the properties displayed in Figure 1, the sets $\mathcal{B}_i$, $i = 1, 2, 3, 4$, in (10) have more special properties as follows:
(a) when $\chi(b) = 1$, $\mathcal{B}_1 \cap \mathcal{B}_3 = \emptyset$, $\mathcal{B}_1 = \mathcal{B}_4$, $\mathcal{B}_2 = \mathcal{B}_3$, and $\mathcal{B}_2 \cap \mathcal{B}_4 = \emptyset$;
(b) when $\chi(b) = -1$, $\mathcal{B}_1 = \mathcal{B}_3$, $\mathcal{B}_1 \cap \mathcal{B}_4 = \emptyset$, $\mathcal{B}_2 \cap \mathcal{B}_3 = \emptyset$, and $\mathcal{B}_2 = \mathcal{B}_4$;
(c) $\mathcal{B}_3 \cap \mathcal{B}_4 = \emptyset$.
From the properties above, we know that

$$\widetilde{\mathcal{B}} = \mathcal{B}_1 \cup \mathcal{B}_2 \text{ and } \mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2.$$

Utilizing the the theory of quadratic character sums, we can get $|\mathcal{B}_1| = |\mathcal{B}_2| = \frac{3^n-3}{4}$. Then, according to Proposition 2, we get $\omega_2 = |\widetilde{\mathcal{B}}| = |\mathcal{B}_1| + |\mathcal{B}_2| = \frac{3^n-3}{2}$, $\omega_1 = |\{0, \pm 1\} \cup \mathcal{B} \backslash \widetilde{\mathcal{B}}| = 3$, and $\omega_0 = p^n - 3 - |\mathcal{B}| = \frac{3^n-3}{2}$. □

As a special case of Theorem 3 in [5], by taking $m = 1$ there, one gets the same result of Theorem 2.

3 Conclusion

In this paper, we study the differential spectrum of the APN function $F(x) = x^d$ over $\mathbb{F}_{p^n}$, where $p^n > 7$, $d = \frac{p^n+1}{4} + \frac{p^n-1}{2}$ if $p^n \equiv 3 \pmod 8$ and $d = \frac{p^n+1}{4}$ if $p^n \equiv 7 \pmod 8$. We first present an efficient algorithm to find the solutions of the differential equation $\mathbb{D}_1 F(x) = b$, and then characterize the conditions on b under which $\mathbb{D}_1 F(x) = b$ has exactly two solutions, one solution and no solution, respectively. We determine the cardinalities of the associated sets by the theory of elliptic curves, and thus obtain the differential spectrum of $F(x)$. Compared with the method in [10], we provide a direct method for computing the differential spectrum of $F(x)$. In addition, the obtained results about the differential equation $\mathbb{D}_1 F(x) = b$ can be used to describe the form of the DDT of $F(x)$. Thus, our method explores more information about the differential properties of this APN function. The idea used in this paper may be used to calculate the differential spectra of other power mappings over finite fields of odd characteristic.

Acknowledgment

The authors wish to thank Dr. Chunlei Li for his valuable discussions and suggestions. Y. Xia and F. Bao were supported in part by the National Natural Science Foundation of China under Grant 62171479, and in part by the Fundamental Research Funds for the Central Universities, South-Central University for Nationalities under Grant CZZ23004. S. Chen was supported in part by the National Natural Science Foundation of China under Grant 61971452 and in part by the Fund for Scientific Research Platforms of South-Central Minzu University under Grant PTZ24004. T. Helleseth is supported by the Research Council of Norway under Grant 311646.

References

[1] C. Blondeau, A. Canteaut, and P. Charpin, "Differential properties of power functions," *Int. J. Inf. Coding Theory*, vol. 1, no. 2, pp. 149-170, 2010.

[2] C. Blondeau, A. Canteaut, and P. Charpin, "Differential properties of $x \mapsto x^{2^t-1}$," *IEEE Trans. Inf. Theory*, vol. 57, no. 12, pp. 8127-8137, 2011.

[3] C. Blondeau and L. Perrin, "More differentially 6-uniform power functions," *Des. Codes Cryptogr.*, vol. 73, no. 2, pp. 487-505, 2014.

[4] C. Boura, A. Canteaut, J. Jean, and V. Suder, "Two notions of differential equivalence on Sboxes," *Des. Codes Cryptogr.*, vol. 87, no. 6, pp. 185-202, 2019.

[5] S. T. Choi, S. Hong, J. S. No, and H. Chung, "Differential spectrum of some power functions in odd prime characteristic," *Finite Fields Appl.*, vol. 21, pp. 11-29, 2013.

[6] T. Helleseth, C. Rong, and D. Sandberg, "New families of almost perfect nonlinear power mappings," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 475-485, 1999.

[7] R. Lidl and H. Niederreiter, *Finite Fields,* Encyclopedia of Mathematics and Its Applications, vol. 20. Cambridge U.K: Cambridge University Press, 1997.

[8] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in cryptology-EUROCRYPT'93, Lecture Notes in Computer Science*, vol. 765. Berlin, Germany: Springer-Verlag, 1994, pp. 55-64.

[9] H. Yan, Y. Xia, C. Li, T. Helleseth, M. Xiong, and J. Luo, "The differential spectrum of the power mapping x^{p^n-3}," *IEEE Trans. Inf. Theory*, vol. 68, no. 8, pp. 5535-5547, 2022.

[10] X. Tan and H. Yan. "Differential spectrum of a class of APN power functions," *Des. Codes Cryptogr.*, vol. 91, no. 8, pp. 2755-2768, 2023.

Appendix A

The Proof of Lemma 2: All these identities are required to calculates the sizes of the sets appeared in Proposition 2. The identities 3) to 13) will be used in the proofs of the identities 14) to 24). We only give the proof for identities 1), 13), 14) and 20) in Table 1. The other identities can be similarly proved.

Identity 1): Let $x = -u$, then we have

$$\sum_{x\in\mathbb{F}_{p^n}} \chi(x(x^2-1)) = \sum_{u\in\mathbb{F}_{p^n}} \chi(-u(u^2-1)) = \chi(-1)\sum_{u\in\mathbb{F}_{p^n}} \chi(u(u^2-1))$$

which implies that $\sum_{x\in\mathbb{F}_{p^n}} \chi(x(x^2-1)) = 0$ since $\chi(-1) = -1$.

Identity 13): Note that

$$\begin{aligned}\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(3x+1)(x+3)\right) &= \sum_{x\in\mathbb{F}_{p^n}} \chi\left(3x(3x+1)(3x+9)\right)\\ &= \sum_{u\in\mathbb{F}_{p^n}} \chi\left(u(u+1)(u+9)\right)\\ &= \sum_{u\in\mathbb{F}_{p^n}^*} \chi\left(\frac{(u+1)(u+9)}{u}\right).\end{aligned}$$

For $u \neq 0$, let

$$\frac{(u+1)(u+9)}{u} = v,$$

then each $v \in \mathbb{F}_{p^n}$ corresponds to $1 + \chi\left((v-4)(v-16)\right)$ u's. Thus, we obtain

$$\begin{aligned}\sum_{u \in \mathbb{F}_{p^n}^*} \chi\left(\frac{(u+1)(u+9)}{u}\right) &= \sum_{v \in \mathbb{F}_{p^n}} \chi(v)\left(1 + \chi((v-4)(v-16))\right) \\ &= \sum_{v \in \mathbb{F}_{p^n}} \chi\left(v(v-4)(v-16)\right) \\ &= \sum_{v \in \mathbb{F}_{p^n}} \chi\left(\frac{v}{4}(\frac{v}{4}-1)(\frac{v}{4}-4)\right).\end{aligned}$$

Furthermore, let $t = \frac{v}{4} - 1$ and $w = -t$, then

$$\begin{aligned}\sum_{u \in \mathbb{F}_{p^n}^*} \chi\left(\frac{(u+1)(u+9)}{u}\right) &= \sum_{v \in \mathbb{F}_{p^n}} \chi\left(\frac{v}{4}(\frac{v}{4}-1)(\frac{v}{4}-4)\right) \\ &= \sum_{t \in \mathbb{F}_{p^n}} \chi\left(t(t+1)(t-3)\right) \\ &= \sum_{w \in \mathbb{F}_{p^n}} \chi\left(w(1-w)(w+3)\right) \\ &= -\Gamma_{p,n}^{(3)}.\end{aligned}$$

Identity 14): Note that

$$\begin{aligned}\sum_{x \in \mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+2x^2)\right) &= \sum_{x \in \mathbb{F}_{p^n}} \chi\left((1-x^2)(1+x^2)\right) \\ &= \sum_{x \in \mathbb{F}_{p^n} \setminus \{\pm 1\}} \chi\left(\frac{1+x^2}{1-x^2}\right).\end{aligned}$$

Let $\frac{1+x^2}{1-x^2} = u$, then x and u satisfy

$$(u+1)x^2 + 1 - u = 0. \tag{25}$$

When $u \neq -1$, (25) is a quadratic equation in variable x, and its discriminant is $\Delta = 4(u+1)(u-1)$. For each $u \neq -1$, it corresponds to $(1 + \chi(\Delta))$ x's via (25). Thus, we obtain

$$\begin{aligned}\sum_{x \in \mathbb{F}_{p^n} \setminus \{\pm 1\}} \chi\left(\frac{1+x^2}{1-x^2}\right) &= \sum_{u \neq -1} \chi(u)\left(1 + \chi((u+1)(u-1))\right) \\ &= 1 + \sum_{u \in \mathbb{F}_{p^n}} \chi(u) + \sum_{u \in \mathbb{F}_{p^n}} \chi\left(u(u^2-1)\right).\end{aligned}$$

This together with the identity 1) shows that $\sum_{x\in\mathbb{F}_{p^n}} \chi\left((1-x^2)(1+x^2)\right) = 1$.

Identity 20): We have

$$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+2x^2)(2+x^2)\right) = \sum_{x\in\mathbb{F}_{p^n}\setminus\{\pm 1\}} \chi\left(\frac{1+x^2}{1-x^2}(2+x^2)\right).$$

Let $\frac{1+x^2}{1-x^2} = u$, then x and u satisfy

$$(u+1)x^2 + 1 - u = 0. \tag{26}$$

When $u \neq -1$, (26) is a quadratic equation in variable x, and its discriminant is $4(u+1)(u-1)$. For each $u \in \mathbb{F}_{p^n}\setminus\{-1\}$, it corresponds $(1+\chi(\Delta))$ x's via (26). Moreover, from (26), we have $2+x^2 = \frac{3u+1}{u+1}$. Thus,

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{p^n}\setminus\{\pm 1\}} \chi\left(\frac{1+x^2}{1-x^2}(2+x^2)\right)\\
&= \sum_{u\neq -1} \chi\left(u\left(\frac{3u+1}{u+1}\right)\right)\left(1+\chi(u+1)(u-1)\right)\\
&= \sum_{u\neq -1} \chi(u(u+1)(3u+1)) + \sum_{u\neq -1} \chi\left(u(3u+1)(u-1)\right)\\
&= \sum_{u\in\mathbb{F}_{p^n}} \chi(u(u+1)(3u+1)) + \sum_{u\in\mathbb{F}_{p^n}} \chi\left(u(3u+1)(u-1)\right) + 1.
\end{aligned}$$

Furthermore, utilizing the identities 7) and 10), we have $\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+2x^2)(2+x^2)\right) = 1+\Gamma^{(2)}_{p,n} - \Gamma^{(3)}_{p,n}$. □

Appendix B

The Proof of Lemma 3:

For the first equation, we have

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{p^n}\setminus\mathcal{A}_1} \left((1-\chi(2-2x^2))(1-\chi(2+2x^2))(1-\chi(2+x^2))\right)\\
&= \sum_{x\in\mathbb{F}_{p^n}} 1 - \sum_{x\in\mathbb{F}_{p^n}} \chi(2-2x^2) - \sum_{x\in\mathbb{F}_{p^n}} \chi(2+2x^2) - \sum_{x\in\mathbb{F}_{p^n}} \chi(2+x^2)\\
&\quad + \sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+2x^2)\right) + \sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+x^2)\right)\\
&\quad + \sum_{x\in\mathbb{F}_{p^n}} \chi\left((2+2x^2)(2+x^2)\right) - \sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+2x^2)(2+x^2)\right)\\
&\quad - \sum_{\mathcal{A}_1} \left((1-\chi(2-2x^2))(1-\chi(2+2x^2))(1-\chi(2+x^2))\right).
\end{aligned}$$

Note that $\sum_{\mathcal{A}_1}((1-\chi(2-2x^2))(1-\chi(2+2x^2))(1-\chi(2+x^2)))=0$, and the character sums associated with any quadratic polynomial can be evaluated by [7, Theorem 5.48]. Then, by Lemma 2, we can obtain the desired result. The second and third identities can be similarly proved, and we omit the proofs here. □

Bounds for the average degree-k monomial density of Boolean functions

Ana Sălăgean
Department of Computer Science
Loughborough University
Loughborough, UK
A.M.Salagean@lboro.ac.uk

Percy Reyes-Paredes
Department of Computer Science
Loughborough University
Loughborough, UK
A.P.Reyes-Paredes@lboro.ac.uk

Abstract

For a Boolean function f represented in algebraic normal form (i.e. as a multivariate polynomial function over $\mathbb{F}_2$) we consider the density of monomials of degree k in f, for each degree k, i.e. the number of monomials of degree k that appear in f, normalized by the total number of possible monomials of degree k. We then average this number over all functions which are affine equivalent to f; we call the resulting quantity, denoted by $\mathrm{add}_k(f)$, the average degree-k monomial density of f. We defined this quantity in our previous work, and showed it is closely related to a probabilistic test we introduced for deciding whether $\deg(f) < k$.

In this paper we give lower and upper bounds for $\mathrm{add}_k(f)$ for polynomials of any degree d (only the particular case $d = k$ having been dealt with in our previous work). There are several consequences of these bounds. Firstly, the $\deg(f) < k$ probabilistic test is guaranteed to have high accuracy when the actual degree of f is not much higher than k. Secondly, it answers negatively the question: does there exist a function f which has no monomials of a particular degree k (with $k < \deg(f)$) and, moreover, it still has no monomials of degree k after applying any affine invertible change of coordinates to f. Thirdly, while the average of $\mathrm{add}_k(f)$ over all n-variable functions f of a fixed degree $d > k$ is equal to 0.5, the distribution of the values is somewhat surprising; when $k \leq n - 10$ and $n \geq 20$, low values of $\mathrm{add}_k(f)$ exist (reaching approximately $\frac{1}{2^{d-k}}$), but there are no values higher than around 0.5005.

Keywords: Algebraic degree, Moebius transform, probabilistic testing, algebraic thickness

1 Introduction and motivation

A Boolean function f in n variables can be uniquely represented in ANF (algebraic normal form), i.e. as a polynomial in n variables over $\mathbb{F}_2$ (the finite field with 2 elements) of degree

at most one in each variable. The degree of this polynomial is called the algebraic degree of f.

The algebraic degree is one of the parameters that measures the nonlinearity of Boolean functions used in cryptography. These Boolean functions must have high algebraic degree, otherwise some attacks can be effective; for example, the higher order derivative attacks, algebraic attacks, cube attacks, and integral attacks. However, the Boolean functions used in cryptography do not reach the highest degree because trade-offs with other parameters need to be considered.

We consider, for each degree k, the density of monomials of degree k in f, i.e. the number of monomials of degree k that appear in f, normalized by the total number of possible monomials of degree k. We then average this number over all functions which are affine equivalent to f; the resulting quantity, denoted by $\mathrm{add}_k(f)$, will be called the average degree-k monomial density of f. While the study of this parameter is interesting in itself, our original motivation comes from its connection to a probabilistic test that we introduced in previous work. Namely, when a cryptographic Boolean function f on $\mathbb{F}_2^n$ with a large number of variables is not given explicitly in ANF (e.g. it is given as a composition of functions, or even as a black box), it may not be feasible to compute its algebraic degree. The existence of a particular monomial $x_{i_1} \cdots x_{i_k}$ of degree k in the ANF of f can be decided by summing the values of f over a vector space generated by the k vectors of the canonical basis $e_{i_1}, \ldots, e_{i_k}$ (this method is also known as the Moebius transform). In [5, 6] we proposed the "$\deg(f) < k$" probabilistic test which generalizes this idea. One sums the values of f over a linear combination of k vectors, and if the result is zero, we say that f passes this instance of the test, otherwise it fails (we recall the full details in Section 2); when the k vectors are linearly independent, this is equivalent to testing the existence of a particular monomial of degree k after applying a random affine invertible change of variables to f. The number of monomials of degree k is likely to be high after the change of variables and therefore it would be easier to probabilistically detect their existence. The probability of failing the test is denoted by $\mathrm{dt}_k(f)$. In [6], we proved lower and upper bounds for $\mathrm{dt}_k(f)$ for the case when the actual degree of f (which is not known apriori) turns out to be k.

The main result of the present paper is Theorem 5 and its Corollary 6. They give lower and upper bounds on $\mathrm{dt}_k(f)$ and $\mathrm{add}_k(f)$ for a function f of any degree, generalising thus the existing result from [6] which only covers the case when f has degree k. These bounds have several consequences. Firstly, when the actual degree of f is not much higher than k, the $\deg(f) < k$ probabilistic test is guaranteed to have high accuracy (in the sense that it has a high probability of reaching the correct conclusion after a small number of tests). Secondly, it answers negatively the question: does there exist a function f which has no monomials of a particular degree k (with $k < \deg(f)$) and, moreover, it still has no monomials of degree k after applying any affine invertible change of coordinates to f. Thirdly, while the average of $\mathrm{add}_k(f)$ over all n-variable functions f of a fixed degree $d > k$ is equal to 0.5, the distribution of the values is somewhat surprising; when $k \leq n - 10$ and $n \geq 20$, low values of $\mathrm{add}_k(f)$ exist (reaching approximately $\frac{1}{2^{d-k}}$), but there are no values higher than around 0.5005.

2 Definitions and existing results

We denote by $\mathbb{F}_2$ the finite field with two elements, represented as $\{0,1\}$, and we denote by $\oplus$ addition in $\mathbb{F}_2$ as well as in the vector space $\mathbb{F}_2^n$. Any function $f:\mathbb{F}_2^n\to\mathbb{F}_2$ can be represented in its algebraic normal form (ANF), i.e. as a polynomial function given by a polynomial of degree at most 1 in each variable:

$$f(x_1,\dots,x_n)=\bigoplus_{a_1,\dots,a_n\in\mathbb{F}_2} c_{a_1,\dots,a_n}x_1^{a_1}\cdots x_n^{a_n},$$

with $c_{a_1,\dots,a_n}\in\mathbb{F}_2$. The degree of this polynomial is called the algebraic degree of f, and here we will call it simply the degree of f and denote it by $\deg(f)$. The coefficients of the ANF of f can be computed by the following formula (see, for example, [4, Chapter 13, Theorem 1]) which is sometimes called the Moebius transform:

$$c_{a_1,\dots,a_n}=\bigoplus_{x_1\le a_1,\dots,x_n\le a_n} f(x_1,\dots,x_n). \tag{1}$$

Two n-variable Boolean functions f and g are *affine equivalent*, denoted by $f\sim g$, if $g=f\circ\varphi_{M,v}$ for some invertible affine function $\varphi_{M,v}:\mathbb{F}_2^n\to\mathbb{F}_2^n$, $\varphi_{M,v}(x)=Mx\oplus v$, where M is an $n\times n$ nonsingular matrix over $\mathbb{F}_2$ and $v\in\mathbb{F}_2^n$ is a vector. If f and g are affine equivalent, then $\deg(f)=\deg(g)$. We therefore say that the algebraic degree is an *affine invariant*.

Definition 1. [6] Let $0\le k\le n$ be integers and let $f:\mathbb{F}_2^n\to\mathbb{F}_2$ be a function. The degree-k monomial density of f, denoted by $\mathrm{dd}_k(f)$, is defined as the number of monomials of degree k in the ANF of f, divided by $\binom{n}{k}$ (the total number of monomials of degree k in n variables). In other words, if the ANF of f is $f(x)=\bigoplus_m c_m m$, with m ranging over all monomials in n variables and $c_m\in\mathbb{F}_2$, then

$$\mathrm{dd}_k(f)=\frac{\mid\{m : m \text{ monomial of degree } k \text{ and } c_m\neq 0\}\mid}{\binom{n}{k}}. \tag{2}$$

The average degree-k monomial density of f, denoted by $\mathrm{add}_k(f)$, is the average (arithmetic mean) of $\mathrm{dd}_k(g)$ over all the functions g such that $f\sim g$, i.e.

$$\mathrm{add}_k(f)=\frac{\sum_{g\sim f}\mathrm{dd}_k(g)}{\mid\{g : g\sim f\}\mid}=\frac{\sum_{M\in GL(n,\mathbb{F}_2),v\in\mathbb{F}_2^n}\mathrm{dd}_k(f\circ\varphi_{M,v})}{2^n(2^n-1)(2^n-2)\cdots(2^n-2^{n-1})}. \tag{3}$$

It was shown in [6, Remark 5] that the two ways of defining add_k in equation (3) are indeed equal.

We recall the proposed $\deg(f)<k$ probabilistictest [5, 6]: pick $u_0,u_1,\dots,u_k\in\mathbb{F}_2^n$. If the equation

$$\bigoplus_{b_1,\dots,b_k\in\mathbb{F}_2} f\left(\left(\bigoplus_{i=1}^{k} b_iu_i\right)\oplus u_0\right)=0 \tag{4}$$

holds, we say that f passes this instance of the test, otherwise it fails. We denoted by $\mathrm{dt}_k(f)$ the probability of f failing the $\deg(f) < k$ test, taken over all all possible choices $u_0, u_1, u_2, \ldots, u_k \in \mathbb{F}_2^n$, i.e.

$$\mathrm{dt}_k(f) = \frac{|\{(u_0, u_1, u_2, \ldots, u_k) \in (\mathbb{F}_2^n)^{k+1} : \bigoplus_{b_1,\ldots,b_k \in \mathbb{F}_2} f\left(\left(\bigoplus_{i=1}^{k} b_i u_i\right) \oplus u_0\right) \neq 0\}|}{2^{(k+1)n}}. \quad (5)$$

If the degree of f is indeed less than k, then f always passes the $\deg(f) < k$ test, i.e. $\mathrm{dt}_k(f) = 0$. We are therefore interested in the values of $\mathrm{dt}_k(f)$ for the case when f has degree at least k. A value of $\mathrm{dt}_k(f)$ which is not very low would mean that after running the test a reasonably small number of times, we have a good chance of having at least one fail (namely, a probability of $1 - (1 - \mathrm{dt}_k(f))^t$ of at least one fail after t tests), and therefore decide, correctly, that $\deg(f) \geq k$.

One can easily check that $\mathrm{dt}_k(f)$ and $\mathrm{add}_k(f)$ are affine invariants. Moreover, it is easy to verify that they do not depend on the terms of f of degree strictly less than k, i.e. if $g = f \oplus h$ with $\deg(h) < k$ then $\mathrm{dt}_k(f) = \mathrm{dt}_k(g)$. Therefore we are working with the equivalence relation $\sim_{k-1}$ induced by affine equivalence on the quotient $RM(n,n)/RM(k-1,n)$, where $RM(k,n)$ denotes the set of polynomials of degree at most k in n variables (also known as the k-th order Reed-Muller code of length 2^n, see [4]). Namely, $f \sim_{k-1} g$ if there is a function h such that $f \sim h$ and $\deg(g - h) \leq k - 1$ (i.e. g and h coincide if we ignore all monomials of degree less than k).

It is noted in [6, Remark 3] that if the vectors $u_1, u_2, \ldots, u_k$ are linearly dependent, then any function f passes that particular instance of the $\deg(f) < k$ test. Therefore, in practice there is no need to run the test when they are linearly dependent. However, there are advantages in defining the probability for arbitrary vectors (one reason being the similar definition for the BLR linearity test; another reason being that Proposition 3 would not hold otherwise; see [6, Remark 3] for further discussion); the probability of failing the $\deg(f) < k$ test, taken over linearly independent vectors, equals $\mathrm{add}_k(f)$ and can be obtained by dividing $\mathrm{dt}_k(f)$ by the probability of k arbitrary vectors being linearly independent, see [6, Theorem 8]:

$$\mathrm{dt}_k(f) \;=\; \mathrm{add}_k(f) \prod_{i=n-k+1}^{n} \left(1 - \frac{1}{2^i}\right). \quad (6)$$

Recall that the discrete derivative of f in a non-zero direction $u \in \mathbb{F}_2^n$ is defined as $\mathrm{D}_u f(x) = f(x \oplus u) \oplus f(x)$. The derivative of order k in directions $u_1, \ldots, u_k$ is defined as $\mathrm{D}^{(k)}_{u_1,\ldots,u_k} f = \mathrm{D}_{u_1}(\mathrm{D}_{u_2}(\ldots \mathrm{D}_{u_k} f))$. For the $\deg(f) < k$ test, the equation (4) can be rewritten as $\mathrm{D}^{(k)}_{u_1,\ldots,u_k} f(u_0) = 0$.

In [6], we proved that if f has actually degree k, the following bounds on $\mathrm{dt}_k(f)$ hold:

Theorem 2. *[6, Theorem 14] Let f be a function of degree k in n variables. Then*

$$0.288788... < \prod_{i=1}^{k} \left(1 - \frac{1}{2^i}\right) \leq \mathrm{dt}_k(f) \leq \frac{1}{2}\left(1 - \frac{1}{2^n}\right)^{k-1} \leq 0.5, \quad (7)$$

where 0.288788... *is the q-Pochhammer symbol at* $(0.5, 0.5, \infty)$. *The lower bound is achieved if and only if* $f(x_1, \ldots, x_n)$ *is affine equiavalent to* $x_1 \ldots x_k \oplus h(x_1, \ldots, x_n)$ *for a polynomial* h *of degree at most* $k-1$.

We also recall the following basic properties:

Proposition 3. *[6, Proposition 10] Let* $f, g_1 : \mathbb{F}_2^n \to \mathbb{F}_2$ *and* $g_2 : \mathbb{F}_2^m \to \mathbb{F}_2$.
(i) If $g(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n)$, *then* $\mathrm{dt}_k(g) = \mathrm{dt}_k(f)$.
(ii) If $g(x_1, \ldots, x_{n+m}) = g_1(x_1, \ldots, x_n) \oplus g_2(x_{n+1}, \ldots, x_{n+m})$, *then* $\mathrm{dt}_k(g) = \mathrm{dt}_k(g_1) + \mathrm{dt}_k(g_2) - 2\mathrm{dt}_k(g_1)\mathrm{dt}_k(g_2)$.

3 Bounds on $\mathrm{dt}_k(f)$ and $\mathrm{add}_k(f)$

We compute first $\mathrm{dt}_k(f)$ for the case when the ANF of f has just one monomial:

Proposition 4. *Let* $f(x_1, \ldots, x_n) = x_1 x_2 \cdots x_d$. *For any* k *with* $1 \le k \le d$ *we have:*

$$\mathrm{dt}_k(f) = \frac{1}{2^{d-k}} \prod_{i=d-k+1}^{d} \left(1 - \frac{1}{2^i}\right).$$

Proof. We can assume that the number of variables n equals d, see Proposition 3(i). Note that $f(x_1, \ldots, x_d) = 1$ if and only if $(x_1, \ldots, x_d) = \mathbf{1}$ where we denote $\mathbf{1} = (1, 1, \ldots, 1)$. Consider the $\deg(f) < k$ test on f at $(u_0, u_1, \ldots, u_k) \in (\mathbb{F}_2^n)^{k+1}$, which checks whether the following equation holds:

$$\bigoplus_{b_1, \ldots, b_k \in \mathbb{F}_2} f(u_0 \oplus \bigoplus_{i=1}^{k} b_i u_i) = 0.$$

This test fails if and only if $u_1, \ldots, u_k$ are linearly independent and $\mathbf{1} \in u_0 \oplus \langle u_1, \ldots, u_k \rangle$. In other words, there are constants $b_i \in \mathbb{F}_2$ such that $\mathbf{1} = u_0 \oplus \bigoplus_{i=1}^{k} b_i u_i$. The number of ways to choose k linearly independent vectors $(u_1, \ldots, u_k) \in (\mathbb{F}_2^n)^k$ is $(2^n - 1)(2^n - 2) \cdots (2^n - 2^{k-1})$. For each of these choices, there are 2^k ways to choose u_0 such that $\mathbf{1} \in u_0 \oplus \langle u_1, \ldots, u_k \rangle$; namely, for each of the 2^k elements $u \in \langle u_1, \ldots, u_k \rangle$, we choose $u_0 = \mathbf{1} \oplus u$.

Therefore, by using the definition of dt_k, we have:

$$\begin{aligned} \mathrm{dt}_k(f) &= \frac{2^k(2^d - 1)(2^d - 2) \cdots (2^d - 2^{k-1})}{2^{(k+1)d}} \\ &= \frac{1}{2^{d-k}} \prod_{i=d-k+1}^{d} \left(1 - \frac{1}{2^i}\right). \end{aligned}$$

□

We now give lower and upper bounds for $\mathrm{dt}_k(f)$:

Theorem 5. *Let f be a polynomial of degree d in n variables. For any k with $1 \leq k \leq d$ we have:*

$$\frac{1}{2^{d-k}} \prod_{i=d-k+1}^{d} \left(1 - \frac{1}{2^i}\right) \leq \mathrm{dt}_k(f) \leq \frac{1}{2}\left(1 - \frac{1}{2^n}\right)^{k-1}.$$

The lower bound is tight; if f is affine equivalent to $x_1 x_2 \cdots x_d + g(x_1, \ldots, x_n)$ for a polynomial g of degree at most $k-1$, then $\mathrm{dt}_k(f)$ equals the lower bound.

Proof. The proof is by induction on d. For $d = 1$ we have $k = 1$, so Theorem 2 completes the proof of this case.

For the inductive step, we assume the statement is true for any degree less than d and prove it for degree d.

The $\deg(f) < k$ test on f at $(u_0, u_1, \ldots, u_k) \in (\mathbb{F}_2^n)^{k+1}$ checks whether the following equation holds:

$$\bigoplus_{b_1,\ldots,b_k \in \mathbb{F}_2} f(u_0 \oplus \bigoplus_{i=1}^{t} b_k u_i) = 0.$$

When $u_1 = \mathbf{0}$ this equation always holds, regardless of f; when $u_1 \neq \mathbf{0}$ the equation above can be rewritten as

$$\bigoplus_{b_2,\ldots,b_k \in \mathbb{F}_2} \mathrm{D}_{u_1} f(u_0 \oplus \bigoplus_{i=2}^{k} b_i u_i) = 0,$$

which is the $\deg(\mathrm{D}_{u_1} f) < k-1$ test at $(u_0, u_2, \ldots, u_k)$. We have therefore

$$\mathrm{dt}_k(f) = \frac{1}{2^n} \sum_{u_1 \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}} \mathrm{dt}_{k-1}(\mathrm{D}_{u_1} f). \tag{8}$$

For the lower bound, recall first that for any $u \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$ we have $\deg(\mathrm{D}_u f) \leq \deg(f) - 1$ (see [2]); u is called a *fast point* for f if $\deg(\mathrm{D}_u f) < \deg(f) - 1$ ([1]). In [1, Theorem 3.2], it was shown that, for a function f of degree d in n variables, the vector $\mathbf{0}$ together with the fast points of f forms a vector space of dimension at most $n - d$.

By denoting by S the set of non-zero vectors in $\mathbb{F}_2^n$ which are not fast points for f, we have therefore $|S| \geq 2^n - 2^{n-d}$. Since $\deg(\mathrm{D}_{u_1} f) = d - 1$ for all $u_1 \in S$, we can apply the induction hypothesis to $\mathrm{D}_{u_1} f$, obtaining $\mathrm{dt}_{k-1}(\mathrm{D}_{u_1} f)) \geq \frac{1}{2^{d-k}} \prod_{i=d-k+1}^{d-1} \left(1 - \frac{1}{2^i}\right)$. By

using these results in (8), we have

$$\begin{aligned}
\mathrm{dt}_k(f) &= \frac{1}{2^n}\sum_{u_1\in\mathbb{F}_2^n\setminus\{\mathbf{0}\}}\mathrm{dt}_{k-1}(\mathrm{D}_{u_1}f)\\
&\geq \frac{1}{2^n}\sum_{u_1\in S}\mathrm{dt}_{k-1}(\mathrm{D}_{u_1}f)\\
&\geq \frac{|S|}{2^n}\frac{1}{2^{d-k}}\prod_{i=d-k+1}^{d-1}\left(1-\frac{1}{2^i}\right)\\
&\geq \frac{2^n-2^{n-d}}{2^n}\frac{1}{2^{d-k}}\prod_{i=d-k+1}^{d-1}\left(1-\frac{1}{2^i}\right)\\
&= \frac{1}{2^{d-k}}\prod_{i=d-k+1}^{d}\left(1-\frac{1}{2^i}\right)
\end{aligned}$$

as required. The fact that the lower bound is achieved with equality when $f\sim_{k-1}x_1\cdots x_d$ is immediate from Proposition 4.

For the upper bound, since $\mathrm{D}_{u_1}f$ has degree strictly less than d, we know by the induction hypothesis that if it has degree at least $k-1$, then $\mathrm{dt}_{k-1}(\mathrm{D}_{u_1}f)\leq\frac{1}{2}\left(1-\frac{1}{2^n}\right)^{k-2}$. If it has degree less than $k-1$, then $\mathrm{dt}_{k-1}(\mathrm{D}_{u_1}f)=0<\frac{1}{2}\left(1-\frac{1}{2^n}\right)^{k-2}$. Hence, we have $\mathrm{dt}_{k-1}(\mathrm{D}_{u_1}f)\leq\frac{1}{2}\left(1-\frac{1}{2^n}\right)^{k-2}$ for each of the 2^n-1 values of $u_1\in\mathbb{F}_2^n\setminus\{\mathbf{0}\}$. Therefore, by using (8), we obtain $\mathrm{dt}_k(f)\leq\frac{1}{2}\left(\frac{2^n-1}{2^n}\right)\left(1-\frac{1}{2^n}\right)^{k-2}=\frac{1}{2}\left(1-\frac{1}{2^n}\right)^{k-1}$ so the upper bound holds. □

Theorem 5 and (6) also yield bounds for $\mathrm{add}_k(f)$:

Corollary 6. *Let f be a polynomial of degree d in n variables. For any k with $1\leq k\leq d$ we have:*

$$\frac{1}{2^{d-k}}\left(\frac{\prod_{i=d-k+1}^{d}\left(1-\frac{1}{2^i}\right)}{\prod_{i=n-k+1}^{n}\left(1-\frac{1}{2^i}\right)}\right)\leq\mathrm{add}_k(f)\leq\frac{1}{2}\left(\frac{\left(1-\frac{1}{2^n}\right)^{k-1}}{\prod_{i=n-k+1}^{n}\left(1-\frac{1}{2^i}\right)}\right). \tag{9}$$

The lower bound is tight; if f is affine equivalent to $x_1x_2\cdots x_d+g(x_1,\ldots,x_n)$ for some polynomial g of degree at most $k-1$, then $\mathrm{add}_k(f)$ equals the lower bound.

We will now examine a number of consequences of Theorem 5 and Corollary 6. Firstly, note that the lower bounds in both cases are non-zero. Therefore:

Corollary 7. *Let f be a Boolean function and let $k<\deg(f)$. There is at least one function g which is affine equivalent to f and has at least one monomial of degree k which appears with non-zero coefficient in the ANF of g.*

In other words, Corollary 7 says that even if a function f has no monomials of a certain degree $k<\deg(f)$, it is not possible that all the functions in its affine equivalence class also have this property.

Next, we estimate the numerical values of the bounds. We are particularly interested in functions in at least 20 variables, as for functions in fewer variables the ANF can be explicitly computed even if the function is given as a black box. For k, we are interested in values of at most 40, as the values of f at 2^k points need to be summed for one $\deg(g) < k$ test, which becomes unfeasible for $k > 40$.

When $n \geq 20$ and $2 \leq k \leq 40$ we have

$$0.49998 < \frac{1}{2}\left(1 - \frac{1}{2^n}\right)^{k-1} \leq 0.5.$$

so we will approximate the upper bound on $\mathrm{dt}_k(f)$ in Theorem 5 by 0.5.

For the other bounds, estimates for the following quantity will be particularly useful:

$$P(a,b) = \prod_{i=a}^{b}\left(1 - \frac{1}{2^i}\right)$$

for integers $1 \leq a \leq b$. (Recall that the q-Pochhammer symbol is defined as $(c;q)_n = \prod_{i=0}^{n-1}(1-cq^i)$ with n a positive integer or ∞, so $P(a,b) = (\frac{1}{2^a};\frac{1}{2})_{b-a}$). It is obvious that for a fixed a, $P(a,b)$ decreases as b increases. When $a = 1$ as b tends to infinity, this quantity converges to a limit (namely $(\frac{1}{2^a};\frac{1}{2})_\infty$) which is in the interval $(0.288788, 0.288789)$; it converges fast, for example for $b = 20$, we are already within this interval and therefore closer than 10^{-6} to the limit. Similarly, the values of $P(a,b)$ for small values of $a = 1,\ldots,10$ and $b \geq 20$ are, to 6 decimal places: 0.288788, 0.577576, 0.770102, 0.880116, 0.938791, 0.969074, 0.984456, 0.992208, 0.996099, 0.998048. For larger values of a, the quantity $P(a,b)$ is close to 1. For example, when $a \geq 11$ we have $P(a,b) \in (0.999, 1)$, and when $a \geq 21$ we have $P(a,b) \in (0.999999, 1)$, for any $b \geq a$.

Using the estimates above for $P(a,b)$, the values of the lower bound on $\mathrm{dt}_k(f)$ from Theorem 5 are tabulated (to 6 decimal places) in Table 1 for $d - k = 0, 1, \ldots, 8$, with the assumption $d \geq 20$. We also computed, based on this lower bound, the number of tests t that we would need to run in order to guarantee a probability of at least 0.95 that a correct decision is reached (i.e. $1 - (1 - \mathrm{dt}_k(f))^t \geq 0.95$). These numerical values show that by running the $\deg(f) < k$ test 769 times we can say with 0.95 confidence that if the actual degree of f (which is unknown) is at most $k + 8$ then the correct conclusion will be reached.

In Table 1, we also computed the lower and upper bounds for $\mathrm{add}_k(f)$, again under the assumption $n \geq d \geq 20$. These bounds were obtained by dividing the lower and upper bounds of $\mathrm{dt}_k(f)$ (with the upper bound approximated as 0.5) by $P(n-k, n) = P(n-d-(d-k))$. We tabulated the values for $d - k = 0, \ldots, 8$, considering two cases: $n - d = 2$ and $n - d = 10$ (any value of $n - d$ higher than 10 giving results very close to the ones for $n - d = 10$).

Let us fix k and d with $k < d$. When f ranges over all n-variable functions of degree d, the number of monomails of degree k in the ANF of f has a binomial distribution with parameters $\binom{n}{k}$ and 0.5; each value $i = 0, 1, \ldots, \binom{n}{k}$ appears with probability $\binom{\binom{n}{k}}{i}\frac{1}{2^{\binom{n}{k}}}$. The number of degree-$k$ monomials in f, averaged over all functions f of degree d, equals

$d-k$	$\mathrm{dt}_k(f)$ lower bound	t	$\mathrm{add}_k(f)$ lower bound $n-d=2$	$\mathrm{add}_k(f)$ upper bound $n-d=2$	$\mathrm{add}_k(f)$ lower bound $n-d=10$	$\mathrm{add}_k(f)$ upper bound $n-d=10$
0	0.288788	9	0.375000	0.649265	0.289070	0.500489
1	0.288788	9	0.328125	0.568107	0.288929	0.500244
2	0.192525	15	0.205078	0.532600	0.192572	0.500122
3	0.110015	26	0.113525	0.515957	0.110028	0.500061
4	0.058674	50	0.059601	0.507895	0.058678	0.500031
5	0.030284	98	0.030521	0.503927	0.030284	0.500015
6	0.015382	194	0.015442	0.501958	0.015382	0.500008
7	0.007752	385	0.007767	0.500978	0.007752	0.500004
8	0.003891	769	0.003895	0.500489	0.003891	0.500002

Table 1: Bounds for $\mathrm{dt}_k(f)$ and $\mathrm{add}_k(f)$ for $n \geq d \geq 20$, and number of tests t for a 0.95 probability of reaching a correct decision

$\frac{1}{2}\binom{n}{k}$ and the standard deviation equals $\frac{1}{2}\sqrt{\binom{n}{k}}$. Since we are interested in the case $n \geq 20$, as long as $k > 0$, this binomial distribution can be approximated by the normal distribution, so, for example, 95% of the values of the degree-k density, $\mathrm{dd}_k(f)$ (which is the number of degree-k monomials divided by $\binom{n}{k}$, as defined in Definition 1), will fall within the interval $[0.5 - \frac{1}{\sqrt{\binom{n}{k}}}, 0.5 + \frac{1}{\sqrt{\binom{n}{k}}}]$, i.e. will be very close to 0.5.

If we average $\mathrm{dd}_k(f)$ within each affine equivalence class (note the classes are not all of the same size), i.e we compute $\mathrm{add}_k(f)$, we would intuitively expect that most of the $\mathrm{add}_k(f)$ values would be close to 0.5, with possibly a small number of them being much lower or much higher.

However, what is surprising is that, for most values of $k < d < n$, Corollary 6 can be used to show that there exist at least one class where $\mathrm{add}_k(f)$ is much lower than 0.5, but there are no classes with $\mathrm{add}_k(f)$ much higher than 0.5. More precisely, from Table 1 we can see that for functions f in at least $n = 30$ variables, if the degree d of f is at most $n - 10$, then $\mathrm{add}_k(f)$ can be quite low (keeping in mind that the lower bound is tight and, for example, for $d - k \leq 6$ the lower bound is just under $\frac{1}{2^{d-k}}$), but, surprisingly, $\mathrm{add}_k(f)$ cannot be any higher than about 0.5005. Namely, by using the previous estimates for $P(a, b)$, we have that $\mathrm{add}_k(f) \leq 0.5/P(n-k, n) < 0.5005$ when $n - k \geq 10$ and $\mathrm{add}_k(f) < 0.5000005$ when $n - k \geq 20$. It is only for functions f where n, d and k are very close to each other that $\mathrm{add}_k(f)$ can be significantly higher than 0.5 (with the extreme case of $n = d = k$, where the density of monomials of degree n for a function of degree n in n variables is obviously equal to 1 as there is only one monomial of degree n and the degree is an affine invariant).

We computed the exact values of $\mathrm{dt}_k(f)$, $k = 3, 4$, for all the 68431 classes of functions of degree 4 in 7 variables, under the equivalence $\sim_2$. A representative for each class was determined by Langevin in [3]. The values of $dt_4(f)$ range between 0.307617 and 0.451813. The lower and upper bounds given by Theorem 5 would be 0.307617 and

0.488373 respectively; so, while the lower bound is achieved, the upper bound is not tight in this case. Likewise, the values of $dt_3(f)$ range between 0.307617 and 0.481934. The lower and upper bounds given by Theorem 5 would be 0.307617 and 0.492218 respectively; so, while the lower bound is achieved, the upper bound is not tight in this case.

Using (6), for polynomials of degree 4 in 7 variables, $\mathrm{add}_4(f) \in [0.346795, 0.509356]$ and $\mathrm{add}_3(f) \in [0.325120, 0.516162]$.

We also considered functions that describe the whole cipher Trivium, Grain-128a, and SNOW-V. Namely, for each cipher, the inputs are the key and initialisation vector and the output is the first bit of the key stream. In each case, we ran the $\deg(f) < k$ test, for $k = 1, 2, \ldots, 10$ at least 20 times. Not surprisingly, the test confirmed that the functions have degree at least 10. The experimental probability of failing the test was within the interval (0.47-0.52) in each case.

4 Conclusions

We studied $\mathrm{add}_k(f)$, a parameter describing the density of monomials of degree k in the Algebraic Normal Form of a Boolean function f, averaged over all functions which are affine equivalent to f. We obtained lower and upper bounds for $\mathrm{add}_k(f)$ for polynomials of any degree d (only the particular case $d = k$ having been dealt with in our previous work). A first consequence is that the $\deg(f) < k$ probabilistic test, introduced by us in previous work, is guaranteed to have high accuracy when the actual degree of f is not much higher than k. We also answered negatively the following natural question: does there exist a function f which has no monomials of a particular degree k (with $k < \deg(f)$) and, moreover, it still has no monomials of degree k after applying any affine invertible change of coordinates to f. Finally, we evaluated the bounds numerically in several typical situations of interest. For example, for functions in at least $n \geq 20$ variables, when $k \leq n - 10$ and $k < \deg(f)$ there are functions with a quite low value for $\mathrm{add}_k(f)$ (approximately $\frac{1}{2^{d-k}}$), but, somewhat surprisingly (seen that $\mathrm{add}_k(f)$ has mean 0.5) there are no functions where $\mathrm{add}_k(f)$ is higher than around 0.5005.

References

[1] Ming Duan, Mohan Yang, Xiaorui Sun, Bo Zhu, and Xuejia Lai. Distinguishing properties and applications of higher order derivatives of Boolean functions. *Information Sciences*, 271:224–235, 2014.

[2] Xuejia Lai. Higher order derivatives and differential cryptanalysis. In Richard E. Blahut, Daniel J. Costello, Jr., Ueli Maurer, and Thomas Mittelholzer, editors, *Communications and Cryptography*, volume 276 of *The Springer International Series in Engineering and Computer Science*, pages 227–233. Springer, 1994.

[3] Philippe Langevin. Classification of RM(4,7)/RM(2,7), January 2012. https://langevin.univ-tln.fr/project/rm742/rm742.html.

[4] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1978.

[5] Ana Sălăgean and Percy Reyes-Paredes. Probabilistic estimation of the degree of Boolean function. The Selmer Center in Secure Communication, The 7th International Workshop on Boolean Functions and their Applications (BFA), September 2022.

[6] Ana Sălăgean and Percy Reyes-Paredes. Probabilistic estimation of the algebraic degree of Boolean functions. *Cryptography and Communications*, 15(6):1199–1215, 2023.

Optimal few-weight codes from projective spaces

Guangkui Xu*
School of Mathematics and Physics
Anhui Jianzhu University
Hefei, China

Operations Research and
Data Science Laboratory
Anhui Jianzhu University
Hefei, China

xuguangkuiy@163.com

Heqian Xu †
School of Mathematics and Statistics
Hefei Normal University
Hefei,China

heqianx@hfnu.edu.cn

Gaojun Luo‡
Department of Mathematics
Nanjing University of Aeronautics and Astronautics
Nanjing, China,

gjluo1990@163.com

Abstract

Linear codes with few weights have been extensively developed because of their wide applications in consumer electronics, data storage system, secret sharing, authentication codes, association schemes, and strongly regular graphs. This paper is devoted to two new constructions of linear codes with few weights over the ring $\mathbb{F}_p + u\mathbb{F}_p$ from projective spaces. Moreover, we determine the Lee weight distributions of these codes by investigating the property of the support of the vectors of $\mathbb{F}_p^m$. Via the Gray map, we obtain three classes of linear codes with few weights over $\mathbb{F}_p$. In some cases, these linear codes are proved to be optimal with respect to the Griesmer bound.

*G. Xu is supported by the National Natural Science Foundation of China under Grants 62172183, 12371339, the PhD Research Startup Fund for Anhui Jianzhu University (No. 2023QDZ29), the innovation team of operation research and combinatorial optimization of Anhui province (No. 2023AH010020), the Natural Science Research Foundation of Anhui Provincial Department of Education (No. 2023AH050194) and the Projects of Natural Science Research in Anhui Colleges and Universities (No. HYB20230132).

†H. Xu is supported by the National Natural Science Foundation of China under Grant 12171134 and the Natural Science Foundation for the Higher Education Institutions of Anhui Province of China under Grant KJ2021A0926.

‡G. Luo is supported by the National Natural Science Foundation of China under Grant 12171241 and the Natural Science Foundation of Jiangsu Province under Grant BK20230867.

1 Introduction

Let $\mathbb{F}_p$ be the finite field with order p, where p is an odd prime. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_p$ is a k-dimensional subspace of $\mathbb{F}_p^n$ with minimum Hamming distance d. The *weight enumerator* of $\mathcal{C}$ is the polynomial $1+N_1x+N_2x^2+\cdots+N_nx^n$, where N_i denotes the number of codewords of Hamming weight i in $\mathcal{C}$. The sequence $(1, N_1, N_2, \cdots, N_n)$ is called the *weight distribution* of the code $\mathcal{C}$. The weight distribution contains important information for estimating the probability of error detection and correction. During the past decade, much attention has been paid to determining the weight distribution of a code. Determining the weight distribution of a given code is not an easy task in general. We call $\mathcal{C}$ a t-weight linear code if the number of nonzero N_i in the sequence $(N_1, N_2, \ldots, N_n)$ is equal to t. Linear codes with few weights have been extensively studied because of their significantly important role in consumer electronics, data storage system, secret sharing, authentication codes, association schemes, and strongly regular graphs.

There exists several bounds on the number of codewords in a linear code given the length n and minimum distance d of the code. It is interesting to construct a linear code achieving one bound. For an $[n, k, d]$ linear code over $\mathbb{F}_p$, the Griesmer bound is given by

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{p^i} \rceil,$$

where $\lceil \cdot \rceil$ is the ceiling function. This bound was proved by Griesmer ([3]) for the binary codes and was generalized by Solomon and Stiffler ([15]) for codes over arbitrary finite filed. A linear code C is *optimal* if its parameters n, k and d meet the Griesmer bound [4].

Let $\mathbb{F}_q$ denote the finite field with q elements, where q is a power of p. In [2], Ding and Niederreiter proposed a generic construction of linear codes over $\mathbb{F}_p$. Let $D = \{d_1, d_2, \ldots, d_n\}$ and $\mathrm{Tr}_p^q(\cdot)$ denote the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. A linear code of length n over $\mathbb{F}_p$ is defined as:

$$\mathcal{C}_D = \{(\mathrm{Tr}_p^q(ad_1), \mathrm{Tr}_p^q(ad_2), \ldots, \mathrm{Tr}_p^q(ad_n)) : a \in \mathbb{F}_q\}. \tag{1}$$

We call D the defining set of $\mathcal{C}_D$. Let $\mathrm{R} = \mathbb{F}_q + u\mathbb{F}_q$ with $u^2 = 0$. It is easy to see that R is a local ring with the maximal ideal $\langle u \rangle$. Let $\mathrm{R}_m = \mathbb{F}_{q^m} + u\mathbb{F}_{q^m}$ with $u^2 = 0$ be an extension ring of R and let R_m^* be the multiplicative group of units of R_m. In [10, 11], the construction defined by (1) was later generalized to codes over finite rings. A linear code over R with a defining set $K = \{d_1, d_2, \ldots, d_n\} \subseteq \mathrm{R}_m^*$ is defined as:

$$\mathcal{C}_K = \{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \ldots, \mathrm{Tr}(xd_n)) : x \in \mathrm{R}_m\}, \tag{2}$$

where Tr is the trace function from R_m to R defined by $Tr(a+ub) = \mathrm{Tr}_p^q(a) + u\mathrm{Tr}_p^q(b)$ for $a + ub \in \mathrm{R}_m$. It is easy to see that $\mathcal{C}_K$ defined in (2) is an R-submodule of R^m. Using this construction, some optimal linear codes with few weights over rings have been obtained by selecting the defining sets (see, for instance [9, 7, 12, 13]).

In recent years, several infinite families of optimal or distance-optimal linear codes from simplicial complexes or down sets were constructed (see [1, 5, 6, 14, 16, 17, 18]). In

[8], Luo and Ling presented infinite families of optimal or distance-optimal linear codes over $\mathbb{F}_p$ from projective spaces and investigated the locality of these linear codes. Inspired by the work in [8, 16], in this paper, we construct two classes of linear codes with few Lee weights over $\mathrm{R} = \mathbb{F}_p + u\mathbb{F}_p$ with $u^2 = 0$ by employing projective spaces. Let V_A be a subspace of $\mathbb{F}_p^m$ and P_A the corresponding projective space of V_A (see Section 2). Let $K_1 = V_{A_1} + uP_{A_2}$ and $K_2 = P_{A_1} + uV_{A_2}$. Based on the construction defined in (2), two classes of linear codes over $\mathrm{R} = \mathbb{F}_p + u\mathbb{F}_p$ are defined as

$$\mathcal{C}_{K_1} = \{c_{\mathbf{x}} = (\langle \mathbf{x}, \mathbf{d} \rangle_{\mathrm{R}})_{\mathbf{d} \in K_1} | \mathbf{x} \in \mathbb{F}_p^m + u\mathbb{F}_p^m\}$$

and

$$\mathcal{C}_{K_2} = \{c_{\mathbf{x}} = (\langle \mathbf{x}, \mathbf{d} \rangle_{\mathrm{R}})_{\mathbf{d} \in K_2} | \mathbf{x} \in \mathbb{F}_p^m + u\mathbb{F}_p^m\},$$

where $\langle \mathbf{x}, \mathbf{d} \rangle_{\mathrm{R}}$ denotes the inner product of two vectors $\mathbf{x}$ and $\mathbf{d}$ of R^m(see Section 2 for definition).

The rest of this paper is organized as follows. Some preliminaries and notation are given in section 2. In Section 3, we determine the Lee weight distributions of linear codes $\mathcal{C}_{K_1}$ and $\mathcal{C}_{K_2}$ by investigating the property of the support of the vectors of $\mathbb{F}_p^m$. In Section 4, we use the Gray map to obtain some few-weight optimal linear codes over $\mathbb{F}_p$. In Section 5, we make a conclusion.

2 Preliminaries

Let $[m]$ be the set of all integers from 1 to m. Let V_{m+1}^* be the set of all nonzero vectors in vector space $\mathbb{F}_p^{m+1}$. For two vectors $\mathbf{x} = (x_1, x_2, \ldots, x_{m+1})$, $\mathbf{x}' = (x_1', x_2', \ldots, x_{m+1}')$ in V_{m+1}^*, we say that $\mathbf{x}$ and $\mathbf{x}'$ are equivalent if there exists a nonzero $c \in \mathbb{F}_p$ such that $\mathbf{x} = c\mathbf{x}'$. The equivalence class is denoted by $[x_1 : x_2 : \cdots : x_{m+1}]$ and consist of all nonzero scalar multiples of $(x_1, x_2, \ldots, x_{m+1})$. Then the set of equivalence classes is the projective space over F_p with dimension m and is denoted by $PG(m, \mathbb{F}_p)$. The elements of $PG(m, \mathbb{F}_p)$ are called points.

Let A be a nonempty subset of $[m]$. Define an $|A|$-dimensional subspace of $\mathbb{F}_p^m$ as follows:

$$V_A = \{(x_1, x_2, \ldots, x_m) : x_i \in \mathbb{F}_p \text{ if } i \in A \text{ and } x_i = 0 \text{ if } i \notin A\}. \tag{3}$$

Let P_A be the corresponding projective space of V_A. In this paper, we always choose the points of P_A whose first nonzero coordinate position is 1 as a vector representing a equivalence class and express all points of P_A as vectors of length m. It is easy to check that $V_A \backslash \{\mathbf{0}\} = \bigcup_{c \in \mathbb{F}_p^*} cP_A$ and $|P_A| = \frac{p^{|A|}-1}{p-1}$. For example, if $m = 5$ and $A = \{1, 2, 4\}$, then

$$V_{\{1,2,4\}} = \{(x_1, x_2, 0, x_4, 0) : x_1, x_2, x_4 \in \mathbb{F}_p\},$$
$$P_{\{1,2,4\}} = \{(1, x_2, 0, x_4, 0) : x_2, x_4 \in \mathbb{F}_p\} \bigcup \{(0, 1, 0, x_4, 0) : x_4 \in \mathbb{F}_p\} \bigcup \{(0, 0, 0, 1, 0)\}.$$

Below we let $\mathrm{R} = \mathbb{F}_p + u\mathbb{F}_p$ and $\mathrm{R}^m = \mathbb{F}_p^m + u\mathbb{F}_p^m$, where $u^2 = 0$. The inner product of vectors $\mathbf{a} = (a_1, a_2, \ldots, a_m)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_m)$ of R^m is defined by $\langle \mathbf{a}, \mathbf{b} \rangle_R = \sum_{i=1}^m a_i b_i$. Similarly, for two vectors $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in \mathbb{F}_p^m$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_m) \in \mathbb{F}_p^m$, we define the inner product of α and β as $\langle \alpha, \beta \rangle_F = \sum_{i=1}^m \alpha_i \beta_i$.

For any $x + uy \in \mathrm{R}$, $x, y \in \mathbb{F}_p$, define the Gray map ϕ from R to $\mathbb{F}_p^2$ by

$$\phi : \mathrm{R} \to \mathbb{F}_p^2, x + uy \mapsto (y, x + y).$$

For $\mathbf{x} = \alpha + u\beta \in \mathrm{R}^m$, $\alpha \in \mathbb{F}_p^m$ and $\beta \in \mathbb{F}_p^m$, the map ϕ can extend naturally to a map from R^m to $\mathbb{F}_p^{2m}$ as follow:

$$\phi : \mathrm{R}^m \to \mathbb{F}_p^{2m}, \mathbf{x} = \alpha + u\beta \mapsto (\beta, \alpha + \beta).$$

Let $\mathcal{C}$ be a linear code of length m over R. Denote by $w_H(\alpha)$ the Hamming weight of $\alpha \in \mathbb{F}_p^m$. For a codeword $\mathbf{c} = \alpha + u\beta$ of $\mathcal{C}$, the Lee weight of $\mathbf{c}$ is defined to the Hamming weight of its Gray image as follows:

$$w_L(\mathbf{c}) = w_L(\alpha + u\beta) = w_H(\beta) + w_H(\alpha + \beta).$$

The *Lee weight enumerator* of $\mathcal{C}$ of length m is the polynomial $1 + B_1 z + B_2 z^2 + \cdots + B_m z^m$, where B_i denotes the number of codewords of Lee weight i in $\mathcal{C}$. The sequence $(1, B_1, B_2, \cdots, B_m)$ is called the *Lee weight distribution* of the code $\mathcal{C}$.

3 The Lee weight distributions of $\mathcal{C}_{K_1}$ and $\mathcal{C}_{K_2}$

In this section, we present two classes of linear codes over R from projective spaces and determine the Lee weight distributions of these codes.

The support of a vector $\mathbf{a} = (a_1, a_2, \ldots, a_m) \in \mathbb{F}_p^m$, denoted by $\mathrm{Supp}(\mathbf{a})$, is defined by $\mathrm{Supp}(\mathbf{a}) = \{1 \le i \le m : a_i \neq 0\}$. For $A \subseteq [m]$ and $\mathbf{a} \in \mathbb{F}_p^m$, let $\mathbf{a}_A$ be a vector obtained from $\mathbf{a}$ by puncturing on coordinates in $[m] \backslash A$. The following three lemmas are crucial in determining the Lee weight distributions of the codes.

Lemma 1. *[8] Let A_1 and A_2 be two subsets of $[m]$. Then we have the following.*

(i)

$$|S_0 = \{\mathbf{a} \in \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_1 = \emptyset\}| = p^{m - |A_1|}$$

and

$$|S_1 = \{\mathbf{a} \in \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_1 \neq \emptyset\}| = p^m - p^{m - |A_1|}.$$

(ii)

$$|S_{20} = \{\mathbf{a} \in \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_1 = \emptyset, \mathrm{Supp}(\mathbf{a}) \cap A_2 = \emptyset\}| = p^{m - |A_1 \cup A_2|},$$

$$|S_{21} = \{\mathbf{a} \in \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_1 = \emptyset, \mathrm{Supp}(\mathbf{a}) \cap A_2 \neq \emptyset\}| = p^{m - |A_1|} - p^{m - |A_1 \cup A_2|},$$

$$|S_{22} = \{\mathbf{a} \in \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_1 \neq \emptyset, \mathrm{Supp}(\mathbf{a}) \cap A_2 = \emptyset\}| = p^{m - |A_2|} - p^{m - |A_1 \cup A_2|}$$

and

$$|S_{23} = \{\mathbf{a} \in \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_1 \neq \emptyset, \mathrm{Supp}(\mathbf{a}) \cap A_2 \neq \emptyset\}| = p^m - p^{m - |A_1|} - p^{m - |A_2|} + p^{m - |A_1 \cup A_2|}.$$

Lemma 2. *Let A_1 and A_2 be two subsets of $[m]$ and let*

$$T_0 = \{(\mathbf{a},\mathbf{b}) \in \mathbb{F}_p^m \times \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_2 = \emptyset, \mathrm{Supp}(\mathbf{b}) \cap A_1 = \emptyset, \mathrm{Supp}(\mathbf{a}+\mathbf{b}) \cap A_1 = \emptyset\},$$

$$T_1 = \{(\mathbf{a},\mathbf{b}) \in \mathbb{F}_p^m \times \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_2 = \emptyset, \mathrm{Supp}(\mathbf{b}) \cap A_1 = \emptyset, \mathrm{Supp}(\mathbf{a}+\mathbf{b}) \cap A_1 \neq \emptyset\},$$

$$T_2 = \{(\mathbf{a},\mathbf{b}) \in \mathbb{F}_p^m \times \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_2 = \emptyset, \mathrm{Supp}(\mathbf{b}) \cap A_1 \neq \emptyset, \mathrm{Supp}(\mathbf{a}+\mathbf{b}) \cap A_1 = \emptyset\}$$

and

$$T_3 = \{(\mathbf{a},\mathbf{b}) \in \mathbb{F}_p^m \times \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_2 = \emptyset, \mathrm{Supp}(\mathbf{b}) \cap A_1 \neq \emptyset, \mathrm{Supp}(\mathbf{a}+\mathbf{b}) \cap A_1 \neq \emptyset\}.$$

Then

$$|T_0| = p^{2m-|A_1|-|A_1\cup A_2|}, |T_1| = |T_2| = p^{m-|A_1|}(p^{m-|A_2|} - p^{m-|A_1\cup A_2|})$$

and

$$|T_3| = p^{m-|A_2|}(p^m - 2p^{m-|A_1|}) + p^{2m-|A_1|-|A_1\cup A_2|}.$$

Proof. For $\mathbf{a},\mathbf{b} \in \mathbb{F}_p^m$, let B be a subset of $\mathrm{Supp}(\mathbf{a}) \cap \mathrm{Supp}(\mathbf{b})$ consisting of the coordinates at which $\mathbf{a}+\mathbf{b}$ is nonzero. It can be verified that

$$\begin{aligned}\mathrm{Supp}(\mathbf{a}+\mathbf{b}) &= \Big(\big(\mathrm{Supp}(\mathbf{a}) \cup \mathrm{Supp}(\mathbf{b})\big) \setminus \big(\mathrm{Supp}(\mathbf{a}) \cap \mathrm{Supp}(\mathbf{b})\big)\Big) \cup B \\ &= \big(\mathrm{Supp}(\mathbf{a}) \cap \mathrm{Supp}(\mathbf{b})^c\big) \cup \big(\mathrm{Supp}(\mathbf{b}) \cap \mathrm{Supp}(\mathbf{a})^c\big) \cup B, \end{aligned} \tag{4}$$

where $\mathrm{Supp}(\mathbf{a})^c = [m] \setminus \mathrm{Supp}(\mathbf{a})$ and $\mathrm{Supp}(\mathbf{b})^c = [m] \setminus \mathrm{Supp}(\mathbf{b})$.

Note that $\{(\mathbf{a},\mathbf{b}) \in \mathbb{F}_p^m \times \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_2 = \emptyset, \mathbf{b} \in \mathbb{F}_p^m\} = T_0 \cup T_1 \cup T_2 \cup T_3$. It suffices to determine the size of T_0, T_1, T_2 by Lemma 1 (i) .

Firstly, we determine the size of T_0. By (4), we have

$$\mathrm{Supp}(\mathbf{a}+\mathbf{b}) \cap A_1 = \big(\mathrm{Supp}(\mathbf{a}) \cap \mathrm{Supp}(\mathbf{b})^c \cap A_1\big) \cup \big(\mathrm{Supp}(\mathbf{b}) \cap \mathrm{Supp}(\mathbf{a})^c \cap A_1\big) \cup (B \cap A_1) = \emptyset.$$

This implies that $\mathrm{Supp}(\mathbf{a}) \cap \mathrm{Supp}(\mathbf{b})^c \cap A_1 = \emptyset$. Since $\mathrm{Supp}(\mathbf{b}) \cap A_1 = \emptyset$, we have $\mathrm{Supp}(\mathbf{b})^c \cap A_1 = A_1$. It follows that $\mathrm{Supp}(\mathbf{a}) \cap A_1 = \emptyset$. That is to say, $\mathrm{Supp}(\mathbf{a}+\mathbf{b}) \cap A_1 = \emptyset$ and $\mathrm{Supp}(\mathbf{b}) \cap A_1 = \emptyset$ if and only if $\mathrm{Supp}(\mathbf{a}) \cap A_1 = \emptyset$ and $\mathrm{Supp}(\mathbf{b}) \cap A_1 = \emptyset$. Hence, T_0 can be written as

$$T_0 = \{(\mathbf{a},\mathbf{b}) \in \mathbb{F}_p^m \times \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_2 = \emptyset, \mathrm{Supp}(\mathbf{b}) \cap A_1 = \emptyset, \mathrm{Supp}(\mathbf{a}) \cap A_1 = \emptyset\}.$$

By Lemma 1, we know that $|T_0| = |S_0| \times |S_{20}| = p^{2m-|A_1|-|A_1\cup A_2|}$.

Secondly, we determine the size of T_1. Note that $B \subseteq \mathrm{Supp}(\mathbf{b})$ and $\mathrm{Supp}(\mathbf{b}) \cap A_1 = \emptyset$. Then $B \cap A_1 = \emptyset$ and $\mathrm{Supp}(\mathbf{b})^c \cap A_1 = A_1$. It follows from (4) that

$$\begin{aligned}\mathrm{Supp}(\mathbf{a}+\mathbf{b}) \cap A_1 &= \big(\mathrm{Supp}(\mathbf{a}) \cap \mathrm{Supp}(\mathbf{b})^c \cap A_1\big) \cup \big(\mathrm{Supp}(\mathbf{b}) \cap \mathrm{Supp}(\mathbf{a})^c \cap A_1\big) \cup (B \cap A_1) \\ &= (\mathrm{Supp}(\mathbf{a}) \cap A_1) \cup \emptyset \cup \emptyset = \mathrm{Supp}(\mathbf{a}) \cap A_1 \neq \emptyset.\end{aligned}$$

This implies that $\mathrm{Supp}(\mathbf{a}+\mathbf{b})\cap A_1 \neq \emptyset$ and $\mathrm{Supp}(\mathbf{b})\cap A_1 = \emptyset$ if and only if $\mathrm{Supp}(\mathbf{a})\cap A_1 \neq \emptyset$ and $\mathrm{Supp}(\mathbf{b}) \cap A_1 = \emptyset$. Hence, T_1 can be written as

$$T_1 = \{(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_p^m \times \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_2 = \emptyset, \mathrm{Supp}(\mathbf{b}) \cap A_1 = \emptyset, \mathrm{Supp}(\mathbf{a}) \cap A_1 \neq \emptyset\}.$$

It then follows from Lemma 1 that $|T_1| = |S_0| \times |S_{22}| = p^{m-|A_1|}(p^{m-|A_2|} - p^{m-|A_1\cup A_2|})$.

Thirdly, we determine the size of T_2. By (4), we know that

$$\mathrm{Supp}(\mathbf{a}+\mathbf{b})\cap A_1 = \big(\mathrm{Supp}(\mathbf{a})\cap \mathrm{Supp}(\mathbf{b})^c \cap A_1\big) \cup \big(\mathrm{Supp}(\mathbf{b})\cap \mathrm{Supp}(\mathbf{a})^c \cap A_1\big) \cup (B \cap A_1) = \emptyset,$$

which implies that $\mathrm{Supp}(\mathbf{a}) \cap \mathrm{Supp}(\mathbf{b})^c \cap A_1 = \emptyset$, $\mathrm{Supp}(\mathbf{b}) \cap \mathrm{Supp}(\mathbf{a})^c \cap A_1 = \emptyset$ and $B \cap A_1 = \emptyset$. It is easy to verify that $\mathrm{Supp}(\mathbf{a}) \cap A_1 \subseteq \mathrm{Supp}(\mathbf{b})$, $\mathrm{Supp}(\mathbf{b}) \cap A_1 \subseteq \mathrm{Supp}(\mathbf{a})$ and $B \cap A_1 = \emptyset$, which implies that $\mathrm{Supp}(\mathbf{a}) \cap A_1 = \mathrm{Supp}(\mathbf{b}) \cap A_1 \neq \emptyset$ from the condition that $\mathrm{Supp}(\mathbf{b}) \cap A_1 \neq \emptyset$. This together $\mathrm{Supp}(\mathbf{b}) \cap A_2 = \emptyset$ implies that $|\mathrm{Supp}(\mathbf{b}) \cap A_1| = |\mathrm{Supp}(\mathbf{a}) \cap A_1| = i$, where $i = 1, 2, \ldots, |A_1 \backslash A_2|$. On the other hand, since $\mathrm{Supp}(\mathbf{a} + \mathbf{b}) \cap A_1 = \emptyset$, we have $\mathbf{a}_{A_1} + \mathbf{b}_{A_1} = \mathbf{0}$. Once the coordinates of $\mathbf{b}_{A_1}$ are determined, the corresponding coordinates of $\mathbf{a}_{A_1}$ are also determined. Note that $\mathbf{a}_{A_1\backslash(\mathrm{Supp}(\mathbf{a})\cap A_1)} = \mathbf{0}$ and $\mathbf{b}_{A_1\backslash(\mathrm{Supp}(\mathbf{b})\cap A_1)} = \mathbf{0}$. For each $1 \leq i \leq |A_1 \backslash A_2|$, if $|\mathrm{Supp}(\mathbf{b}) \cap A_1| = i$, then there are $(p-1)^i p^{m-|A_1|}\binom{|A_1\backslash A_2|}{i}$ choices for $\mathbf{b}$ and $p^{m-|A_1\cup A_2|}$ choices for $\mathbf{a}$ such that the conditions in T_2 are satisfied. Then

$$|T_2| = \sum_{i=1}^{|A_1\backslash A_2|} \binom{|A_1\backslash A_2|}{i} (p-1)^i p^{m-|A_1|} p^{m-|A_1\cup A_2|} = p^{m-|A_1|}(p^{m-|A_2|} - p^{m-|A_1\cup A_2|}).$$

Note that $\{(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_p^m \times \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_2 = \emptyset, \mathbf{b} \in \mathbb{F}_p^m\} = T_0 \cup T_1 \cup T_2 \cup T_3$. It follows from Lemma 1 (i) that

$$|T_3| = p^{2m-|A_2|} - |T_0| - |T_1| - |T_2| = p^{m-|A_2|}(p^m - 2p^{m-|A_1|}) + p^{2m-|A_1|-|A_1\cup A_2|}.$$

This completes the proof. □

Lemma 3. *Let A_1 and A_2 be two subsets of $[m]$ and let*

$$R_0 = \{(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_p^m \times \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_2 \neq \emptyset, \mathrm{Supp}(\mathbf{b}) \cap A_1 = \emptyset, \mathrm{Supp}(\mathbf{a} + \mathbf{b}) \cap A_1 = \emptyset\},$$
$$R_1 = \{(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_p^m \times \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_2 \neq \emptyset, \mathrm{Supp}(\mathbf{b}) \cap A_1 = \emptyset, \mathrm{Supp}(\mathbf{a} + \mathbf{b}) \cap A_1 \neq \emptyset\},$$
$$R_2 = \{(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_p^m \times \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_2 \neq \emptyset, \mathrm{Supp}(\mathbf{b}) \cap A_1 \neq \emptyset, \mathrm{Supp}(\mathbf{a} + \mathbf{b}) \cap A_1 = \emptyset\},$$

and

$$R_3 = \{(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_p^m \times \mathbb{F}_p^m | \mathrm{Supp}(\mathbf{a}) \cap A_2 \neq \emptyset, \mathrm{Supp}(\mathbf{b}) \cap A_1 \neq \emptyset, \mathrm{Supp}(\mathbf{a} + \mathbf{b}) \cap A_1 \neq \emptyset\}.$$

Then

$$|R_0| = p^{m-|A_1|}(p^{m-|A_1|} - p^{m-|A_1\cup A_2|}),$$
$$|R_1| = |R_2| = p^{m-|A_1|}(p^m - p^{m-|A_2|} - p^{m-|A_1|} + p^{m-|A_1\cup A_2|}),$$

and

$$|R_3| = p^m(p^m - p^{m-|A_2|}) - p^{m-|A_1|}(2p^m - 2p^{m-|A_2|} - p^{m-|A_1|} + p^{m-|A_1\cup A_2|}).$$

Proof. The proof is similar to that of Lemma 2 and is omitted. □

In the following, we always assume that A_1 and A_2 be two nonempty subsets of $[m]$. Let V_{A_1}, V_{A_2} be two subspaces of $\mathbb{F}_p^m$ defined in (3). Let P_{A_2} be the corresponding projective space of V_{A_2}. The following theorem shows that $\mathcal{C}_{K_1}$ has at most four Lee weights, where $K_1 = V_{A_1} + uP_{A_2}$.

Theorem 4. *Let $A_1, A_2 \subseteq [m]$ and $K_1 = V_{A_1} + uP_{A_2} \subseteq \mathrm{R}^m$. Then the code $\mathcal{C}_{K_1}$ is a code with length $\frac{p^{|A_1|}(p^{|A_2|}-1)}{p-1}$ and size $p^{|A_1|+|A_1\cup A_2|}$. The Lee weight distribution of $\mathcal{C}_{K_1}$ is listed in Table 1, where T_i and R_i are given in Lemmas 2 and 3, $i = 0, 1, 2, 3$.*

Table 1: The Lee weight distribution of $\mathcal{C}_{K_1}$ in Theorem 4

Lee weight i	Frequency B_i
0	$\lvert T_0\rvert$
$p^{\lvert A_1\rvert-1}(p^{\lvert A_2\rvert}-1)$	$\lvert T_1\rvert + \lvert T_2\rvert$
$2p^{\lvert A_1\rvert-1}(p^{\lvert A_2\rvert}-1)$	$\lvert T_3\rvert + \lvert R_3\rvert$
$p^{\lvert A_1\rvert-1}(2p^{\lvert A_2\rvert}-1)$	$\lvert R_1\rvert + \lvert R_2\rvert$
$2p^{\lvert A_1\rvert+\lvert A_2\rvert-1}$	$\lvert R_0\rvert$

Proof. It is clear that $|K_1| = \frac{p^{|A_1|}(p^{|A_2|}-1)}{p-1}$, i.e., the length of $\mathcal{C}_{K_1}$ is $\frac{p^{|A_1|}(p^{|A_2|}-1)}{p-1}$.

For $\mathbf{x} = \alpha + u\beta \in \mathrm{R}^m$, where $\alpha \in \mathbb{F}_p^m, \beta \in \mathbb{F}_p^m$, the Lee weight of the codeword $c_{\mathbf{x}}$ of the code $\mathcal{C}_{K_1}$ is given by

$$\begin{aligned}
w_L(c_{\mathbf{x}}) &= w_L((\langle \mathbf{x}, \mathbf{d}\rangle_{\mathrm{R}})_{\mathbf{d}\in K_1}) = w_L\big((\langle \alpha + u\beta, d_1 + ud_2\rangle_{\mathrm{R}})_{d_1\in V_{A_1}, d_2\in P_{A_2}}\big) \\
&= w_L\big((\langle \alpha, d_1\rangle_F + u(\langle \alpha, d_2\rangle_F + \langle \beta, d_1\rangle_F))_{d_1\in V_{A_1}, d_2\in P_{A_2}}\big) \\
&= w_H((\langle \alpha, d_2\rangle_F + \langle \beta, d_1\rangle_F)_{d_1\in V_{A_1}, d_2\in P_{A_2}}) + w_H((\langle \alpha+\beta, d_1\rangle_F + \langle \alpha, d_2\rangle_F)_{d_1\in V_{A_1}, d_2\in P_{A_2}}) \\
&= |K_1| - \frac{1}{p}\sum_{y\in\mathbb{F}_p}\sum_{d_1\in V_{A_1}}\sum_{d_2\in P_{A_2}} \zeta_p^{y(\langle \alpha, d_2\rangle_F + \langle \beta, d_1\rangle_F)} \\
&\quad + |K_1| - \frac{1}{p}\sum_{y\in\mathbb{F}_p}\sum_{d_1\in V_{A_1}}\sum_{d_2\in P_{A_2}} \zeta_p^{y(\langle \alpha+\beta, d_1\rangle_F + \langle \alpha, d_2\rangle_F)} \\
&= 2p^{|A_1|-1}(p^{|A_2|}-1) - \frac{1}{p}\sum_{y\in\mathbb{F}_p^*}\sum_{d_2\in P_{A_2}} \zeta_p^{y\langle \alpha, d_2\rangle_F}\sum_{d_1\in V_{A_1}} \zeta_p^{y\langle \beta, d_1\rangle_F} \\
&\quad - \frac{1}{p}\sum_{y\in\mathbb{F}_p^*}\sum_{d_2\in P_{A_2}} \zeta_p^{y\langle \alpha, d_2\rangle_F}\sum_{d_1\in V_{A_1}} \zeta_p^{y\langle \alpha+\beta, d_1\rangle_F}, \qquad (5)
\end{aligned}$$

where ζ_p is a primitive p-th root of unity. Next we divide the proof into five cases.

Case 1 ($\mathrm{Supp}(\beta) \cap A_1 = \emptyset, \mathrm{Supp}(\alpha+\beta) \cap A_1 = \emptyset, \mathrm{Supp}(\alpha) \cap A_2 = \emptyset$): Note that $\mathrm{Supp}(\beta) = \mathrm{Supp}(y\beta)$ for any $y \in \mathbb{F}_p^*$. It is easy to check that $\sum_{d_1\in V_{A_1}} \zeta_p^{y\langle \beta, d_1\rangle_F} =$

$\sum_{d_1 \in V_{A_1}} \zeta_p^{y(\langle \alpha+\beta, d_1 \rangle_F)} = p^{|A_1|}$ when $\mathrm{Supp}(\beta) \cap A_1 = \emptyset$ and $\mathrm{Supp}(\alpha+\beta) \cap A_1 = \emptyset$. In this case,

$$\begin{aligned} w_L(c_{\mathbf{x}}) &= 2p^{|A_1|-1}(p^{|A_2|}-1) - 2p^{|A_1|-1} \sum_{y \in \mathbb{F}_p^*} \sum_{d_2 \in P_{A_2}} \zeta_p^{y(\langle \alpha, d_2 \rangle_F)} \\ &= 2p^{|A_1|-1}(p^{|A_2|}-1) - 2p^{|A_1|-1} \sum_{d_2' \in V_{A_2}^*} \zeta_p^{\langle \alpha, d_2' \rangle_F} \\ &= 2p^{|A_1|-1}(p^{|A_2|}-1) - 2p^{|A_1|-1}(p^{|A_2|}-1) = 0 \end{aligned}$$

due to $\mathrm{Supp}(\alpha) \cap A_2 = \emptyset$ and the fact that $V_{A_2} \backslash \{\mathbf{0}\} = \bigcup_{y \in \mathbb{F}_p^*} cP_{A_2}$. It follows from Lemma 2 that the number of $\mathbf{x}$ with $w_L(c_{\mathbf{x}}) = 0$ is $|T_0|$.

Case 2 ($\mathrm{Supp}(\beta) \cap A_1 = \emptyset, \mathrm{Supp}(\alpha+\beta) \cap A_1 = \emptyset, \mathrm{Supp}(\alpha) \cap A_2 \neq \emptyset$): Similarly,

$$\sum_{d_1 \in V_{A_1}} \zeta_p^{y(\langle \beta, d_1 \rangle_F)} = \sum_{d_1 \in V_{A_1}} \zeta_p^{y(\langle \alpha+\beta, d_1 \rangle_F)} = p^{|A_1|}$$

when $\mathrm{Supp}(\beta) \cap A_1 = \emptyset$ and $\mathrm{Supp}(\alpha+\beta) \cap A_1 = \emptyset$. In this case, by (5), we have $w_L(c_{\mathbf{x}}) = 2p^{|A_1|+|A_2|-1}$ when $\mathrm{Supp}(\alpha) \cap A_2 \neq \emptyset$. It follows from Lemma 3 that the number of $\mathbf{x}$ with $w_L(c_{\mathbf{x}}) = 2p^{|A_1|+|A_2|-1}$ is $|R_0|$.

Case 3 ($\mathrm{Supp}(\beta) \cap A_1 = \emptyset, \mathrm{Supp}(\alpha+\beta) \cap A_1 \neq \emptyset, \mathrm{Supp}(\alpha) \cap A_2 = \emptyset$) or ($\mathrm{Supp}(\beta) \cap A_1 \neq \emptyset, \mathrm{Supp}(\alpha+\beta) \cap A_1 = \emptyset, \mathrm{Supp}(\alpha) \cap A_2 = \emptyset$): Note that

$$\sum_{d_1 \in V_{A_1}} \zeta_p^{y(\langle \beta, d_1 \rangle_F)} = 0 \qquad \text{or} \qquad \sum_{d_1 \in V_{A_1}} \zeta_p^{y(\langle \alpha+\beta, d_1 \rangle_F)} = p^{|A_1|}$$

when $\mathrm{Supp}(\beta) \cap A_1 \neq \emptyset$ or $\mathrm{Supp}(\alpha+\beta) \cap A_1 \neq \emptyset$. In this case, we have $w_L(c_{\mathbf{x}}) = p^{|A_1|-1}(p^{|A_2|}-1)$ when $\mathrm{Supp}(\alpha) \cap A_2 = \emptyset$ from (5). It follows from Lemma 2 that the number of $\mathbf{x}$ with $w_L(c_{\mathbf{x}}) = p^{|A_1|-1}(p^{|A_2|}-1)$ is $|T_1| + |T_2|$.

Case 4 ($\mathrm{Supp}(\beta) \cap A_1 = \emptyset, \mathrm{Supp}(\alpha+\beta) \cap A_1 \neq \emptyset, \mathrm{Supp}(\alpha) \cap A_2 \neq \emptyset$) or ($\mathrm{Supp}(\beta) \cap A_1 \neq \emptyset, \mathrm{Supp}(\alpha+\beta) \cap A_1 = \emptyset, \mathrm{Supp}(\alpha) \cap A_2 \neq \emptyset$): By a way similar to the one used in the Case 3, we have $w_L(c_{\mathbf{x}}) = p^{|A_1|-1}(2p^{|A_2|}-1)$ when $\mathrm{Supp}(\alpha) \cap A_2 \neq \emptyset$ from (5). By Lemma 3, the number of $\mathbf{x}$ with $w_L(c_{\mathbf{x}}) = p^{|A_1|-1}(2p^{|A_2|}-1)$ is $|R_1| + |R_2|$.

Case 5 ($\mathrm{Supp}(\beta) \cap A_1 \neq \emptyset, \mathrm{Supp}(\alpha+\beta) \cap A_1 \neq \emptyset, \mathrm{Supp}(\alpha) \cap A_2 = \emptyset$) or ($\mathrm{Supp}(\beta) \cap A_1 \neq \emptyset, \mathrm{Supp}(\alpha+\beta) \cap A_1 \neq \emptyset, \mathrm{Supp}(\alpha) \cap A_2 \neq \emptyset$): It is clear that

$$\sum_{d_1 \in V_{A_1}} \zeta_p^{y(\langle \beta, d_1 \rangle_F)} = \sum_{d_1 \in V_{A_1}} \zeta_p^{y(\langle \alpha+\beta, d_1 \rangle_F)} = 0$$

when $\mathrm{Supp}(\beta) \cap A_1 \neq \emptyset$ and $\mathrm{Supp}(\alpha+\beta) \cap A_1 \neq \emptyset$. In this case, $w_L(c_{\mathbf{x}}) = 2p^{|A_1|-1}(p^{|A_2|}-1)$ and the number of $\mathbf{x}$ with $w_L(c_{\mathbf{x}}) = 2p^{|A_1|-1}(p^{|A_2|}-1)$ is $|T_3| + |R_3|$.

To determine the dimension of $\mathcal{C}_{K_1}$,we define a mapping

$$\tau : \mathrm{R}^m \to \mathcal{C}_{K_1}, \mathbf{x} \mapsto \mathbf{c}_{\mathbf{x}}.$$

It is easy to check that τ is an epimorphism from R^m to $\mathcal{C}_{K_1}$. By the homomorphism theorem, $\mathcal{C}_{K_1}$ is isomorphic to $\mathrm{R}^m/\mathrm{Ker}\tau$, where $\mathrm{Ker}\tau = \{\mathbf{x} \in \mathcal{C}_{K_1} | \mathbf{c}_{\mathbf{x}} = \mathbf{0}\}$. Hence, the size of $\mathcal{C}_{K_1}$ is $\frac{p^{2m}}{|T_0|} = p^{|A_1|+|A_1 \cup A_2|}$.

This completes the proof. □

If we choose some special subsets A_1,A_2 of $[m]$, then C_{K_1} has three or two Lee weights.

Corollary 5. *Let $A_1, A_2 \subseteq [m]$ with $A_1 \subset A_2$. Then $\mathcal{C}_{K_1}$ is a three-Lee-weight code with length $\frac{p^{|A_1|}(p^{|A_2|}-1)}{p-1}$ and size $p^{|A_1|+|A_2|}$, and the Lee weight distribution of $\mathcal{C}_{K_1}$ is listed in Table 2, where T_i $(i = 0, 3)$ and R_i $(i = 0, 1, 2, 3)$ are given in Lemmas 2 and 3.*

Table 2: The Lee weight distribution of $\mathcal{C}_{K_1}$ in Corollary 5

Lee weight i	Frequency B_i
0	$\lvert T_0\rvert$
$2p^{\lvert A_1\rvert-1}(p^{\lvert A_2\rvert}-1)$	$\lvert T_3\rvert + \lvert R_3\rvert$
$p^{\lvert A_1\rvert-1}(2p^{\lvert A_2\rvert}-1)$	$\lvert R_1\rvert + \lvert R_2\rvert$
$2p^{\lvert A_1\rvert+\lvert A_2\rvert-1}$	$\lvert R_0\rvert$

Proof. It is easy to check that $|T_1| = |T_2| = p^{m-|A_1|}(p^{m-|A_2|} - p^{m-|A_1\cup A_2|}) = 0$ when $A_1 \subset A_2$. Then the conclusion follows from Theorem 4. □

The next corollary follows immediately when $A_1 = A_2$.

Corollary 6. *Let $A_1 = A_2$. Then the code $\mathcal{C}_{K_1}$ is a two-Lee-weight code with length $\frac{p^{|A_1|}(p^{|A_1|}-1)}{p-1}$ and size $p^{2|A_1|}$, and the Lee weight distribution of $\mathcal{C}_{K_1}$ is listed in Table 3, where T_i $(i = 0, 3)$ and R_i $(i = 1, 2, 3)$ are given in Lemmas 2 and 3.*

Table 3: The Lee weight distribution of $\mathcal{C}_{K_1}$ in Corollary 6

Lee weight i	Frequency B_i
0	$\lvert T_0\rvert$
$2p^{\lvert A_1\rvert-1}(p^{\lvert A_2\rvert}-1)$	$\lvert T_3\rvert + \lvert R_3\rvert$
$p^{\lvert A_1\rvert-1}(2p^{\lvert A_2\rvert}-1)$	$\lvert R_1\rvert + \lvert R_2\rvert$

In the following theorem, we determine the Lee weight distributions of the code $\mathcal{C}_{K_2}$, where $K_2 = P_{A_1} + uV_{A_2}$.

Theorem 7. *Let $A_1, A_2 \subseteq [m]$ and $K_2 = P_{A_1} + uV_{A_2} \subseteq \mathrm{R}^m$. Then the code $\mathcal{C}_{K_2}$ is a three-Lee-weight code with length $\frac{p^{|A_2|}(p^{|A_1|}-1)}{p-1}$ and size $p^{|A_1|+|A_1\cup A_2|}$. The Lee weight distribution of $\mathcal{C}_{K_2}$ is listed in Table 4, where T_i and R_i are given in Lemmas 2 and 3, $i = 0, 1, 2, 3$.*

Proof. The proof is similar to that of Theorem 4 and is omitted. □

Corollary 8. *Let $A_1, A_2 \subseteq [m]$ with $A_1 \subseteq A_2$. Then $\mathcal{C}_{K_2}$ is a two-Lee-weight code with length $\frac{p^{|A_2|}(p^{|A_1|}-1)}{p-1}$ and size $p^{|A_1|+|A_2|}$. Moreover, the Lee weight distribution of $\mathcal{C}_{K_2}$ is listed in Table 5, where T_i $(i = 0, 3)$ and R_i $(i = 0, 1, 2, 3)$ are given in Lemmas 2 and 3.*

Table 4: The Lee weight distribution of $\mathcal{C}_{K_2}$ in Theorem 7

Lee weight i	Frequency B_i
0	$\lvert T_0\rvert$
$p^{\lvert A_1\rvert+\lvert A_2\rvert-1}$	$\lvert T_1\rvert+\lvert T_2\rvert$
$2p^{\lvert A_2\rvert-1}(p^{\lvert A_1\rvert}-1)$	$\lvert R_0\rvert+\lvert R_1\rvert+\lvert R_2\rvert+\lvert R_3\rvert$
$2p^{\lvert A_1\rvert+\lvert A_2\rvert-1}$	$\lvert T_3\rvert$

Table 5: The Lee weight distribution of $\mathcal{C}_{K_2}$ in Corollary 8

Lee weight i	Frequency B_i
0	$\lvert T_0\rvert$
$2p^{\lvert A_2\rvert-1}(p^{\lvert A_1\rvert}-1)$	$\lvert R_0\rvert+\lvert R_1\rvert+\lvert R_2\rvert+\lvert R_3\rvert$
$2p^{\lvert A_1\rvert+\lvert A_2\rvert-1}$	$\lvert T_3\rvert$

4 Some optimal linear codes from the image of the codes $\mathcal{C}_{K_1}$ and $\mathcal{C}_{K_2}$ under Gray map

In this section, we show that the image of the codes $\mathcal{C}_{K_1}$ and $\mathcal{C}_{K_2}$ under Gray map have few weights over $\mathbb{F}_p$ and obtain some optimal codes in some case.

Theorem 9. *Let the symbols be the same as those in Corollary 5. Then $\phi(\mathcal{C}_{K_1})$ is a three-weight code over $\mathbb{F}_p$ with parameters $[\frac{2p^{|A_1|}(p^{|A_2|}-1)}{p-1}, |A_1|+|A_2|, 2p^{|A_1|-1}(p^{|A_2|}-1)]$ and the weight enumerator*

$$1+\frac{|T_3|+|R_3|}{|T_0|}z^{2p^{|A_1|-1}(p^{|A_2|}-1)}+\frac{|R_1|+|R_2|}{T_0}z^{p^{|A_1|-1}(2p^{|A_2|}-1)}+\frac{|R_0|}{|T_0|}z^{2p^{|A_1|+|A_2|-1}},$$

where T_i $(i=0,3)$ and R_i $(i=0,1,2,3)$ are given in Lemmas 2 and 3. Furthermore, $\phi(\mathcal{C}_{K_1})$ is optimal with respect to the Griesmer bound.

Proof. By the Gray map, we can get the weight distribution of $\phi(\mathcal{C}_{K_1})$ from the Lee weight distribution of $\mathcal{C}_{K_1}$ in Corollary 5. We now show that $\phi(\mathcal{C}_{K_1})$ is optimal with respect to the Griesmer bound. Note that $\phi(\mathcal{C}_{K_1})$ is a p-ary code with parameters $[\frac{2p^{|A_1|}(p^{|A_2|}-1)}{p-1}, |A_1|+|A_2|, 2p^{|A_1|-1}(p^{|A_2|}-1)]$. Then we have

$$\begin{aligned}
&\sum_{i=0}^{|A_1|+|A_2|-1}\left\lceil\frac{2p^{|A_1|-1}(p^{|A_2|}-1)}{p^i}\right\rceil\\
&=\sum_{i=0}^{|A_1|-1}\left\lceil\frac{2p^{|A_1|-1}(p^{|A_2|}-1)}{p^i}\right\rceil+\sum_{i=|A_1|}^{|A_1|+|A_2|-1}\left\lceil\frac{2p^{|A_1|-1}(p^{|A_2|}-1)}{p^i}\right\rceil\\
&=2p^{|A_1|-1}(p^{|A_2|}-1)+2p^{|A_1|-2}(p^{|A_2|}-1)+\cdots+2(p^{|A_2|}-1)+2p^{|A_2|-1}+2p^{|A_2|-2}+\cdots+2\\
&=2\frac{p^{|A_1|}-1}{p-1}(p^{|A_2|}-1)+2\frac{p^{|A_2|}-1}{p-1}=2p^{|A_1|}(\frac{p^{|A_2|}-1}{p-1}).
\end{aligned}$$

Hence, $\phi(\mathcal{C}_{K_1})$ is optimal with respect to the Griesmer bound. □

Corollary 10. *Let the symbols be the same as those in Corollary 6. Then $\phi(\mathcal{C}_{K_1})$ is a two-weight code over $\mathbb{F}_p$ with parameters $[\frac{2p^{|A_1|}(p^{|A_1|}-1)}{p-1}, 2|A_1|, 2p^{|A_1|-1}(p^{|A_1|}-1)]$ and the weight enumerator*

$$1+\frac{|T_3|+|R_3|}{|T_0|}z^{2p^{|A_1|-1}(p^{|A_1|}-1)}+\frac{|R_1|+|R_2|}{|T_0|}z^{p^{|A_1|-1}(2p^{|A_1|}-1)},$$

where T_i $(i=0,3)$ and R_i $(i=1,2,3)$ are given in Lemmas 2 and 3. Furthermore, $\phi(\mathcal{C}_{K_1})$ is optimal with respect to the Griesmer bound.

By the Gray map, we obtain the following class of two-weight optimal linear codes over $\mathbb{F}_p$.

Theorem 11. *Let the symbols be the same as those in Corollary 8. Then $\phi(\mathcal{C}_{K_2})$ is a two-weight linear code over $\mathbb{F}_p$ with parameters $[\frac{2p^{|A_2|}(p^{|A_1|}-1)}{p-1}, |A_1|+|A_2|, 2p^{|A_2|-1}(p^{|A_1|}-1)]$ and the weight enumerator*

$$1+\frac{|R_0|+|R_1|+|R_2|+|R_3|}{|T_0|}z^{2p^{|A_2|-1}(p^{|A_1|}-1)}+\frac{|T_3|}{|T_0|}z^{2p^{|A_1|+|A_2|-1}},$$

where T_i $(i=0,3)$ and R_i $(i=0,1,2,3)$ are given in Lemmas 2 and 3. Furthermore, $\phi(\mathcal{C}_{K_2})$ is optimal with respect to the Griesmer bound.

Remark 12. (i) It should be noted that these two codes in Corollary 10 and Theorem 11 have different weight distribution. Hence, they are inequivalent to each other even if they have the same parameters when $A_1 = A_2$. (ii) The parameters and weight distributions of our optimal codes are closely related to subsets A_1 and A_2 of $[m]$. It is believed that our construction can produce some optimal codes with flexible and new parameters. Furthermore, we did not find optimal codes equivalent to our optimal linear codes in these references [6, 9, 7, 11, 14, 18].

5 Concluding remarks

In this paper, we presented two classes of linear codes $\mathcal{C}_{K_1}$ and $\mathcal{C}_{K_2}$ over $\mathbb{F}_p + u\mathbb{F}_p$ from projective spaces, where $K_1 = V_{A_1} + uP_{A_2}$ and $K_2 = P_{A_1} + uV_{A_2}$. By investigating the property of the vectors of $\mathbb{F}_p^m$, we determined the Lee weight distribution of these linear codes. We obtained some p-ary optimal linear codes from the Gray image of the codes $\mathcal{C}_{K_1}$ and $\mathcal{C}_{K_2}$.

References

[1] S. Chang, J. Y. Hyun. Linear codes from simplicial complexes, Des. Codes Cryptogr., 86: 2167– 2181, 2018.

[2] C. Ding, H. Niederreiter. Cyclotomic linear codes of order 3. IEEE Trans. Inform. Theory, 53 (6): 2274-2277, 2007.

[3] J. H. Griesmer, A bound for error-correcting codes, IBM J. Res., 4(5): 532-542, 1960.

[4] W. C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[5] J. Y. Hyun, J. Lee, Y. Lee. Infinite families of optimal linear codes constructed from simplicial complexes. IEEE Trans. Inf. Theory, 66(11): 6762-6773, 2020.

[6] J. Y. Hyun, H. K. Kim, M. Na. Optimal non-projective linear codes constructed from down-sets. Discret. Appl. Math., 254: 135-145, 2019.

[7] G. Luo, X. Cao, G. Xu, S. Xu. A new class of optimal linear codes with flexible parameters. Discret. Appl. Math., 237: 126-131, 2018.

[8] G. Luo, S. Ling. Application of optimal p-ary linear codes to alphabet-optimal locally repairable codes. Des. Codes Cryptogr., 90: 1271-1287 2022.

[9] H. Liu, Y. Maouche. Two or few-weight trace codes over $\mathbb{F}_q + u\mathbb{F}_q$. IEEE Trans. Inf. Theory, 65(5): 2696-2703, 2019.

[10] M. Shi ,Y. Liu, P. Solé. Optimal two-weight codes from trace codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE Commun. Lett., 20(12): 2346-2349, 2016.

[11] M. Shi, R. Wu, Y. Liu, P. Solé. Two and three weight codes over $\mathbb{F}_p + u\mathbb{F}_p$. Cryptogr. Commun., 9(5): 637-646, 2017.

[12] M. Shi, Y. Guan, P. Solé. Two new families of two-weight codes. IEEE Trans. Inf. Theory, 63(10): 6240-6246, 2017.

[13] M. Shi, R. Wu, L. Qian, S. Lin, P. Solé. New classes of p-ary few weights codes. Bull. Malays. Math. Sci. Soc., 42(4): 1393-1412, 2019.

[14] M. Shi, X. Li. Two classes of optimal p-ary few-weight codes from down-sets. Discrete Appl. Math., 290:60-67,2021.

[15] G. Solomon, J.J. Stiffler. Algebraically punctured cyclic codes. Inform. Control, 8(2): 170-179, 1965.

[16] Y. Wu, X. Zhu, Q. Yue. Optimal few-weight codes from simplicial complexes. IEEE Trans. Inf. Theory, 66(6): 3657-3663, 2020.

[17] Y. Wu, Y. Lee. Binary LCD and self-orthogonal codes via simplicial complexes. IEEE Commun. Lett., 24(6): 1159-1162, 2020.

[18] Y. Wu, J. Y. Hyun. Few-weight codes over $\mathbb{F}_p + u\mathbb{F}_p$ associated with down sets and their distance optimal Gray image. Discrete Appl. Math., 283: 315-322, 2020.

Filtering Modified de Bruijn Sequences with Designated Linear Complexity

Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
ggong@uwaterloo.ca

Kalikinkar Mandal
Faculty of Computer Science
University of New Brunswick
Fredericton, NB, E3B 5A3
kmandal@unb.ca

Abstract

In this preliminary work, we study the construction of filtering modified de Bruijn sequence generators and the linear complexity/span of filtering modified de Bruijn sequences. We study two filtering generator constructions consisting of an NLFSR that generates a modified de Bruijn sequence and a filtering function. In our first construction, the filtering function is based on an LFSR that can be selected so that the filtering sequence can have a chosen attainable linear complexity. Moreover, for a proper choice of an LFSR feedback, the filtering sequence can be another modified de Bruijn sequence with a minimum linear complexity. For our second filtering generator, we present some properties of the filtering functions and experimentally study the filtering functions and the linear span of corresponding filtering modified de Bruijn sequences. Our results show that the filtering function does not always guarantee the high linear complexity of a filtering sequence even when the modified de Bruijn sequence generated by the NLFSR has an optimal linear complexity.

1 Introduction

Pseudorandom sequence or number generators (PRSGs/PRNGs) are at the heart of modern stream cipher constructions (e.g., Grain [16], Trivium [6], SNOW-3/V [8], and ZUC [33]). Feedback shift registers (FSRs) provide an efficient mechanism to generate pseudorandom sequences. There are two types of FSRs, namely linear feedback shift register (LFSR) and nonlinear feedback shift register (NLFSR). The preferred randomness properties of a pseudorandom sequence are long period, balance, equal distribution of tuples, 2-level autocorrelation, low crosscorrelation and high linear span [4, 13, 30]. Well-known binary sequences are maximum length sequences (in short, m-sequences), de Bruijn sequences and modified de Bruijn sequences. De Bruijn and modified de Bruijn sequences have known randomness properties such as long period, balancedness, ideal tuple distribution and high linear complexity [25, 26, 27, 3], and can also be generated by NLFSRs with a minimal storage/length.

A binary de Bruijn sequence is a sequence of period 2^n where each n-tuple occurs exactly once in one period of the sequence. A *modified de Bruijn* sequence is a pseudorandom sequence with period $2^n - 1$ where each *nonzero* n-tuple occurs exactly once in one period of the sequence. A modified de Bruijn sequence is also called a *span* n sequence. m-sequences are a class of span n sequences that can be generated by LFSRs. We interchangeably use the terms modified de Bruijn sequence and span n sequence. The total number of binary de Bruijn sequences of period 2^n (also modified de Bruijn of period $2^n - 1$) is $2^{2^{n-1}-n}$ [5].

There is a one-to-one correspondence between a de Bruijn sequence and a modified de Bruijn sequence, which is as follows. A span n sequence can be constructed from a de Bruijn sequence by removing one zero from the run of zeros of length n, and similarly, a de Bruijn sequence can be formed from a span n sequence by adding one zero to the run of zeros of length $n-1$. From a security point of view, the linear span or linear complexity is an unpredictability property of a sequence. However, the stability of the linear span is crucial. As mentioned in [14], by adding one zero to the run of zeros of length $n-1$ to an m-sequence, the linear span of the resultant de Bruijn sequence becomes high, which varies between $2^{n-1}+n$ and 2^n-1. But, after removing any one zero from the run of zeros of length n from the resultant de Bruijn sequence, it becomes an m-sequence or span n sequence with linear span n. This example suggests to study the linear span property of a modified de Bruijn sequence, instead of de Bruijn sequences, for their use in cryptographic applications such as designing stream ciphers and PRNGs.

There is a large volume of works in the literature that broadly focus on (i) searching de Bruijn sequences and modified de Bruijn sequences by an exhaustive search, e.g., in [20, 7, 31]; (ii) constructions of de Bruijn sequences and modified de Bruijn sequences, for example, by joining two or more cycles using conjugates, e.g., in [10, 29, 17, 18, 28, 19, 23, 1]; and (iii) studying statistical and randomness properties such as linear span of de Bruijn sequences and modified de Bruijn sequences, e.g., in [3, 9, 23, 25, 26, 11]. Till today, except for the m-sequences, the linear span n distribution of NLFSR generated span n sequences is unknown. The works in [22, 21] study the constructions of filtering de Bruijn generators with proven tuple distribution properties.

A classical filtering generator consists of an LFSR and a filtering function where the filtering function is chosen to improve the security properties of the filtering sequence or keystream, including the linear span. For an LFSR-based filtering generator, an upper bound of the linear span of the filtering sequence is proved [32]. For LFSR-based filtering generators, existing literature has focused on improving the security of the filtering sequences with a suitable cryptographic filtering function with properties such as high algebraic degree, algebraic immunity and nonlinearity.

An intuitive methodology to design a secure PRNG or stream cipher is to choose all components with best cryptographic properties. When constructing a PRNG or stream cipher using an NLFSR, although a modified de Bruijn sequence could have a large linear span, it cannot be directly used as a keystream generator, otherwise, the internal state will be output. So a filter function or a finite state machine function needs to be employed to the internal state and the keystream will be the output of this function. In this way, the internal state is masked.

In this work, we consider a generalized filtering generator in which we replace the LFSR by an NLFSR generating a modified de Bruijn sequence and require the filtering sequence to be a modified de Bruijn sequence. We call such generator a *modified de Bruijn or span n generator*. As various randomness properties such as long period, balanceness, and equal distribution of tuples in a modified de Bruijn sequence are inherently offered, our focus is to study the linear span of a filtering modified de Bruijn generator. We ask the following question:

When the linear span of the underlying modified de Bruijn sequence generated by an NLFSR is high, can the filtering function always preserve the high linear span of the filtering sequence?

Unfortunately, our study shows that it is possible that the linear span of filtered modified de Bruijn (MDB) sequences could be dropped, even dropped to the minimum linear span n, i.e., the output filtered modified de Bruijn sequence could be an m-sequence with linear span n. As mentioned above, the main motivation behind studying this question that the filtering functions used an NLFSR-based filtering generator are well-chosen to meet cryptographic requirements.

We present two constructions of filtering modified de Bruijn sequence generators consisting of an NLFSR that generates a modified de Bruijn sequence and a filtering function. For our first construction, we consider an LFSR as a filter function that is chosen in such a way that the filtering sequence can have a chosen attainable linear span. We show another construction of an LFSR for which the output filtering sequence is also a modified de Bruijn sequence with the minimum linear span (i.e., an m-sequence). Our second filtering modified de Bruijn generator consists of an NLFSR and a nonlinear filtering function. We experimentally study the filtering functions and the linear span of filtering modified de Bruijn sequences. Our results show that there exist nonlinear filtering functions that could drop the linear span of the filtering modified de Bruijn sequences.

2 Basic concepts and properties of binary modified de Bruijn sequences

In this section, we first define some notations, basic definitions and properties of de Bruijn or modified de Bruijn n sequences.

Notations. We will use the following notations throughout the paper.

- $\mathbb{F}_2 = \{0, 1\}$ is the Galois field with two elements.
- $\mathbb{F}_{2^n}$ is a finite field of size 2^n defined by a primitive element α that is the root of the primitive polynomial $p(x) = \sum_{i=0}^{n-1} c_i x^{n-1} + x^n, c_i \in \mathbb{F}_2$.
- $\mathrm{tr}_1^m(x) = x + x^2 + x^{2^2} + \cdots x^{2^{m-1}}$ is the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$.
- $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ denotes the residue ring modulo N
- $\mathbb{F}_2^n = \{(x_0, \cdots, x_{n-1}) \,|\, x_i \in \mathbb{F}_2\}$

2.1 Nonlinear feedback shift register sequences

Let $f(x_0, \cdots, x_{n-1})$ be a feedback function defined from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Let $\mathbf{s} = \{s_i\}$, $s_i \in \mathbb{F}_2$ be a binary sequence generated by f as

$$s_{n+i} = f(s_i, s_{i+1}, \cdots, s_{i+n-1}), i = 0, 1, 2, \cdots .$$

Figure 1 shows a block diagram of the feedback shift register sequence generation. If f is a linear function, then $\mathbf{s}$ is referred to as a linear feedback shift register (LFSR) sequence, otherwise, it is called a nonlinear feedback shift register (NLFSR) sequence. The sequence $\mathbf{s}$ is periodic if and only if the feedback function has the following form $f(x_0, \cdots, x_{n-1}) = x_0 + g(x_1, \cdots, x_{n-1})$ where g is defined from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2$ [12]. In this work, we consider only periodic sequences of period $2^n - 1$ or 2^n. The randomness properties of LFSR sequences are well-understood, see Golomb and Gong's book [13].

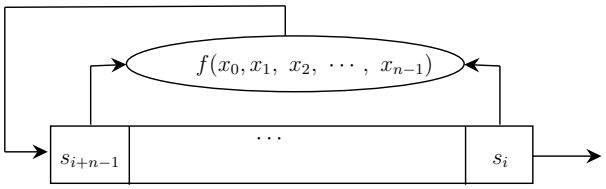


Figure 1: A diagram of an n-stage feeback shift register sequence generation.

Definition 1 (De Bruijn sequence)**.** An NLFSR sequence $\mathbf{s} = \{s_i\}$ over $\mathbb{F}_2$ is called a *de Bruijn* (DB) sequence of order or stage n if the period of $\mathbf{s}$ is 2^n where every n-tuple occurs exactly once in one period.

Definition 2 (Modified de Bruijn or span $\boldsymbol{n}$ sequence)**.** An NLFSR sequence $\mathbf{s} = \{s_i\}$ over $\mathbb{F}_2$ is called a *modified de Bruijn* or *span* n sequence of order n if the period of $\mathbf{s}$ is $2^n - 1$ where every nonzero n-tuple occurs exactly once in one period.

The *linear span or linear complexity* of a sequence is the length of the shortest LFSR that produces the sequence. We also use these two terms interchangeably. The Berlekamp-Massey algorithm can be used to compute the shortest LFSR given a sequence [24].

Property 3. The linear span of a de Bruijn sequence, denoted as LS_{db}, is bounded by $2^{n-1} + n \leq \mathsf{LS}_{db} \leq 2^n - 1$ [3]. On the other hand, the linear span of a span n sequence, denoted as LS_s, is bounded by $n \leq \mathsf{LS}_s \leq 2^n - 2$ [25].

From this property, we call that a span n sequence has the optimal linear span if its linear span is equal to $2^n - 2$.

2.2 Basic properties of binary modified de Bruijn sequences

Sequence and function representations. As our focus is on span n sequences, we recall some properties, more specifically, the trace representation of sequences with period $2^n - 1$ in the following lemma.

Lemma 4. *[13] For a binary sequence* $\mathbf{u} = (u_0, \cdots, u_{2^n-2})$ *of period* $2^n - 1$*, it has the following trace representation:*

$$f(x) = \sum_{r \in I} Tr_1^{n_r}(\gamma_r x^r), \gamma_r \in \mathbb{F}_{2^{n_r}}, \text{ with } u_i = f(\alpha^i), 0 \le i < 2^n - 2 \tag{1}$$

where α *is a primitive element in* $\mathbb{F}_{2^n}$*,* I *is the set consisting of all coset leaders modulo* $2^n - 1$ *and* $Tr_1^{n_r}(x) = x + x^2 + \cdots + x^{2^{n_r-1}}$ *where* $n_r \mid n$*.*

Theorem 5. *(Sequence version) For any binary sequence of period* $2^n - 1$ *generated by a nonlinear feedback shift register of* n *stages, say* $\{a_i\}$*, with linear span* $> n$*, there exists a filtering function* $h(x_0, \cdots, x_{n-1})$ *such that*

$$z_i = h(a_i, a_{i+1}, \cdots, a_{i+n-1}), i = 0, 1, \cdots, 2^n - 2$$

which is a sequence generated by an n*-stage LFSR. In other words, the filtering sequence* $\{z_i\}$ *has linear span* n*, which is the minimum of the linear span of a binary sequence with period* $2^n - 1$*.*

This result is rather surprising at the first glance, since intuitively, we may consider that linear span of filtering sequences should not be decreased. However, the result is contrary. It can decrease to the minimum value of any binary sequence with period $2^n - 1$.

We can have the function version of Theorem 5.

Theorem 6. *(Function version) Let* α *be a primitive element of* $\mathbb{F}_{2^n}$*,* I *be the set consisting of the coset leaders modulo* $2^n - 1$*, and* f *is a mapping from* $\mathbb{F}_{2^n}$ *to* $\mathbb{F}_2$ *with the following univariate polynomial representation*

$$f(x) = \sum_{r \in I} Tr_1^{n_r}(\gamma_r x^r), \gamma_r \in \mathbb{F}_{2^{n_r}}, \tag{2}$$

where at least one of r *satisfies* $n_r = n$ *and* $\gamma_r \neq 0$ *and* $a_i = f(\alpha^i), 0 \le i \le 2^n - 2$*. Then, there exists a function* h *from* $\mathbb{F}_2^n$ *to* $\mathbb{F}_2$ *such that*

$$h((f(x), f(\alpha x), \cdots, f(\alpha^{n-1}x)) = Tr(\beta x^t), \beta \in \mathbb{F}_{2^n}.$$

Discrete Fourier transformation. Let $\mathbf{a} = \{a_i\}$ be a binary sequence of period $N = 2^n - 1$. The Discrete Fourier Transform (DFT) of $\mathbf{s}$ is defined as

$$A_i = \sum_{j=0}^{N} a_i \alpha^{-ij}, i = 0, 1, \cdots, N-1$$

where α is the primitive element of $\mathbb{F}_{2^n}$. The sequence $\mathbf{A} = \{A_i\}$ is called a spectral sequence of $\mathbf{a}$ which is over $\mathbb{F}_{2^n}$. The Inverse Discrete Fourier Transform (IDFT) of $\mathbf{A} = \{A_i\}$ is defined by

$$a_i = \sum_{j=0}^{N} A_i \alpha^{ij}, i = 0, 1, \cdots, N-1$$

where α is the primitive element of $\mathbb{F}_{2^n}$. If we write the spectral sequence $\mathbf{A}$ as a polynomial $A(x) = \sum_{j=0}^{N-1} A_j x^j, A_j \in \mathbb{F}_{2^n}$, then the original sequence can be written as $a_i = A(\alpha^i), i = 0, 1, 2, \cdots, N-1$. According to Blahut's theorem [2], the linear span of $\mathbf{a}$ is the number of non-zero terms in the spectral sequence $\mathbf{A} = \{A_i\}$. The polynomial $A(x)$ can also be written in terms of the trace function, as shown in Fact 7.

Fact 7 (Trace representation from DFT)**.** *[14] The polynomial $A(x)$ can be written as*

$$A(x) = \sum_{i \in I} tr_1^{n_i}(A_i x^i)$$

where i is the cyclotomic coset leaders modulo N, $n_i | n$ is the number of elements in the coset for the cost leader i, and $tr_1^{n_i}(x)$ is the trace function from $\mathbb{F}_{2^{n_i}}$ to $\mathbb{F}_2$.

3 New Constructions

In this section, we present the constructions of new filtering generators based on a span n sequence and filtering functions. We study the linear span of the filtering sequences.

3.1 New filtering construction with designated linear complexity

Let $\mathbf{s} = \{s_i\} = (s_0, s_1, \cdots, s_{2^n-2})$ be a span n sequence of period $N = 2^n - 1$, generated by an NLFSR with a feedback function $f(x_0, x_1, \cdots, x_{n-1})$ as follows:

$$s_{n+i} = f(s_i, s_{i+1}, \cdots, s_{i+n-1}), i = 0, 1, \cdots.$$

Let $S_i = (s_i, s_{i+1}, s_{i+2}, \cdots, s_{i+n-1})$ be the i-th state of the NLFSR. Suppose $q(x) = \sum_{i=0}^{L} q_i x^i, q_i \in \mathbb{F}_2$ be a polynomial of degree L over $\mathbb{F}_2$. We construct a sequence $\mathbf{v} = \{v_i\}$ as

$$v_i = \sum_{j=0}^{L} q_i s_{i+j}, i = 0, 1, \cdots, N-1.$$

When the index $(i+j)$ exceeds N, a modulo N operation is applied. The construction of the sequence $\mathbf{v}$ can be viewed as applying an LFSR filter with the connection polynomial $q(x)$ to the span n sequence $\mathbf{s}$. Figure 2 shows a high-level overview of this generator.

In Figure 2, computing v_i can be viewed as an *expansion-then-compression* operation where the NLFSR expands the state S_i to a sequence $(s_i, s_{i+1}, s_{i+2}, \cdots, s_{i+L})$ of length $L+1$ using the nonlinear feedback function f, and then the LFSR takes the sequence as an input to its state and compresses it to a single bit v_i, which is the LFSR feedback computation. One can also view the process of computing the filtering sequence using an LFSR of length L as applying a filtering function on the internal state of the NLFSR S_i. Mathematically, this process can be written as

$$v_i = h(S_i) = h(s_i, s_{i+1}, s_{i+2}, \cdots, s_{i+n-1}), i = 0, 1, 2, \cdots, 2^n - 2,$$

for some Boolean function h in n variables.

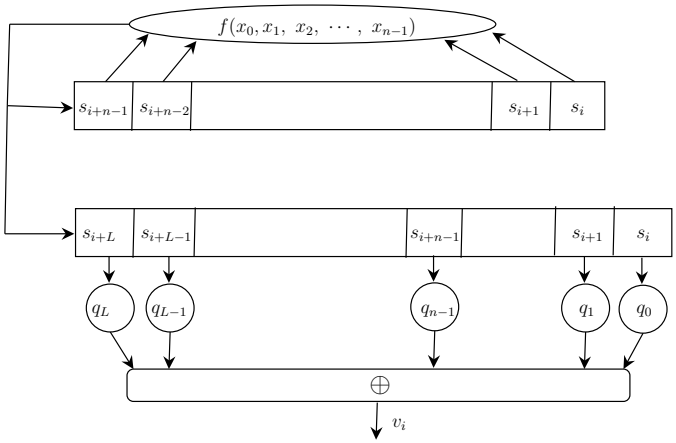


Figure 2: Construction of a filtering generator with designated linear span

Construction 1 (*Filtering sequence with known linear span).* A filtering sequence $\mathbf{v} = \{v_i\}$ with a known linear span is constructed as follows:

1. Let the sequence $\mathbf{s} = \{s_i\}$ be a span n sequence with the linear span $T \leq 2^n - 2$, the maximal value (i.e., the optimal case) where $s_i = A(\alpha^i) = \sum_{i \in I} \mathrm{tr}_1^{n_i}(\gamma_i \alpha^i)$ for some $\gamma_i \in \mathbb{F}_{2^n}$ and $I \subset I_0$ where I_0 is the set of *all* coset leaders modulo $2^n - 1$ and I consisting of those with $\gamma_i \neq 0$.

2. Let α be the primitive root of a primitive polynomial $t(x)$ defining $\mathbb{F}_{2^n}$. Let $t_{\alpha^i}(x)$ be the minimal polynomial of $\alpha^i, i \in I$. We denote

$$p(x) = \prod_{i \in I} t_{\alpha^i}(x).$$

   When the sequence $\mathbf{s}$ has the optimal linear span, we have

$$p(x) = p_0(x) := \frac{x^{2^n - 1} + 1}{x + 1}.$$

3. Select two subsets of coset leaders, denoted by J, $J \subset I$ and $J_0 \subset I_0$ disjoint with I. We compute $u(x) = u_J(x) u_{J_0}(x)$ where $u_k(x) = \prod_{i \in k} t_{\alpha^i}(x)$ where $k \in \{J, J_0\}$. Set $q(x) = p_0(x)/u(x) = \sum_{i=0}^{L} q_i x^i, q_i \in \mathbb{F}_2$ where $L = deg(q(x)) = T - deg(u(x))$ and $2^n - 2 - deg(u(x))$ when $\mathbf{s}$ has the optimal linear span, we have $u(x) = u_J(x)$ as $J_0 = \emptyset$.

4. Compute the filtering sequence $\mathbf{v} = \{v_t\}$ as

$$v_i = \sum_{j=0}^{L} q_j s_{i+j}, i = 0, 1, \cdots, 2^n - 2.$$

We now prove the linear span of the filtering sequence in Construction 1 in Theorem 8. The linear span of $\mathbf{v}$ can be proved by counting the non-zero spectral values in the spectral sequence of $\mathbf{v}$. The proof is similar to that of Theorem 1 in [15].

Theorem 8. *Let* $\mathbf{v} = \{v_i\}$ *be the filtering sequence generated in Construction 1. The linear span of* $\mathbf{v}$ *is* $\mathsf{LS}(\mathbf{v}) = deg(u_J(x))$.

Proof. As $\mathbf{s}$ is a span n sequence, the minimal polynomial of $\mathbf{s}$ for an LFSR is $p(x) = \prod_{i\in I} t_{\alpha^i}(x)$. Thus $\mathbf{v} = \{v_i\}$. According to [15], the relation between the spectral sequences of $\mathbf{v}$ and $\mathbf{a}$ is $V_i = A_i q(\alpha^i)$. Let $K = (I\backslash J) \subset I$. Then $q(\alpha^j) = 0$ and $j = k \cdot 2^i, 0 \le i \le n_k - 1$ for all coset leaders $k \in K$ and n_k is the size for the coset leader k, and $q(\alpha^j) \neq 0$ and $j = k \cdot 2^i, 0 \le i \le n_k - 1$ for all coset leaders $k \in J$. As $A_i \neq 0, 1 \le i \le 2^n - 2$, therefore $V_j = 0$ with $j = k \cdot 2^i, 0 \le i \le n_k - 1$ for all coset leaders $k \in K$ and $V_j \neq 0$ with $j = k \cdot 2^i, 0 \le i \le n_k - 1, k \in J$. Thus, the linear span of $\mathbf{v}$ is $\mathsf{LS}(v) = \sum_{k\in J} n_k = \deg(u_J(x))$. When $\mathbf{s}$ has the optimal linear span, we have $u(x) = u_J(x)$. □

Remark 9. By using this method, the linear span of the filtered sequence is not increasing. But it could decrease to the minimum linear of a span n sequence, which is an m-sequence.

When $\mathbf{s}$ is a span n sequence, in general, for any polynomial $q(x)$ of degree L, the filtering sequence $\mathbf{v}$ is not a span n sequence. We show a construction below that guarantees the filtering sequence is also a span n sequence with the worse linear span. In the following, we restrict ourselves to the case the span n sequence has the optimal linear span case in Construction 1 for simplicity.

Construction 2 (*Filtering span* $\boldsymbol{n}$ *sequence construction).* The steps to construct a filtering sequence that is also a span n sequence are as follows:

1. In Construction 1, select a coset leader $r \in I$ with $\gcd(r, 2^n-1)$. Set $q(x) = p(x)/t_{\alpha^r}(x) = \sum_{i=0}^{L} q_i x^i, q_i \in \mathbb{F}_2$ where $L = \deg(q(x)) = 2^n - 2 - n$.
2. Compute the filtering sequence $\mathbf{v} = \{v_t\}$ as

$$v_i = \sum_{j=0}^{L} q_j s_{i+j}, i = 0, 1, \cdots, 2^n - 2.$$

The filtering sequence $\mathbf{v} = \{v_i\}$ is an m-sequence that can be generated by $t_{\alpha^r}(x)$.

Proposition 10. *The number of different LFSR filtering polynomials* $q(x)$ *for which the sequence* $\mathbf{v}$ *in Construction 2 is an m-sequence, is* $\frac{\phi(2^n-1)}{n}$.

Proof. The proof follows from the fact that the number of coset leaders r with coset size n and $\gcd(r, 2^n - 1) = 1$ is $\frac{\phi(2^n-1)}{n}$. □

Construction 3 (*Computing* $\boldsymbol{h}$*).* The trace representation of h is computed as follows.

1. The mapping h from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is defined as

$$\begin{aligned} h(s_0, s_1, \cdots, s_{n-1}) &\to v_0 \\ h(s_1, s_2, \cdots, s_n) &\to v_1 \\ \vdots \qquad &\quad \vdots \\ h(s_{2^n-2}, s_0, \cdots, s_{n-2}) &\to v_{2^n-2} \end{aligned}$$

2. Let α be the primitive root of a primitive polynomial $t(x)$ defining $\mathbb{F}_{2^n}$. Apply the DFT on the above mapping to obtain the trace representation of h (using Fact 7).

We now give an example for this constriction.

Example 1. Let $n = 4$. Let α be a root of $t(x) = x^4+x+1$ in $\mathbb{F}_{2^4}$. Consider the feedback function $f(x_0, x_1, x_2, x_3) = x_0 + x_1 + x_2 + x_1x_2$ over $\mathbb{F}_2$. The NLFSR corresponding to f generates a span n sequence $\mathbf{s} = 111100010110100$ of period 15. The trace representation of $\mathbf{s}$ is

$$A(x) = \mathrm{tr}(\alpha^{13}x) + \mathrm{tr}(x^3) + \mathrm{tr}(x^5) + \mathrm{tr}(\alpha^{10}x^7).$$

Let $t_{\alpha^i}(x)$ be the minimal polynomial of $\alpha^i, i \in I = \{1, 3, 5, 7\}$. Then, $p(x) = \prod_{i\in I} t_{\alpha^i}(x) = t_\alpha(x)t_{\alpha^3}(x)t_{\alpha^5}(x)t_{\alpha^7}(x)$. If $r = 7$, then $q(x) = p(x)/t_{\alpha^r}(x) = \sum_{i=0}^{L} q_i x^i, q_i \in \mathbb{F}_2, L = \deg(q(x)) = 10$ where

$$q(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

The filtering sequence $\mathbf{v} = \{v_i\}$ is computed as

$$v_i = s_i + s_{i+1} + s_{i+2} + s_{i+4} + s_{i+5} + s_{i+8} + s_{i+10}, i = 0, 1, \cdots, 14.$$

where $\mathbf{v} = 001000111101011$, which is an m-sequence of period $2^4 - 1 = 15$ for $t_{\alpha^7}(x) = 1 + x^3 + x^4$. The filtering function h for the LFSR filtering is given by

$$h(x) = \mathrm{tr}(\alpha^2 x) + \mathrm{tr}(\alpha^3 x^3) + \mathrm{tr}(\alpha^7 x^7).$$

Remark 11. According the DFT, we may explicitly obtain the trace representation of the the filtering h in Construction 3 as follows. Let $f(x_0, x_1, \cdots, x_{n-1})$ be a feedback function of a modified de Bruijn sequence $\mathbf{s} = \{s_i\}$ generated by an FSR. Let $S_i = (s_i, s_{i+1}, \cdots, s_{i+n-1})$ be the state of the FSR. Suppose σ is the mapping that uniquely maps S_i to an element of $\mathbb{F}_{2^n}$, i.e., $\sigma : S_i \to \alpha^i, i = 0, 1, 2, \cdots, 2^n - 2$. Then the following function h is given by

$$\begin{aligned} h(\beta_i) &= \mathrm{tr}(\sigma^d(S_i)) \\ &= \mathrm{tr}(\beta\alpha^{di}), \end{aligned}$$

where $\sigma^d(S_i) = \alpha^{di}$ and $\beta = q(\alpha^d)$ and the coset of d has the full size modulo $2^n - 1$.

Iteratively computing the LFSR filtering sequence. For simplicity, we assume that the NLFSR generating a span n sequence has the optimal linear span. In Construction 2, the filtering polynomial $q(x)$ is the product of a set of minimal polynomials, say $q(x) = p_1(x)p_2(x)\cdots p_m(x)$. Then, computing $\mathbf{v}$ by the LFSR filter with connection polynomial $q(x)$ is equivalent to computing the filtering sequence iteratively by an LFSR with connection polynomial $p_i(x)$ for $i = 1, 2, \cdots, m$. That is, computing $\mathbf{v} = q(\mathcal{L})\mathbf{s}$ is equivalent to computing $\mathbf{v}_i = p_i(\mathcal{L})\mathbf{v}_{i-1}, i = 1, 2, \cdots, m$ where $\mathbf{v}_0 = \mathbf{s}$, $\mathbf{v} = \mathbf{v}_m$ and $\mathcal{L}$ is the left shift operator. In other words, applying the LFSR filter with the connection polynomial $p_i(x)$ on $\mathbf{v}_{i-1}$ drops the linear span by the degree of $p_i(x)$. This way an LFSR filter can be chosen so that a filtering sequence with the required linear span is achieved.

3.2 Filtering modified de Bruijn sequence generators

Motivated by the construction of the filtering generator in Section 3.1, we consider another filtering generator consisting of an NLFSR with a feedback function $f(x_0, x_1, \cdots, x_{n-1})$ generating a modified de Bruijn sequence and a Boolean filtering function g in n variables. The binary modified de Bruijn sequence $\mathbf{s} = \{s_i\}$ is generated as

$$s_{i+n} = f(s_i, s_{i+1}, \cdots, s_{i+n-1}), i \geq 0.$$

The *filtering sequence* $\mathbf{b} = \{b_i\}$ is generated from $\mathbf{s}$ using the filtering function g as

$$b_i = g(s_i, s_{i+1}, \cdots, s_{i+n-1}), i \geq 0.$$

When $\mathbf{s}$ has the period $2^n - 1$, the sequence $\mathbf{b}$ also will have the period $2^n - 1$. We desire the filtering sequence $\mathbf{b} = \{b_i\}$ to be a modified de Bruijn sequence, other than an m-sequence. We call such generator as a filtering modified de Bruijn or span n generator. Figure 3 shows a diagram of a filtering span n generator. Example 2 shows the existence of filtering functions for which the filtering sequence is also a modified de Bruijn sequence, other than an m-sequence.

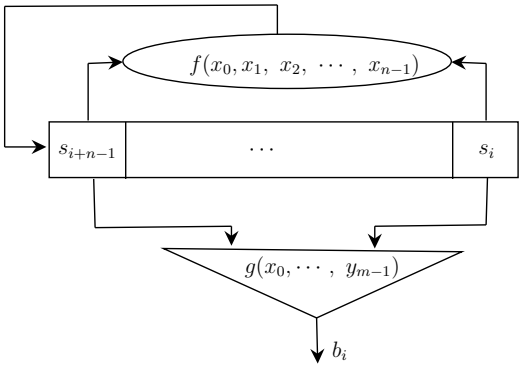


Figure 3: A block diagram of a filtering span n generator

Example 2. Let $n = 4$. Consider the feedback function $f(x_0, x_1, x_2, x_3) = x_0 + x_2 + x_1x_2 + x_1x_3$. The following recurrence relation with the initial state $(1, 1, 1, 1)$ generates the span n sequence $\mathbf{a} = 111101000101100$ with linear span 14:

$$a_{i+4} = f(a_i, a_{i+1}, a_{i+2}, a_{i+3}) = a_i + a_{i+2} + a_{i+1}a_{i+2} + a_{i+1}a_{i+3}, i \geq 0.$$

The filtering function $g(x_0, x_1, x_2, x_3) = x_0 + x_1 + x_1x_3$ on $\mathbf{a}$ produces a filtering sequence $\mathbf{b} = 101111000110100$, which is also a span n sequence and the linear span is 12.

For a suitable choice of a feedback function f and a filtering function g, both sequences $\mathbf{s}$ and $\mathbf{b}$ are span n sequences of period $2^n - 1$. In Proposition 12, we list some (trivial) filtering functions g that generates a span n sequence when the NLFSR generate a span n sequence. The proof is straightforward. So, we omit it.

Proposition 12. *Let f be a feedback function in n variables that generates a span n sequence $\mathbf{s} = \{s_i\}$ of period $2^n - 1$. Let g be a filtering function used to generate a filtering span n sequence $\mathbf{b} = \{b_i\}$. The following filtering functions g generates shift equivalent span n sequences:*

- *$g(x_0, x_1, \cdots, x_{n-1}) = x_i, 0 \leq i \leq n-1$ produces a span n sequence $\mathbf{b}$ with $\mathbf{b} = \mathcal{L}^i(\mathbf{a})$ where $\mathcal{L}$ is the left shift operator.*
- *$g(x_0, x_1, \cdots, x_{n-1}) = f(x_0, x_1, \cdots, x_{n-1})$ produces a span n sequence $\mathbf{b}$ with $\mathbf{b} = \mathcal{L}^n(\mathbf{a})$.*

4 Experimental Results

In Construction 2, we have seen that some filtering functions constructed from an LFSR minimal polynomial reduces the linear complexity to the minimum. This inspires us to understand the linear span of filtering span n sequences for different filtering functions.

Experimental parameters. We perform an experiment to exhaustively search for all feedback functions that generate span n sequences for $n = 4$ and 5, and partially for $n = 6$. For $n = 4$, we consider all filtering functions (i.e., 2^{15} Boolean functions), and for each span n sequence, we generate the filtering sequences. Our experimental results show that, for each span n sequence $\mathbf{s}$, out of 2^{15} filtering sequences, only 240 filtering sequences are span n sequences, which include all shift equivalent span n sequences of period 15. The total number of shift distinct span n sequences are 16. In Table 1, we present the distribution of the filtering functions that generate (shift distinct) span n sequences with different linear span values. Similarly, for $n = 5$, we checked for several span n sequences that, out of 2^{31} filtering sequences (as there are 2^{31} filtering functions), only 63488 ($= 2048 \times 31$) filtering sequences are span n sequences, which also includes all shift equivalent span n sequences of period 31. The total number of shift distinct span n sequences are 2048. Our experimental results in Table 1 also validates Proposition 10 for Construction 2.

In [25], Mayhew and Golomb (IEEE-IT 1990) studied the linear span distribution of span n sequences and presented experimental results on the number of span n sequences for different linear span values for $n = 4, 5$, and 6. In Table 1, we summarize their results on the number of span n sequences for an easy reference.

Table 1: Distribution of filtering functions that generate (shift distinct) span n sequences and their linear span

$n = 4$			$n = 5$		
Linear span	Number of filtering	Number of span n [25]	Linear span	Number of filtering	Number of span n [25]
4	2	2	5	6	6
12	4	4	15	10	10
14	10	10	20	4	4
			25	306	306
			30	1722	1722

We make the following conjecture on the distribution of the filtering functions.

Conjecture 1. For $n \geq 4$, in a filtering modified de Bruijn sequence generator, the distribution of filtering functions g that map a span n sequence $\mathbf{s}$ to another filtering span n sequence $\mathbf{b}$ is the same as the linear span distribution of span n sequences.

5 Conclusion and Future Work

In this work, we studied the construction of filtering modified de Bruijn sequence generators from the linear complexity point of view. We presented two filtering generator constructions that can give a chosen linear complexity. We experimentally studied the filtering functions and the linear span of corresponding filtering modified de Bruijn sequences. Our results show that the filtering function does not always preserve the high linear complexity of the filtering sequence even when the underlying modified de Bruijn sequence has a high linear complexity. This phenomenon suggests that for cryptographic applications, the filtering functions, in addition to well-known crypto properties such as high algebraic degree and algebraic/correlation/spectral immunity, should be chosen carefully to prevent from dropping the linear complexity drastically.

As a future work, we have been continuing to our work to prove Conjecture 1 and also study other crypto properties of the filtering functions that give filtering span n sequences.

References

[1] S. R. Blackburn, T. Etzion, and K. G. Paterson. Permutation polynomials, de bruijn sequences, and linear complexity. *Journal of Combinatorial Theory, Series A*, 76(1):55–82, 1996.

[2] R. E. Blahut. Theory and practice of error control codes. *Addison-Wesley*, 1983.

[3] A. H. Chan, R. A. Games, and E. L. Key. On the complexities of de bruijn sequences. *Journal of Combinatorial Theory, Series A*, 33(3):233–246, 1982.

[4] L. Chen and G. Gong. *Communication system security*. CRC press, 2012.

[5] N. G. De Bruijn. A combinatorial problem. *Proceedings of the Section of Sciences of the Koninklijke Nederlandse Akademie van Wetenschappen te Amsterdam*, 49(7):758–764, 1946.

[6] C. De Cannière. Trivium: A stream cipher construction inspired by block cipher design principles. In S. K. Katsikas, J. López, M. Backes, S. Gritzalis, and B. Preneel, editors, *Information Security*, pages 171–186, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[7] E. Dubrova. A list of maximum-period nlfsrs, 2012.

[8] P. Ekdahl, T. Johansson, A. Maximov, and J. Yang. A new snow stream cipher called snow-v. *Cryptology ePrint Archive*, 2018.

[9] T. Etzion. Linear complexity of de bruijn sequences-old and new results. *IEEE Transactions on Information Theory*, 45(2):693–698, 1999.

[10] H. Fredricksen. A survey of full length nonlinear shift register cycle algorithms. *SIAM review*, 24(2):195–221, 1982.

[11] R. Games and A. Chan. A fast algorithm for determining the complexity of a binary sequence with period 2^n (corresp.). *IEEE Transactions on Information Theory*, 29(1):144–146, 2006.

[12] S. W. Golomb. *Shift Register Sequences*. Aegean Park Press, USA, 1981.

[13] S. W. Golomb and G. Gong. *Signal design for good correlation: for wireless communication, cryptography, and radar*. Cambridge University Press, 2005.

[14] G. Gong. Randomness and representation of span n sequences. In S. W. Golomb, G. Gong, T. Helleseth, and H.-Y. Song, editors, *Sequences, Subsequences, and Consequences*, pages 192–203, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[15] G. Gong, S. Ronjom, T. Helleseth, and H. Hu. Fast discrete fourier spectra attacks on stream ciphers. *IEEE Transactions on Information Theory*, 57(8):5555–5565, 2011.

[16] M. Hell, T. Johansson, A. Maximov, and W. Meier. *The Grain Family of Stream Ciphers*, pages 179–190. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[17] C. Li, X. Zeng, C. Li, and T. Helleseth. A class of de Bruijn sequences. *IEEE Transactions on Information Theory*, 60(12):7955–7969, 2014.

[18] C. Li, X. Zeng, C. Li, T. Helleseth, and M. Li. Construction of de Bruijn sequences from lfsrs with reducible characteristic polynomials. *IEEE Transactions on Information Theory*, 62(1):610–624, 2015.

[19] K. Mandal and G. Gong. Cryptographically strong de Bruijn sequences with large periods. In *Selected Areas in Cryptography: 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers 19*, pages 104–118. Springer, 2013.

[20] K. Mandal and G. Gong. Generating good span n sequences using orthogonal functions in nonlinear feedback shift registers. *Open Problems in Mathematics and Computational Science*, pages 127–162, 2014.

[21] K. Mandal and G. Gong. On ideal t-tuple distribution of orthogonal functions in filtering de bruijn generators. *Advances in Mathematics of Communications*, 16(3):597–619, 2022.

[22] K. Mandal, B. Yang, G. Gong, and M. Aagaard. On ideal t-tuple distribution of filtering de bruijn sequence generators. *Cryptography Commun.*, 10(4):629–641, jul 2018.

[23] K. Mandal, B. Yang, G. Gong, and M. Aagaard. Analysis and efficient implementations of a class of composited de Bruijn sequences. *IEEE Transactions on Computers*, 69(12):1835–1848, 2020.

[24] J. Massey. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, 15(1):122–127, 1969.

[25] G. Mayhew and S. Golomb. Linear spans of modified de Bruijn sequences. *IEEE Transactions on Information Theory*, 36(5):1166–1167, 1990.

[26] G. L. Mayhew. Weight class distributions of de Bruijn sequences. *Discrete Mathematics*, 126(1):425–429, 1994.

[27] G. L. Mayhew and S. W. Golomb. Characterizations of generators for modified de Bruijn sequences. *Advances in Applied Mathematics*, 13(4):454–461, 1992.

[28] J. Mykkeltveit, M.-K. Siu, and P. Tong. On the cycle structure of some nonlinear shift register sequences. *Information and control*, 43(2):202–215, 1979.

[29] J. Mykkeltveit and J. Szmidt. On cross joining de Bruijn sequences. *Contemporary Mathematics*, 63:335–346, 2015.

[30] J.-S. No, S. W. Golomb, G. Gong, H.-K. Lee, and P. Gaal. Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation. *IEEE Transactions on Information Theory*, 44(2):814–817, 1998.

[31] T. Rachwalik, J. Szmidt, R. Wicik, and J. Zabłocki. Generation of nonlinear feedback shift registers with special-purpose hardware. In *2012 Military Communications and Information Systems Conference (MCC)*, pages 1–4. IEEE, 2012.

[32] R. A. Rueppel. *Analysis and design of stream ciphers*. Springer Science & Business Media, 2012.

[33] SAGE. Specification of the 3GPP confidentiality and integrity algorithms 128-eea3 & 128-eia3. document 2: ZUC specification. version 1.6, etsi/sage, 2011., 2011. https://www.gsma.com/aboutus/wp-content/uploads/2014/12/eea3eia3zucv16.pdf.

New Successor Rules to Efficiently Produce Exponentially Many Binary de Bruijn Sequences

Zuling Chang
School of Mathematics and Statistics
Zhengzhou University
450001 Zhengzhou, China
zuling_chang@zzu.edu.cn

Martianus Frederic Ezerman
School of Physical and Mathematical Sciences
Nanyang Technological University
21 Nanyang Link, Singapore 637371
fredezerman@ntu.edu.sg

Pinhui Ke
Key Laboratory of
Network Security and Cryptology
Fujian Normal University
350117 Fuzhou, China
keph@fjnu.edu.cn

Qiang Wang
School of Mathematics and Statistics
Carleton University
1125 Colonel By Drive
Ottawa ON K1S 5B6, Canada
wang@math.carleton.ca

Abstract

We propose a new general criteria to design successor rules for binary de Bruijn sequences and show that prior fast algorithms based on successor rules are special instances. We efficiently generate exponentially many binary de Bruijn sequences for any given order n. Producing the next bit in each such sequence takes $O(n)$ memory and $O(n)$ time. We devise computational routines to confirm the claims.

1 Introduction

A 2^n-periodic binary sequence is a *binary de Bruijn sequence* of order n if every binary n-tuple occurs exactly once within each period. There are $2^{2^{n-1}-n}$ such sequences [1]. They appear in many guises, drawing the attention of researchers from varied backgrounds and interests. Being balanced and having maximum period [2, 3] make these sequences applicable in coding and communication systems. A subclass with properly calibrated nonlinearity property can also be useful in cryptography.

Experts have been using tools from diverse branches of mathematics to study their generations and properties, see, *e.g.*, the surveys in [4] and [5] for further details. Of enduring interest are methods that excel in three measures: fast, with low memory requirement, and capable of generating a large number of sequences. Known constructions

come with some trade-offs with respect to these measures. Notable examples include Lempel's D-Morphism [6], an approach via preference functions described in [7] and in [3], greedy algorithms with specific preferences, *e.g.*, in [8] and, more recently, in [9], as well as various fast generation proposals, *e.g.*, those in [10] and in [11].

The most popular construction approach is the *cycle joining method* (CJM) [3]. It serves as the foundation of many techniques. A main drawback of the CJM, in its most general form, is the amount of computation to be done prior to actually generating the sequences. Given a feedback shift register, one must first determine its cycle structure before finding the conjugate pairs to build the so-called adjacency graph. Enumerating the spanning trees comes next. Once these general and involved steps have been properly done, then generating a sequence, either randomly or based on a predetermined rule, is very efficient in both time and memory. The main advantage, if carried out in full, is the large number of output sequences, as illustrated in [12, Table 3].

There are fast algorithms that can be seen as applications of the CJM on specially chosen conjugate pairs and designated initial states. They often produce a very limited number of de Bruijn sequences. One can generate a de Bruijn sequence, named the `granddady` in [10], in $O(n)$ time and $O(n)$ space per bit. A related de Bruijn sequence, named the `grandmama`, was built in [11]. Huang gave another early construction that joins the cycles of the *complementing circulating register* (CCR) in [13]. Etzion and Lempel proposed some algorithms to generate de Bruijn sequences based on the *pure cycling register* (PCR) and the *pure summing register* (PSR) in [14]. Their algorithms generate a number, exponential in n, of sequences at the expense of higher memory requirement.

Jansen, Franx, and Boekee established a requirement to determine some conjugate pairs in [15], leading to another fast algorithm. In [16], Sawada, Williams, and Wong proposed a simple de Bruijn sequence construction, which turns out to be a special case of the method in [15]. Gabric *et al.* generalized the last two works to form simple successor rule frameworks in [17]. Further generalization to k-ary de Bruijn sequences in [18] and [20] followed. Zhu *et al.* in [19], building upon the framework in [17], proposed two efficient generic successor rules based on the properties of the feedback function $f(x_0, x_1, \ldots, x_{n-1}) = x_0 + x_1 + x_{n-1}$ for $n \geq 3$. Each rule produces at least 2^{n-3} binary de Bruijn sequences.

Our Contributions

We generate de Bruijn sequences by using novel relations and orders on the cycles in combination with suitable successor rules. We define new classes of successor rules and, then, prove that they generate, respectively, a number, exponential in n, of de Bruijn sequences. In particular, the number of generated sequences based on the PCR of order n is $2(n-1)(n-2)\ldots 1 = 2 \cdot (n-1)!$. The cost to output the next bit is $O(n)$ time and $O(n)$ space. Nearly all known successor rules in the literature generate only a handful of de Bruijn sequences each. The few previously available approaches that can generate an exponential number of de Bruijn sequences require more space than the ones we are proposing.

A high level explanation of our approach is as follows. We begin with the set of cycles produced by any nonsingular feedback shift register. To join all of these cycles into a single

cycle, *i.e.*, to obtain a binary de Bruijn sequence, one needs a valid successor rule that assigns a uniquely identified state in one cycle to a uniquely identified state in another cycle and ensure that all of the cycles are joined in the end. If the cycles are represented by the vertices of an adjacency graph, then producing a de Bruijn sequence in the CJM corresponds to finding a spanning tree in the graph. We identify several new relations and orders on both the cycles and on the states in each cycle. These ensure the existence of spanning trees in the corresponding adjacency graphs.

We collect preliminary notions and several useful known results in Section 2. Section 3 presents our new general criteria. Section 4 shows how to apply the criteria on the cycles of the PCR, leading to scores of new successor rules. The last section summarizes our contributions and lists some future directions.

2 Preliminaries

2.1 Basic Definitions

An *n-stage shift register* is a circuit of n consecutive storage units, each containing a bit. The circuit is clock-regulated, shifting the bit in each unit to the next stage as the clock pulses. A shift register generates a binary code if one adds a feedback loop that outputs a new bit s_n based on the n bits $\mathbf{s}_0 = s_0, \ldots, s_{n-1}$, called an *initial state* of the register. The corresponding Boolean *feedback function* $f(x_0, \ldots, x_{n-1})$ outputs s_n on input $\mathbf{s}_0$. A *feedback shift register* (FSR) outputs a binary sequence $\mathbf{s} = \{s_i\} = s_0, s_1, \ldots, s_n, \ldots$ that satisfies the recursive relation $s_{n+\ell} = f(s_\ell, s_{\ell+1}, \ldots, s_{\ell+n-1})$ for $\ell = 0, 1, 2, \ldots$. For $N \in \mathbb{N}$, if $s_{i+N} = s_i$ for all $i \geq 0$, then $\mathbf{s}$ is *N-periodic* or *with period N* and one writes $\mathbf{s} = (s_0, s_1, s_2, \ldots, s_{N-1})$. The least among all periods of $\mathbf{s}$ is called the *least period* of $\mathbf{s}$.

We say that $\mathbf{s}_i = s_i, s_{i+1}, \ldots, s_{i+n-1}$ is *the i^{th} state* of $\mathbf{s}$. Its *predecessor* is $\mathbf{s}_{i-1}$ while its *successor* is $\mathbf{s}_{i+1}$. For $s \in \mathbb{F}_2$, let $\bar{s} := s + 1 \in \mathbb{F}_2$. Extending the definition to any binary vector or sequence $\mathbf{s} = s_0, s_1, \ldots, s_{n-1}, \ldots$, let $\overline{\mathbf{s}} := \overline{s_0}, \overline{s_1}, \ldots, \overline{s_{n-1}}, \ldots$. An arbitrary state $\mathbf{v} = v_0, v_1, \ldots, v_{n-1}$ of $\mathbf{s}$ has $\widehat{\mathbf{v}} := \overline{v_0}, v_1, \ldots, v_{n-1}$ and $\widetilde{\mathbf{v}} := v_0, \ldots, v_{n-2}, \overline{v_{n-1}}$ as its *conjugate* state and *companion* state, respectively. Hence, $(\mathbf{v}, \widehat{\mathbf{v}})$ is a *conjugate pair* and $(\mathbf{v}, \widetilde{\mathbf{v}})$ is a *companion pair*.

For any FSR, distinct initial states generate distinct sequences. There are 2^n distinct sequences generated from an FSR with feedback function $f(x_0, x_1, \ldots, x_{n-1})$. They are periodic if and only if f is *nonsingular*, *i.e.*, f expressible as $f(x_0, x_1, \ldots, x_{n-1}) = x_0 + h(x_1, \ldots, x_{n-1})$, for some Boolean function $h(x_1, \ldots, x_{n-1})$ whose domain is $\mathbb{F}_2^{n-1}$ [3, p. 116]. All feedback functions in this paper are nonsingular. An FSR is *linear* or an LFSR if its feedback function has the form $f(x_0, x_1, \ldots, x_{n-1}) = x_0 + c_1 x_1 + \ldots + c_{n-1} x_{n-1}$, with $c_i \in \mathbb{F}_2$, and its *characteristic polynomial* is $f(x) = x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + 1 \in \mathbb{F}_2[x]$. Otherwise, it is *nonlinear* or an NLFSR. Further properties of LFSRs are treated in, *e.g.*, [22] and [23].

For an N-periodic sequence $\mathbf{s}$, the *left shift operator* L maps $(s_0, s_1, \ldots, s_{N-1}) \mapsto (s_1, s_2, \ldots, s_{N-1}, s_0)$, with the convention that L^0 fixes $\mathbf{s}$. The *right shift operator* R is

defined analogously. The set

$$[\mathbf{s}] := \{\mathbf{s}, L\mathbf{s}, \ldots, L^{N-1}\mathbf{s}\} = \{\mathbf{s}, R\mathbf{s}, \ldots, R^{N-1}\mathbf{s}\} \tag{1}$$

is a *shift equivalent class*. Sequences in the same shift equivalent class correspond to the same cycle in the state diagram of FSR [22]. We call a periodic sequence in a shift equivalent class a *cycle*. If an FSR with feedback function f generates r disjoint cycles $C_1, C_2, \ldots, C_r$, then its *cycle structure* is $\Omega(f) = \{C_1, C_2, \ldots, C_r\}$. A cycle can also be viewed as a set of consecutive n-stage states in the corresponding periodic sequence. Since the cycle are disjoint, we can write $\mathbb{F}_2^n = C_1 \cup C_2 \cup \ldots \cup C_r$. When $r = 1$, the corresponding FSR is of *maximal length* and its output is a de Bruijn sequence of order n.

The *weight* of an N-periodic cycle C, denoted by $\mathrm{wt}(C)$, is $|\{0 \le j \le N-1 : c_j = 1\}|$. Similarly, the weight of a state is the number of 1s in the state. The lexicographically least N-stage state in any N-periodic cycle is called its *necklace*. As discussed in, *e.g.*, [24] and [17], there is a fast algorithm that determines whether or not a state is a necklace in $O(N)$ time. In fact, one can efficiently sort all distinct states in C. The standard `python` implementation is `timsort` [25]. It was developed by Tim Peters based on McIlroy's techniques in [26]. In the worst case, its space and time complexities are $O(N)$ and $O(N \log N)$ respectively. A closely related proposal, by Buss and Knop, is in [27].

Given disjoint cycles C and C' in $\Omega(f)$ with the property that some state $\mathbf{v}$ in C has its conjugate state $\widehat{\mathbf{v}}$ in C', interchanging the successors of $\mathbf{v}$ and $\widehat{\mathbf{v}}$ joins C and C' into a cycle whose feedback function is

$$\widehat{f} := f(x_0, x_1, \ldots, x_{n-1}) + \prod_{i=1}^{n-1}(x_i + \overline{v_i}). \tag{2}$$

Similarly, if the companion states $\mathbf{v}$ and $\widetilde{\mathbf{v}}$ are in two distinct cycles, then interchanging their predecessors joins the two cycles. If this process can be continued until all cycles that form $\Omega(f)$ merge into a single cycle, then we obtain a de Bruijn sequence. The CJM is, therefore, predicated upon knowing the cycle structure of $\Omega(f)$ and is closely related to a graph associated to the FSR.

Given an FSR with feedback function f, its *adjacency graph* G_f, or simply G if f is clear, is an undirected multigraph whose vertices correspond to the cycles of $\Omega(f)$. The number of edges between two vertices is the number of shared conjugate (or companion) pairs, with each edge labelled by a specific pair. It is well-known that there is a bijection between the set of spanning trees of G and the set of all inequivalent de Bruijn sequences constructible by the CJM on input f.

A *pure cycling register* (PCR) *of order* n is an LFSR with feedback function and characteristic polynomial

$$f_{\mathrm{PCR}}(x_0, x_1, \ldots, x_{n-1}) = x_0 \text{ and } f_{\mathrm{PCR}}(x) = x^n + 1. \tag{3}$$

Let $\phi(\cdot)$ be the Euler totient function. The number of distinct cycles in $\Omega(f_{\mathrm{PCR}})$ is known, *e.g.*, from [3], to be

$$Z_n := \frac{1}{n}\sum_{d|n} \phi(d) 2^{\frac{n}{d}}. \tag{4}$$

By definition, all states in any given n-periodic cycle $C_{\text{PCR}} := (c_0, c_1, \ldots, c_{n-1}) \in \Omega(f_{\text{PCR}})$ have the same number of ones.

2.2 Jansen-Franx-Boekee (JFB) Algorithm

In [15], Jansen *et al.* proposed an algorithm to generate de Bruijn sequences by the CJM. Suppose that the FSR with a feedback function $f(x_0, x_1, \ldots, x_{n-1})$ is given. They defined the *cycle representative* of any cycle of the FSR to be its lexicographically smallest n-stage state. If the FSR is the PCR of order n, then it is clear that the cycle representative is its necklace. Based on the cycle representative, we can impose an order on the cycles. For arbitrary cycles C and C' in Ω_f, we say that $C \prec_{\text{lex}} C'$ if and only if the cycle representative of C is lexicographically less than that of C'. This *lexicographic order* defines a total order on the cycles of the said PCR.

On current state $\mathbf{s}_i = s_i, s_{i+1}, \ldots, s_{i+n-1}$, the next state $\mathbf{s}_{i+1} = s_{i+1}, s_{i+2}, \ldots, s_{i+n}$ is produced based on the assignment rule in Algorithm 1. The correctness of the JFB Algorithm rests on the fact that the cycle representative in any cycle C_1 which does not contain the all zero state $0, \ldots, 0$ is unique. Its companion state is guaranteed to be in another cycle C_2 with $C_2 \prec_{\text{lex}} C_1$. This ensures that we have a spanning tree and, hence, the resulting sequence must be de Bruijn.

Algorithm 1 Jansen-Franx-Boekee (JFB) Algorithm

```
1: if s_i = s_i, 0, ..., 0 then
2:     s_{i+1} ← 0, ..., 0, s_i + 1
3: else
4:     if s_{i+1}, ..., s_{i+n-1}, 0 or s_{i+1}, ..., s_{i+n-1}, 1 is a cycle representative then
5:         s_{i+1} ← s_{i+1}, ..., s_{i+n-1}, f(s_i, ..., s_{i+n-1}) + 1
6:     else
7:         s_{i+1} ← s_{i+1}, ..., s_{i+n-1}, f(s_i, ..., s_{i+n-1})
```

The main task of keeping track of the cycle representatives in Algorithm 1 may require a lot of time if the least periods of the cycles are large. For cases where all cycles produced by a given FSR have small least periods, *e.g.*, in the case of the PCR or the PSR of order n, the algorithm generates de Bruijn sequences very efficiently. The space complexity is $O(n)$ and the time complexity lies between $O(n)$ and $O(n \log n)$ to output the next bit.

Sawada *et al.* proposed a simple fast algorithm on the PCR to generate a de Buijn sequence [16]. Their algorithm is a special case of the JFB Algorithm. Later, in [17], Gabric and the authors of [16] considered the PCR and the complemented PCR, also known as the CCR, and proposed several fast algorithms to generate de Bruijn sequences by ordering the cycles lexicographically according to their respective necklace and co-necklace. They replace the generating algorithm by some *successor rule*.

The general thinking behind the approach is as follows. Given an FSR with a feedback function $f(x_0, x_1, \ldots, x_{n-1})$, let A label some condition which guarantees that the resulting

sequence is de Bruijn. For any state $\mathbf{c} := c_0, c_1, \ldots, c_{n-1}$, the successor rule assigns

$$\rho_A(\mathbf{c}) = \begin{cases} f(\mathbf{c}) + 1, \text{ if } \mathbf{c} \text{ satisfies } A, \\ f(\mathbf{c}), \text{ otherwise.} \end{cases} \tag{5}$$

The usual successor of $\mathbf{c}$ is $c_1, \ldots, c_{n-1}, f(c_0, \ldots, c_{n-1})$. Every time $\mathbf{c}$ satisfies Condition A, however, its successor is *redefined* to be $c_1, \ldots, c_{n-1}, f(c_0, \ldots, c_{n-1}) + 1$. The last bit of the successor is *the complement* of the last bit of the usual successor under the feedback function f. The basic idea of a successor rule is to determine spanning trees in G_f by identifying a suitable Condition A. Seen in this light, the rule implements the CJM by assigning successors to carefully selected states.

3 New General Criteria for Successor Rules

New successor rules for de Bruijn sequences can be established by defining some relations or orders on the cycles of FSRs with special properties to construct spanning trees in G_f. This section proves a general criteria that such rules must meet. The criteria will be applied successfully, in latter sections, to the PCR and the PSR of any order n. The generality of the criteria allows for further studies to be conducted on the feasibility of using broader families of FSRs for fast generation of de Bruijn sequences.

We adopt set theoretic definitions and facts from [21]. Given Ω_f, we define a binary *relation* $\prec$ on $\Omega_f := \{C_1, C_2, \ldots, C_r\}$ as a set of ordered pairs in Ω_f. If $C \prec C$ for every $C \in \Omega_f$, then $\prec$ is said to be *reflexive*. Let $1 \leq i, j, k \leq r$. We say that $\prec$ is *transitive* if $C_i \prec C_j$ and $C_j \prec C_k$, together, imply $C_i \prec C_k$. It is *symmetric* if $C_i \prec C_j$ implies $C_j \prec C_i$ and *antisymmetric* if the validity of both $C_i \prec C_j$ and $C_j \prec C_i$ implies $C_i = C_j$.

The relation $\prec$ is called a *preorder* on Ω_f if it is reflexive and transitive. It becomes a *partial order* if it is an antisymmetric preorder. If $\prec$ is a partial order with either $C_i \prec C_j$ or $C_j \prec C_i$, for any C_i and C_j, then it is a *total order*. A totally ordered set Ω_f is called a *chain*. Hence, we can now say that $\prec_{\text{lex}}$ defined in Subsection 2.2 is a total order on the corresponding chain Ω_f.

Theorem 1. *Given an FSR with feedback function f, let $\prec$ be a transitive relation on $\Omega(f) := \{C_1, C_2, \ldots, C_r\}$ and let $1 \leq i, j \leq r$.*

1. *Let there be a unique cycle C with the property that $C \prec C'$ for any cycle $C' \neq C$,* i.e., *C is the unique smallest cycle in $\Omega(f)$. Let ρ be a successor rule that can be well-defined as follows. If any cycle $C_i \neq C$ contains a uniquely defined state whose successor can be assigned by ρ to be a state in a cycle $C_j \neq C_i$ with $C_j \prec C_i$, then ρ generates a de Bruijn sequence.*

2. *Let there be a unique cycle C with the property that $C' \prec C$ for any cycle $C' \neq C$,* i.e., *C is the unique largest cycle in $\Omega(f)$. Let ρ be a successor rule that can be well-defined as follows. If any cycle $C_i \neq C$ contains a uniquely defined state whose successor can be assigned by ρ to be a state in a cycle $C_j \neq C_i$ with $C_i \prec C_j$, then ρ generates a de Bruijn sequence.*

Proof. We prove the first case by constructing a rooted tree whose vertices are all of the cycles in $\Omega(f)$. This exhibits a spanning tree in the adjacency graph of the FSR according to the specified successor rule. The second case can be similarly argued.

Based on the condition set out in the first case, each $C_i \neq C$ contains a unique state whose assigned successor under ρ is in $C_j \neq C_i$, revealing that C_i and C_j are adjacent. Since $C_j \prec C_i$, we direct the edge **from** C_i **to** C_j. It is easy to check that, except for C whose outdegree is 0, each vertex has outdegree 1. Since $\prec$ is transitive, there is a unique path from the vertex to C. We have thus built a spanning tree rooted at C. □

There are two tasks to carry out in using Theorem 1. First, one must define a suitable transitive relation among the cycles to obtain the unique smallest or largest cycle C. The second task is to determine the unique state in each cycle. A sensible approach is to designate a state $\mathbf{v}$ as the *benchmark state* in each cycle C. We then uniquely define a state $\mathbf{w}$ in C with respect to the benchmark state. The cycle representative, *i.e.*, the necklace in the PCR, is the most popular choice for $\mathbf{v}$. In this paper we mainly use the necklace as the benchmark state in each cycle.

4 Successor Rules from Pure Cycling Registers

In applying the criteria in Theorem 1 to the PCR of any order n, it is good to consider the positions of the states in each cycle *relative to its necklace* by ordering the states in several distinct manners. This general route is chosen since we can check whether or not a state is a necklace in $O(n)$ time and $O(n)$ space. If the relative position of a state to the necklace is efficient to pinpoint, then the derived successor rule also runs efficiently.

4.1 The Weight Relation on the Pure Cycling Register

The cycles of the PCR share a nice property. All of the states in any cycle C are shift-equivalent and share the same weight $\mathrm{wt}(C)$. Hence, we can define a *weight relation* on the cycles based simply on their respective weights. For cycles $C_i \neq C_j$, we say that $C_i \prec_{\mathrm{wt}} C_j$ if and only if $\mathrm{wt}(C_i) < \mathrm{wt}(C_j)$. The relation $\prec_{\mathrm{wt}}$ is not even a preorder, making it differs qualitatively from the lexicographic order.

Example 2. The PCR of order 6 generates $C_1 := (001001)$ and $C_2 := (000111)$, with $C_1 \succ_{\mathrm{lex}} C_2$, since the necklace 001001 in C_1 is lexicographically larger than the necklace 000111 in C_2. In the weight relation, $C_1 \prec_{\mathrm{wt}} C_2$ since $\mathrm{wt}(C_1) = 2 < 3 = \mathrm{wt}(C_2)$. □

The following successor rules rely on the weight relation.

Theorem 3. *For the PCR of order n, if a successor rule $\rho(x_0, x_1, \ldots, x_{n-1})$ satisfies one of the following conditions, then it generates a de Bruijn sequence.*

1. *For any $C_i \neq (0)$, the rule ρ exchanges the successor of a uniquely determined state $\mathbf{v}_i \in C_i$ with a state $\mathbf{w}_j$ in C_j, where $C_j \prec_{\mathrm{wt}} C_i$.*

2. *For any $C_i \neq (1)$, the rule ρ exchanges the successor of a uniquely determined state $\mathbf{v}_i \in C_i$ with a state $\mathbf{w}_j$ in C_j, where $C_i \prec_{\mathrm{wt}} C_j$.*

Proof. To prove the first case, note that $(0) \prec_{\mathrm{wt}} C_i$ for any $C_i \neq (0)$ in $\Omega(f_{\mathrm{PCR}})$. By the stated condition, C_i contains a unique state $\mathbf{v}_i$ such that its conjugate $\mathbf{w}_j := \widehat{\mathbf{v}}_i$ is in C_j and $\mathrm{wt}(C_j) < \mathrm{wt}(C_i)$. The successor rule ρ satisfies the criteria in Theorem 1. The proof for the second case is similar. □

Theorem 3 reduces the task to generate de Bruijn sequences by using ρ to performing one of two procedures. The first option is to find the *uniquely determined state* $\mathbf{v}_i \in C_i \neq (0)$ whose conjugate state $\widehat{\mathbf{v}}_i$ is guaranteed to be in C_j with $\mathrm{wt}(C_j) < \mathrm{wt}(C_i)$. The second option is to find the *uniquely determined state* $\mathbf{v}_i$ in each $C_j \neq (1)$ whose conjugate state $\widehat{\mathbf{v}}_i$ is guaranteed to be in C_j with $\mathrm{wt}(C_j) > \mathrm{wt}(C_i)$. If, for every C_i, its $\mathbf{v}_i$ can be determined quickly, then generating the de Bruijn sequence is efficient. Following the two cases in Theorem 3, the rule ρ comes in two forms. Let $\mathbf{c} := c_0, c_1, \ldots, c_{n-1}$.

First, let $\mathcal{A}$ be

> In $C := (0, c_1, \ldots, c_{n-1})$, the uniquely determined state $\mathbf{v}$ is $0, c_1, \ldots, c_{n-1}$. Its conjugate $\widehat{\mathbf{v}}$ has $\mathrm{wt}(\widehat{\mathbf{v}}) > \mathrm{wt}(\mathbf{v})$, which implies $\widehat{\mathbf{v}}$ is in C' with $C \prec_{\mathrm{wt}} C'$.

We confirm that the relevant requirement in Theorem 3 is met by

$$\rho_{\mathcal{A}}(\mathbf{c}) = \begin{cases} \overline{c_0}, \text{ if } 0, c_1, \ldots, c_{n-1} \text{ satisfies } \mathcal{A}, \\ c_0, \text{ otherwise.} \end{cases} \tag{6}$$

Second, let $\mathcal{B}$ be

> In $C := (c_1, \ldots, c_{n-1}, 1)$, the uniquely determined state $\mathbf{v}$ is $c_1, \ldots, c_{n-1}, 1$. Its companion $\widetilde{\mathbf{v}}$ has $\mathrm{wt}(\widetilde{\mathbf{v}}) < \mathrm{wt}(\mathbf{v})$, which means that $\widetilde{\mathbf{v}}_i$ is in C' with $C' \prec_{\mathrm{wt}} C$.

Hence, the successor rule

$$\rho_{\mathcal{B}}(\mathbf{c}) = \begin{cases} \overline{c_0}, \text{ if } c_1, \ldots, c_{n-1}, 1 \text{ satisfies } \mathcal{B}, \\ c_0, \text{ otherwise,} \end{cases} \tag{7}$$

fulfills the requirement in Theorem 3.

Based on $\mathcal{A}$ and $\mathcal{B}$, valid successor rules can be easily formulated once we manage to determine a unique state whose first bit is 0, respectively, whose last bit is 1, in each $C \neq (1)$, respectively, $C \neq (0)$.

4.2 Under the Shift Order

Imposing a *shift order* on the states in a given cycle yields a lot of feasible successor rules. We call a state whose first entry is 0 a *leading zero state* or an LZ state in short. Analogously, a state whose last entry is 1 is said to be an *ending one state* or an EO state.

The necklace in a given cycle $(c_0, c_1, \ldots, c_{n-1}) \neq (1)$ must begin with 0, *i.e.*, its necklace is an LZ state. Here we define a *special left shift operator*, denoted by L_{lz}. Applied on a given LZ state $\mathbf{v} := 0, c_1, \ldots, c_{n-1}$ the operator L_{lz} outputs the first LZ state obtained by

consecutive left shifts on $\mathbf{v}$. More formally, $L_{\text{lz}}\,\mathbf{v} := \mathbf{v}$ if $c_1, \ldots, c_{n-1} = 1, \ldots, 1$. Otherwise, let $1 \le j < n$ be the least index such that $c_j = 0$. Then

$$L_{\text{lz}}\,\mathbf{v} := 0, c_{j+1}, \ldots, c_{n-1}, 0, c_1, \ldots, c_{j-1}.$$

Similarly, the necklace in any $C \neq (0)$ must end with 1, *i.e.*, it is an EO state. Given a state $\mathbf{u} := c_1, \ldots, c_{n-1}, 1$, the special operator L_{eo} fixes $\mathbf{u}$ if $c_1, \ldots, c_{n-1} := 0, \ldots, 0$. Otherwise, let $1 \le j < n$ be the least index such that $c_j = 1$. Then

$$L_{\text{eo}}\,\mathbf{u} := c_{j+1}, \ldots, c_{n-1}, 1, c_1, \ldots, c_{j-1}, 1.$$

In other words, $L_{\text{eo}}\,\mathbf{u}$ is the first EO state found upon consecutive left shifts on $\mathbf{u}$.

For these two special operators, the convention is to let

$$\begin{cases} L_{\text{lz}}^0\,\mathbf{v} = \mathbf{v}, \\ L_{\text{eo}}^0\,\mathbf{u} = \mathbf{u}, \end{cases} \quad \text{and} \quad \begin{cases} L_{\text{lz}}^k\,\mathbf{v} = L_{\text{lz}}^{k-1}(L_{\text{lz}}\,\mathbf{v}), \\ L_{\text{eo}}^k\,\mathbf{u} = L_{\text{eo}}^{k-1}(L_{\text{eo}}\,\mathbf{u}), \end{cases} \quad \text{for } k > 0.$$

Proposition 4. *With arbitrarily chosen $2 \le t \le n$, we let $1 = k_1 < k_2 < \cdots < k_t = n+1$ and $k_{t-1} < n$. For a state $\mathbf{c} := c_0, c_1, \ldots, c_{n-1}$, let $\mathbf{v} := 0, c_1, \ldots, c_{n-1}$ and $\mathbf{u} := c_1, \ldots, c_{n-1}, 1$. The following two successor rules generate de Bruijn sequences of order n.*

$$\rho_{\text{lz}}(\mathbf{c}) = \begin{cases} \overline{c_0}, \text{ if } k_i \le \mathrm{wt}(\overline{\mathbf{v}}) < k_{i+1} \\ \quad \text{for some } i \text{ and} \\ \quad L_{\text{lz}}^{k_i-1}\,\mathbf{v} \text{ is a necklace}, \\ c_0, \text{ otherwise.} \end{cases} \qquad \rho_{\text{eo}}(\mathbf{c}) = \begin{cases} \overline{c_0}, \text{ if } k_i \le \mathrm{wt}(\mathbf{u}) < k_{i+1} \\ \quad \text{for some } i \text{ and} \\ \quad L_{\text{eo}}^{k_i-1}\,\mathbf{u} \text{ is a necklace}, \\ c_0, \text{ otherwise.} \end{cases} \tag{8}$$

In Proposition 4 we let $k_t = n+1$ for consistency since $\mathrm{wt}(\overline{\mathbf{v}}) = n$ in $C = (0)$ and $\mathrm{wt}(\mathbf{u}) = n$ in $C = (1)$. Each of these special cycles has only a single state. The reason to have $k_{t-1} < n$ is then clear. The correctness of Proposition 4 comes from Theorem 3 and the fact that the state satisfying the respective conditions in ρ_{lz} and ρ_{eo} is uniquely determined in the corresponding cycle.

Proposition 5. *Each of the successor rules ρ_{lz} in (8) generates 2^{n-2} de Bruijn sequences of order n.*

Proof. We supply the proof for ρ_{lz} in (8), the other case being similar to argue. For each $1 \le \ell < n$, there exists at least one cycle of the PCR of order n having ℓ distinct LZ states. To verify existence, one can, *e.g.*, inspect the cycle $(\underbrace{00\ldots0}_{\ell}\underbrace{11\ldots1}_{n-\ell})$ for each $1 \le \ell < n$. On the other hand, taking all possible $2 \le t \le n$, there are 2^{n-2} distinct sets $\{1 = k_1, k_2, \ldots, k_{t-1}, k_t = n+1\}$ with $k_{t-1} < n$. Distinct sets provide distinct successor rules, producing 2^{n-2} inequivalent de Bruijn sequences in total. □

We are not quite done yet. Here are two more general successor rules whose validity can be routinely checked.

Proposition 6. *Let k be a nonnegative integer. For a state $\mathbf{c} := c_0, c_1, \ldots, c_{n-1}$, let $\mathbf{v} := 0, c_1, \ldots, c_{n-1}$ and $\mathbf{u} := c_1, \ldots, c_{n-1}, 1$. The following successor rules generate de Bruijn sequences of order n.*

$$\rho(\mathbf{c}) = \begin{cases} \overline{c_0}, \text{ if } L_{\mathrm{lz}}^k \mathbf{v} \text{ is a necklace,} \\ c_0, \text{ otherwise.} \end{cases} \qquad \rho(\mathbf{c}) = \begin{cases} \overline{c_0}, \text{ if } L_{\mathrm{eo}}^k \mathbf{u} \text{ is a necklace,} \\ c_0, \text{ otherwise.} \end{cases} \tag{9}$$

Proposition 7. *The number of distinct de Bruijn sequences of order n produced by each of the rules in (9) is*

$$\operatorname{lcm}(1, 2, \ldots, n-1) \geq (n-1)\binom{n-2}{\lfloor \frac{n-2}{2} \rfloor} \geq 2^{n-2}. \tag{10}$$

Proof. We supply the counting for the successor rule in (9). We know from the proof of Proposition 5 that, for each $1 \leq \ell < n$, there exists at least one cycle of the PCR of order n having ℓ distinct LZ states. For a given k, we construct the system of congruences

$$\{k \equiv a_i \pmod{i} \text{ for } i \in \{1, 2, \ldots, n-1\}\}. \tag{11}$$

The number of resulting distinct de Bruijn sequences of order n is equal to the number of solvable systems of congruences in (11). The sequences are distinct because different nonempty subsets of $\{a_1, \ldots, a_{n-1}\}$, whose corresponding systems are solvable, lead to different choices for the uniquely determined states in the respective cycles. By a generalized Chinese Remainder Algorithm in [28, Section 2.4], the number is $\operatorname{lcm}(1, 2, \ldots, n-1)$. From [29, Section 2] we get the lower bounds $(n-1)\binom{n-2}{\lfloor \frac{n-2}{2} \rfloor} \geq 2^{n-2}$. □

Proposition 6 includes the constructions of de Bruijn sequences from the PCR of order n in [17] as special cases. Taking $k \in \{0, 1, \operatorname{lcm}(1, 2, \ldots, n-1) - 1\}$ in the first rule in (9), for instance, outputs three sequences, including the PCR4 in [17] and `granddaddy`. Using the second rule in (9) with $k \in \{0, 1, \operatorname{lcm}(1, 2, \ldots, n-1) - 1\}$ yields sequences that include PCR3 (J1) in [17] and `grandmama`.

For the successor rules in Propositions 4 and 6, generating the next bit means checking if a state is a cycle's necklace by repeated simple left shifts. This can be done in $O(n)$ time and $O(n)$ space. We generalize Proposition 6 to define more successor rules.

Theorem 8. *Let $g(k) : \{1, 2, \ldots, n\} \mapsto \{0, 1, \ldots, k-1\}$ be an arithmetic function. As before, for any $\mathbf{c} := c_0, c_1, \ldots, c_{n-1}$, let $\mathbf{v} := 0, c_1, \ldots, c_{n-1}$ and $\mathbf{u} := c_1, \ldots, c_{n-1}, 1$. The following successor rules generate de Bruijn sequences of order n.*

$$\rho_{\mathrm{lz}}^g(\mathbf{c}) = \begin{cases} \overline{c_0}, \text{ if } L_{\mathrm{lz}}^{g(\mathrm{wt}(\overline{\mathbf{v}}))} \mathbf{v} \text{ is a necklace,} \\ c_0, \text{ otherwise.} \end{cases} \qquad \rho_{\mathrm{eo}}^g(\mathbf{c}) = \begin{cases} \overline{c_0}, \text{ if } L_{\mathrm{eo}}^{g(\mathrm{wt}(\mathbf{u}))} \mathbf{u} \text{ is a necklace,} \\ c_0, \text{ otherwise.} \end{cases} \tag{12}$$

For a cycle with $1 \leq \ell \leq n-1$ distinct LZ states, there are ℓ distinct ways to choose the uniquely determined state according to $g(\ell)$. The counting for ℓ distinct EO states is identical. It is then straightforward to confirm that each successor rule in Theorem 8 can generate $(n-1)!$ distinct de Bruijn sequences of order n by using all possible $g(\ell)$.

5 Conclusions

We have proposed a general design criteria for feasible successor rules. They perform the cycle joining method to output binary de Bruijn sequences. The focus of our demonstration is on their efficacy and efficiency when applied to the pure cycling register (PCR) of any order $n \geq 3$. Going beyond the often explored route of relying on the lexicographic ordering of the cycles, we have shown that many transitive relations can also be used to order the cycles. We have enumerated the respective output sizes of various specific successor rules that can be validly defined based on the general criteria. A straightforward complexity analysis has confirmed that generating the next bit in each resulting sequence is efficient.

We assert that the criteria we propose here can be applied to *all nonsingular FSRs*. If a chosen FSR has cycles with small least periods, then the complexity to produce the next bit can be kept low. Interested readers are invited to come up with feasible successor rules for their favourite FSRs. We intend to do the same and to further look into, among others, the cryptographic properties of the binary de Bruijn sequences produced by more carefully designed successor rules.

References

[1] N. G. de Bruijn, "A combinatorial problem," *Koninklijke Nederlandse Akademie v. Wetenschappen*, vol. 49, pp. 758–764, 1946.

[2] A. H. Chan, R. A. Games, and E. L. Key, "On the complexities of de Bruijn sequences," *J. Combinat. Theory, Ser. A*, vol. 33, no. 3, pp. 233 – 246, 1982.

[3] S. W. Golomb, *Shift Register Sequences*, 3rd ed. World Scientific, 2017.

[4] A. Ralston, "De Bruijn sequences - a model example of the interaction of discrete mathematics and computer science," *Math. Mag.*, vol. 55, no. 3, pp. 131–143, 1982.

[5] H. Fredricksen, "A survey of full length nonlinear shift register cycle algorithms," *SIAM Review*, vol. 24, no. 2, pp. 195–221, 1982.

[6] A. Lempel, "On a homomorphism of the de Bruijn graph and its applications to the design of feedback shift registers," *IEEE Trans. Comput.*, vol. C-19, no. 12, pp. 1204–1209, Dec 1970.

[7] A. Alhakim, "Spans of preference functions for de Bruijn sequences," *Discrete Appl. Math.*, vol. 160, no. 7, pp. 992 – 998, 2012.

[8] M. H. Martin, "A problem in arrangements," *Bull. Amer. Math. Soc.*, vol. 40, no. 12, pp. 859–865, Dec 1934.

[9] Z. Chang, M. F. Ezerman, and A. A. Fahreza, "On greedy algorithms for binary de Bruijn sequences," *Appl. Algebra Eng. Commun.*, vol. 33, pp. 523–550, Nov 2022.

[10] H. Fredricksen, "Generation of the Ford sequence of length 2^n, n large," *J. Combinat. Theory, Ser. A*, vol. 12, no. 1, pp. 153–154, Jan 1972.

[11] P. B. Dragon, O. I. Hernandez, J. Sawada, A. Williams, and D. Wong, "Constructing de Bruijn sequences with co-lexicographic order: The k-ary grandmama sequence,"

Eur. J. Comb., vol. 72, pp. 1–11, 2018.

[12] Z. Chang, M. F. Ezerman, S. Ling, and H. Wang, "On binary de Bruijn sequences from LFSRs with arbitrary characteristic polynomials," *Des. Codes Cryptogr.*, vol. 87, no. 5, pp. 1137–1160, May 2019.

[13] Y. Huang, "A new algorithm for the generation of binary de Bruijn sequences," *J. Algorithms*, vol. 11, no. 1, pp. 44–51, Mar 1990.

[14] T. Etzion and A. Lempel, "Algorithms for the generation of full-length shift-register sequences," *IEEE Trans. Inform. Theory*, vol. 30, no. 3, pp. 480–484, May 1984.

[15] C. Jansen, W. Franx, and D. Boekee, "An efficient algorithm for the generation of de Bruijn cycles," *IEEE Trans. Inform. Theory*, vol. 37, no. 5, pp. 1475–1478, 1991.

[16] J. Sawada, A. Williams, and D. Wong, "A surprisingly simple de Bruijn sequence construction," *Discrete Math.*, vol. 339, no. 1, pp. 127–131, Jan 2016.

[17] D. Gabric, J. Sawada, A. Williams, and D. Wong, "A framework for constructing de Bruijn sequences via simple successor rules," *Discrete Math.*, vol. 341, no. 11, pp. 2977–2987, Nov 2018.

[18] J. Sawada, A. Williams, and D. Wong, "A simple shift rule for k-ary de Bruijn sequences," *Discrete Math.*, vol. 340, no. 3, pp. 524–531, Mar 2017.

[19] Y. Zhu, Z. Chang, M. F. Ezerman, and Q. Wang, "An efficiently generated family of binary de Bruijn sequences," *Discrete Math.*, vol. 344, no. 6, 112368, Jun 2021.

[20] D. Gabric, J. Sawada, A. Williams, and D. Wong, "A successor rule framework for constructing k-ary de Bruijn sequences and universal cycles," *IEEE Trans. Inform. Theory*, vol. 66, no. 1, pp. 679–687, Jan 2020.

[21] P. Halmos, *Naive Set Theory*, ser. Undergraduate Texts in Mathematics. Springer, New York, 1974.

[22] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: for Wireless Communication, Cryptography, and Radar*. Cambridge Univ. Press, New York, 2004.

[23] R. Lidl and H. Niederreiter, *Finite Fields*, ser. Encyclopaedia of Mathematics and its Applications. Cambridge Univ. Press, New York, 1997.

[24] K. S. Booth, "Lexicographically least circular substrings," *Inform. Process. Lett.*, vol. 10, no. 4-5, pp. 240–242, Jul 1980.

[25] T. Peters. [python-dev] Sorting. [Online]. Available: https://mail.python.org/pipermail/python-dev/2002-July/026837.html

[26] P. McIlroy, "Optimistic sorting and information theoretic complexity," in *Proc.* 4th *ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 1993, pp. 467–474.

[27] S. Buss and A. Knop, "Strategies for stable merge sorting," in *Proc.* 13th *ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2019, pp. 1272–1290.

[28] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*. World Scientific, Singapore, 1996.

[29] B. Farhi, "An identity involving the least common multiple of binomial coefficients and its application," *Amer. Math. Monthly*, vol. 116, no. 9, pp. 836–839, 2009.

On the linear complexity of shrunken sequences

Ana I. Gómez
Universidad Rey Juan Carlos
Móstoles, Madrid, Spain
ana.gomez.perez@urjc.es

Domingo Gómez-Pérez
Universidad de Cantabria
Santander, Spain
domingo.gomez@unican.es

Verónica Requena
Universidad de Alicante
Alicante, Spain
vrequena@ua.es

Abstract

The shrinking generator is a pseudorandom bit generator based on the combination of two linear feedback shift registers of maximum period. These registers are synchronized with a common clock and produce binary sequences with good statistical properties. Due to its simplicity and efficient implementation, the shrinking generator is particularly suitable for stream cipher cryptographic schemes and most proposed attacks rely on the properties of the generator. Consequently, its analysis serves as the foundation for other interleave constructions. In our work, we present a closed formula for the linear complexity of its output. Additionally, we establish the first bound on its linear complexity profile. Our techniques involve two-dimensional arrays and their interleave structure, which could prove valuable for other pseudorandom bit generators.

1 Introduction

Pseudo-Random Number Generators (PRNGs) are deterministic algorithms [10, 21] used to generate number sequences which appear to be random. They are employed for cryptographic applications such as key and nonce generation, digital signatures, masking protocols, IoT security, etc.

Linear Feedback Shift Registers (LFSRs) play an important part in the design of cryptographic PNRGs [15, 23]. Binary sequences generated by maximal-period LFSRs, whose characteristic polynomial is primitive, are called PN-sequences or m-sequences [13]. These have been extensively used in many and diverse applications such as e-Commerce, mobile wireless communications, digital broadcasting, or cryptography (stream ciphers) [3, 20], because they exhibit the largest possible period and present good randomness

properties such as balancedness, low correlation, excellent run distribution, and so forth. However, they are easily predictable due to their inherent linearity. In order to ensure their cryptographic suitability, maintaining at the same time the pseudorandomness properties, different design techniques are applied: non-linear filtering, combinatorial generators, clock-controlled generators, or the irregular decimation of PN-sequences, among others. We focus our attention on the latter.

Irregularly decimating the output sequences of m-sequences generates powerful PN-RGs [9] i.e. it produces sequences with good cryptographic properties. One of the most important generators in this family is the *shrinking generator (SG)* [8], built from two LFSRs with different lengths. This generator is fast, easy to implement, and generates good cryptographic sequences, which is appropriated for efficient applications in low-end devices such as stream cipher cryptosystems [2, 4, 9]. A great family of decimation-based sequence generators have emerged from the former: the self-shrinking generator [19], the generalized self-shrinking generator [16], the modified self-shrinking generator [17], and the t-modified self-shrinking generator [7]. Each of these generators are based on same principle, with different approaches to avoid certain attacks to the linearity of the construction. We focus on the shrinking generator, because it is the original architecture of the generators as a starting study that we hope can be extended for the derived families.

The row by row (snake like) folding of a sequences produces arrays which are useful in single periodic or aperiodic applications. This structure in the shrinking generator was explored by Cardell et al. [6] in order to characterize the cryptographic related properties.

Our analysis is based on the transformation of sequences into arrays using the Chinese remainder theorem (CRT). This is equivalent to folding a sequence along the leading diagonal of an array whose dimensions are relatively prime. The equivalence in this case between both array construction methods has already been studied and understood [14]. This implies that in the case of a sequence built by the shrinking generator the columns are cyclic shifts of a shorter m-sequence. This fundamental difference to the row by row folding is crucial to study the properties of the array.

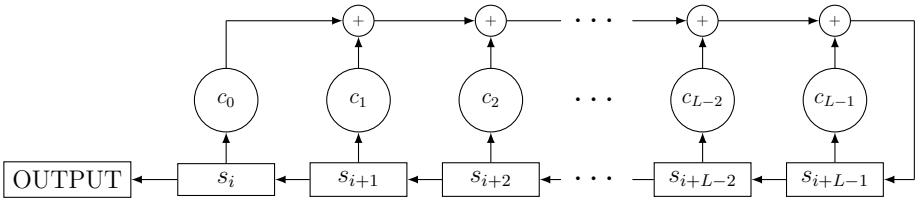
This paper is structured as follows: Section 2 introduces the necessary background and presents the main theorem of our study. In Section 3, we provide the proof of the main result with a detailed and rigorous justification for our theorem. Finally, we finish the paper with conclusions and future works in Section 4, where we summarize our findings and suggest potential directions for future research

2 Mathematical Preliminaries and main result

Let $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ be the set of nonnegative integers and $\mathbb{F}_2 = \{0, 1\}$ the Galois field of two elements. A *binary sequence* (s_i) is a mapping from $\mathbb{N}_0$ to $\mathbb{F}_2$. It is *periodic* if there exists a positive integer T such that $s_{i+T} = s_i$, for all $i \in \mathbb{N}_0$.

A linear feedback shift register (LFSR) [13] is an electronic device with L memory cells (stages) with binary content. At every clock pulse, the binary element of each stage is shifted to the adjacent one and a new element is computed through the linear feedback to fill the empty stage (see Figure 1).

Figure 1: LFSR of length L



We present the definition of two security metrics for sequences which rely on LFSRs: the *linear complexity* and the *linear complexity profile*.

Definition 1. Let L be a positive integer and $c_0, c_1, \ldots, c_{L-1} \in \mathbb{F}_2$. A binary sequence $\mathbf{s} = (s_i)$ satisfying

$$s_{i+L} = \sum_{j=0}^{L-1} c_j s_{i+j}, \tag{1}$$

for all $i \in \mathbb{N}_0$ is called an (L-th order) *linear recurring sequence (LRS)* and the monic polynomial

$$C(x) = x^L + \sum_{j=0}^{L-1} c_j x^j \in \mathbb{F}_2[x]$$

is the *characteristic polynomial* of the recurrence and we say that the sequence is generated by $C(x)$. The minimal order of an LRS is called *linear complexity* and denoted by $L(\mathbf{s})$, that describes the unique *minimal polynomial*. This is equivalent to the shortest LFSR that generates such a sequence.

The *linear complexity profile* denoted by $L(\mathbf{s}, N)$ is the function depending on N that outputs the smallest order L such that $s_0, \ldots, s_{N-1}$ are the first elements of the L-th order LRS.

In cryptographic applications, the linear complexity must be large and resemble the expected value of a random sequence, which is approximately half the period, that is, $L(\mathbf{s}) \simeq T/2$ [22]. It is clear that a low linear complexity implies the sequence is predictable [5, 12, 18]. However, it fails to capture irregularities in part of the sequence, that can be detected by the linear complexity profile. The latter is a non-decreasing function on N and, for a T-periodic sequence $\mathbf{s}$, $L(\mathbf{s}) = L(\mathbf{s}, 2T)$.

A linear recurring sequence generated by an LFSR of order L such that its least period is $2^L - 1$ is called *maximal length sequence* or *m-sequence*. These kind of sequences are easily generated using the *trace function*. For $\mathbb{F}_{2^L}$, the Galois field of 2^L elements, we consider the trace function:

$$\mathrm{Tr}(x) = \sum_{i=0}^{L-1} x^{2^i}.$$

We recall the following properties for m-sequences, which can be found in [13, Definition 4.6, Corollary 4.6, Property 5.3, Theorem 5.3]. We denote the polynomial rings $\mathbb{F}_2[x] \subset \mathbb{F}_2[x, y]$.

Proposition 2. *Let (a_i) be an m-sequence generated by a polynomial $p(x) \in \mathbb{F}_2[x]$ of degree L. It satisfies the following statements:*

- *Its period is $T = 2^L - 1$.*
- *The number of ones occurring within a period is $2^{L-1} = {}^{(T+1)}/_2$ and the number of zeros is $2^{L-1} - 1 = {}^{(T-1)}/_2$.*
- *It has the shift-and-add property, i.e. for any $k_1, k_2 \in \mathbb{N}_0$, either $a_{i+k_1} + a_{i+k_2} = 0$ for every $i \in \mathbb{N}_0$ or there exists $k_3 \in \mathbb{N}_0$ such that the sum equals a_{i+k_3} for every $i \in \mathbb{N}_0$.*
- *For a primitive element $\alpha \in \mathbb{F}_{2^L}$, there exists $k \in \mathbb{N}_0$ such that $a_i = \mathrm{Tr}(\alpha^{i+k})$ for every $i \in \mathbb{N}_0$.*

In order to define a *shrunken sequence*, we consider two m-sequences (a_i) and (b_i) with characteristic polynomials $p_1(x), p_2(x) \in \mathbb{F}_2[x]$ of degrees L_1 and L_2, with $L_1 \leq L_2$. We restrict ourselves to the case $\gcd(L_1, L_2) = 1$, so that the periods $2^{L_1} - 1$ and $2^{L_2} - 1$ are coprime as well. The *shrinking generator* is the decimation of (b_i) by (a_i), i.e. the subsequence of (b_i) that selects only indices for which $a_i = 1$. In other words, ordering increasingly the set $I = \{i \in \mathbb{N}_0 \mid a_i = 1\}$, we obtain a sequence (i_j) in $\mathbb{N}_0$. The shrinking generator output is the sequence given by (b_{i_j}) with $i_j \in I$, denoted by $\mathbf{s} = (s_j)$. It is called shrunken sequence and its least period is $(2^{L_2} - 1)2^{L_1 - 1}$. Regarding the linear complexity, the only known bounds are $L_2 2^{L_1 - 2} < L(\mathbf{s}) \leq L_2 2^{L_1 - 1}$ [8]. However, those bounds are not tight and it has been an open problem to calculate it theoretically.

Moreover, Fuster-Sabater and Caballero Gil [11] prove that the minimal polynomial is of the form $(p(x))^m$, where $2^{L_1 - 2} < m \leq 2^{L_1 - 1}$ and $p(x)$ is the minimal polynomial of (b_i). The main result of this paper is the following one. The proof is given in Section 3.

Theorem 3. *The linear complexity of a shrunken sequence* $\mathbf{s}$ *is*

$$L(\mathbf{s}) = L_2 \cdot 2^{L_1 - 1}, \quad \textit{when } 2^{L_1} \cdot (2^{L_1} - 1) < L_2.$$

Under the same assumptions, the linear complexity profile $L(\mathbf{s}, N)$ is equal to $L(\mathbf{s})$ if $N > L_2 \cdot 2^{L_1}$.

A *two-dimensional array* of periods n_1 and n_2 is a mapping $\mathbf{A} : \mathbb{N}_0^2 \to \mathbb{F}_2$ satisfying $\mathbf{A}(\alpha_1 + n_1, \alpha_2 + n_2) = \mathbf{A}(\alpha_1, \alpha_2)$, for every $(\alpha_1, \alpha_2) \in \mathbb{N}_0^2$.

The *composition method* is able to construct a two-dimensional array from an initial sequence and a shift sequence, see for example [14]. It starts from an n_1-periodic binary sequence (e_i) and a n_2-periodic integer sequence (t_j), referred as *column* and *shift*, respectively. The resulting array is defined by

$$\mathbf{A}(i, j) = e_{i - t_j}. \tag{2}$$

If the periods n_1 and n_2 are coprime, the diagonal $s_j = \mathbf{A}(j \mod n_1, j \mod n_2)$ covers the whole array by the Chinese Remainder Theorem. This transformation is called *unfolding* of an array and the result is the *unfolded sequence*.

The following result, which is a consequence of [6, Proposition 2], shows that any shrunken sequence is the unfolding of an array obtained by the composition method. While the original result applies to the row by row or interleave method, it is possible to transform from interleave method to the composition method in many cases [14]. We recall that, for an m-sequence with period $2^{L_1} - 1$, the number of ones within a period is 2^{L_1-1}.

Proposition 4 ([6, 14])**.** *Let L_1, L_2 be coprime positive integers with $L_1 < L_2$ and let (a_i), (b_i) be m-sequences with (coprime) periods $T_1 = 2^{L_1} - 1$ and $T_2 = 2^{L_2} - 1$. Let $\delta \in \{1, \ldots, T_2 - 1\}$ such that $T_1 \cdot \delta = 2^{L_1-1} \mod T_2$. Denote by (i_j) the sequence of indices belonging to the set I defined previously, i.e. $a_{i_j} = 1$ and define the (2^{L_1-1})-periodic sequence*

$$t_j = \delta \cdot i_j - j \mod T_2.$$

Then, the shrunken sequence is the result of unfolding the array given by the composition of (b_i) and (t_j).

Let us recall the definition of linear complexity for two-dimensional arrays [1].

Definition 5. A polynomial $C = \sum_{(\alpha_1,\alpha_2)\in S\subset\mathbb{N}_0^2} c_{\alpha_1,\alpha_2} x^{\alpha_1} y^{\alpha_2} \in \mathbb{F}_2[x, y]$ is *valid* for the two-dimensional array $\mathbf{A}$ when the equation

$$\sum_S c_{\alpha_1,\alpha_2}\, \mathbf{A}(\alpha_1 + \beta_1, \alpha_2 + \beta_2) = 0 \tag{3}$$

holds for every $\beta_1, \beta_2 \in \mathbb{N}_0$. In this case, we also say that $\mathbf{A}$ *satisfies* the two-dimensional linear recurrence relation given by C. If it holds for specific β_1, β_2, we say that the equation is valid at (β_1, β_2) for $\mathbf{A}$. For the case of periodic two-dimensional arrays, the set of all valid polynomials forms a zero-dimensional ideal and the number of solutions counting its multiplicity in the algebraic closure is known as the *linear complexity* of the array.

We finish this section summarizing some known facts about the linear complexity of arrays and its relation with that of the corresponding unfolded sequences [1].

Proposition 6. *Given $\mathbf{A}$, (e_i), and (t_j), defined as in Equation (2), the following facts hold:*

1. *If a polynomial in $\mathbb{F}_2[x]$ is valid for $\mathbf{A}$, it is a multiple of the minimal polynomial of (e_i).*
2. *The minimal polynomial of the unfolded sequence is the smallest-degree polynomial $D(z)$ such that $D(xy)$ is valid for $\mathbf{A}$.*
3. *The linear complexity of $\mathbf{A}$ equals that of its unfolded sequence.*

Proof. For the first item, suppose that $C(x)$ is valid for $\mathbf{A}$, then

$$\sum_S c_{\alpha_1} \mathbf{A}(\alpha_1 + \beta_1, \beta_2) = 0.$$

Taking into account Equation (2)

$$\sum_S c_{\alpha_1} e_{\alpha_1+\beta_1+t_{\beta_2}} = 0,$$

which implies that it is a characteristic polynomial of (e_i), i.e. it is a multiple of the minimal polynomial of (e_i).

For the second item, the unfolded sequence $s_i = \mathbf{A}(i \mod n_1, i \mod n_2)$ for all $j \in \mathbb{N}_0$. A characteristic polynomial for (s_i), $D(z)$, satisfies

$$0 = \sum_{j=0}^{L} d_j s_{i+j} = \sum_{j=0}^{L} d_j \mathbf{A}(i+j \mod n_1, i+j \mod n_2),$$

which implies that the polynomial $D(xy)$ is valid for $\mathbf{A}$ by Equation (3). The last item is proven in [1] and this finishes the proof. □

3 Proof of the main result

We are ready to prove Theorem 3. The shrunken sequence defined by the m-sequences (a_i) and (b_i), with minimal polynomials $p_1(x)$ and $p_2(x)$ of degrees L_1 and L_2, is, according to Proposition 4, the unfolding of an array. Namely, of $\mathbf{A}(i, j) = b_{i-t_j}$, which is obtained as the composition of (b_i), with period $T_2 = 2^{L_2} - 1$, and a shift sequence (t_j), whose period is $\tau = 2^{L_1-1}$.

We will prove that the ideal of valid polynomials for the array is $(p_2(x), y^\tau - 1)$, from where the theorem's first statement follows. On one hand, it is straightforward that $p_2(x), y^\tau - 1$ are valid polynomials.

On other hand, any valid polynomial is in the ideal, note that

$$(y+1)^\tau = y^\tau - 1 \qquad \text{and} \qquad (y+1)^{\tau-1} = 1 + y + y^2 + \cdots + y^{\tau-1}.$$

We consider firstly a valid polynomial in $\mathbb{F}_2[x]$. By the first item of Proposition 6, it must be a multiple of $p_2(x)$. Suppose that there exists a valid polynomial not in the ideal above. We can assume that it takes the form

$$C(x, y) = \sum_{i=0}^{\tau-1} C_i(x)(y+1)^i \qquad (\deg C_i(x) < \deg p_2(x),\ \forall i),$$

with at least one index i for which $C_i(x) = \sum_i c_i x^i$ is not the zero polynomial. Let n be the lowest of those indices. Then, we have

$$(y+1)^{\tau-1-n}\ C(x, y) = C_n(x)(y+1)^{\tau-1} + D(x, y)(y+1)^\tau,$$

so that $C_n(x)(y+1)^{\tau-1} = \sum_i \sum_{j=0}^{\tau-1} c_i x^i y^j$ is valid. In particular, for every $l = 0, \ldots, T_2 - 1$, it holds at $(l, 0)$. Fix a primitive element $\alpha \in \mathbb{F}_{2^{L_2}}$. According to Proposition 2, there exists $k \in \mathbb{N}_0$ such that $b_i = \mathrm{Tr}(\alpha^{i+k})$, for every $i \in \mathbb{N}_0$. Then, for every index l,

$$0 = \sum_{i=0}^{L_2-1} \sum_{j=0}^{\tau-1} c_i b_{i+l-t_j} = \mathrm{Tr}\left(\alpha^{k+l} \sum_{i=0}^{L_2-1} c_i \alpha^i \sum_{j=0}^{\tau-1} \alpha^{-t_j} \right) = 0.$$

The power set $\{\alpha^{k+l} \mid l = 0, \ldots, T_2 - 1\}$ equals the whole $\mathbb{F}_{2^{L_2}}^*$. Therefore, it must be

$$\left(\sum_{i=0}^{L_2-1} c_i \alpha^i \right) \left(\sum_{j=0}^{\tau-1} \alpha^{-t_j} \right) = 0.$$

Since $C_n(x)$ is not zero, neither is the first factor. Writing $T_1 = 2^{L_1} - 1$ and (i_j) and δ as in Proposition 4, we get

$$0 = \sum_{j=0}^{\tau-1} \alpha^{j-\delta \cdot i_j} = \sum_{j=0}^{\tau-1} (\alpha')^{T_1 \cdot (j-\delta \cdot i_j)} = \sum_{j=0}^{\tau-1} (\alpha')^{(2\cdot\tau-1)\cdot j - \tau \cdot i_j}$$

so that α' is a root of $G(x) = x^{(2\tau-1)\cdot\tau} \sum_{i=0}^{\tau-1} x^{(2\cdot\tau-1)\cdot j - \tau \cdot i_j}$, where $(\alpha')^{T_1} = \alpha$. However, the polynomial $G(x)$ has degree less than $2 \cdot \tau \cdot (2 \cdot \tau - 1)$ but this is a contradiction with the fact that α' is a primitive root and its minimal polynomial has degree L_2. This completes the proof of the first statement.

For the other one, for $N > L_2(2^{L_1-1})$, we are going to calculate $L(\mathbf{s}, N)$. Take a linear recurrence that holds for N points of sequence $\mathbf{s}$, then there is a characteristic polynomial $p(z)$ associated to the linear recurrence. The first N positions of the sequence $\mathbf{s}$ evenly spaced with constant separation in the array $\mathbf{A}$, then at least L_2 points in each column corresponds to the first N elements of the sequence. Due to the fact that each column is the m-sequence (b_i) with $p_2(x)$ then $\mathbf{A}$ can be reconstructed, therefore $p(z)$ is a characteristic polynomial for $\mathbf{s}$ and $\deg p(x) \geq L(\mathbf{s})$. This finishes the proof.

4 Conclusions and future work

In this paper, we have a obtained the exact value of the linear complexity of shrunken sequences under a certain condition. We conjecture that this result holds on a more general settings, due to observation of computer experiments carried on. As far as we know, this work is also the first one which studies the linear complexity profile of shrunken sequences and provides an initial bound. Our computational experiments also suggest that the linear complexity is maximal, even in parts of the sequence, when sufficient number of terms are taken. This fact limits the applicability of attacks based on the linear structure of the sequence, given a more stronger security than initially expected.

Further studies on the linear complexity of the generalized sequences are left as an open problem. The starting point could be to analyse several computational simulations on the linear complexity and the linear complexity profile.

As a future work, we would like to obtain some improved bounds for these sequences; and, also to study the linear complexity profile for the other families of decimation-based sequences generators. Results on this direction may lead to establish a relation between arrays and these families of sequences, which could help to deepen the understanding of these generators and obtain stronger results in statistical properties like number of runs, balancedness, etc.

Acknowledgements

The work of the second author was supported by Protocolos Seguros En Redes Descentralizadas (Ayuda Financiada Contrato Programa Gob Cantabria -UC). The work of the third author was partially supported by the I+D+i project VIGROB-287 of the Universitat d'Alacant.

References

[1] Rafael Arce-Nazario, Francis Castro, Domingo Gomez-Perez, Oscar Moreno, José Ortiz-Ubarri, Ivelisse Rubio, and Andrew Tirkel. Multidimensional linear complexity analysis of periodic arrays. *Applicable Algebra in Engineering, Communication and Computing*, 31:43–63, 2020.

[2] Côme Berbain, Olivier Billet, Anne Canteaut, Nicolas Courtois, Henri Gilbert, Louis Goubin, Aline Gouget, Louis Granboulan, Cédric Lauradoux, Marine Minier, Thomas Pornin, and Hervé Sibert. Sosemanuk, a fast software-oriented stream cipher. In Matthew Robshaw and Olivier Billet, editors, *New Stream Cipher Designs: The eSTREAM Finalists*, pages 98–118, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[3] Alex Biryukov and Leo Perrin. State of the art in lightweight symmetric cryptography. Cryptology ePrint Archive, Report 2017/511, 2017. https://ia.cr/2017/511.

[4] Susil Kumar Bishoi, Kedarnath Senapati, and BR Shankar. Shrinking generators based on σ-LFSRs. *Discrete Applied Mathematics*, 285:493–500, 2020.

[5] Simon R. Blackburn. The linear complexity of the self-shrinking generator. *IEEE Transactions on Information Theory*, 45(6):2073–2077, 1999.

[6] Sara D. Cardell, Diego F. Aranha, and Amparo Fúster-Sabater. Recovering decimation-based cryptographic sequences by means of linear CAs. *Logic Journal of the IGPL*, 28(4):430–448, 2020.

[7] Sara D. Cardell and Amparo Fúster-Sabater. The t-modified self-shrinking generator. In Yong Shi, Haohuan Fu, Yingjie Tian, Valeria V. Krzhizhanovskaya, Michael Harold Lees, Jack Dongarra, and Peter M. A. Sloot, editors, *Computational Science – ICCS 2018*, pages 653–663, Cham, 2018. Springer International Publishing.

[8] Don Coppersmith, Hugo Krawczyk, and Yishay Mansour. The shrinking generator. In Douglas R. Stinson, editor, *Advances in Cryptology — CRYPTO' 93*, pages 22–39, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.

[9] Sara D. Cardell and Amparo Fúster-Sabater. *Cryptography with Shrinking Generators: Fundamentals and Applications of Keystream Sequence Generators Based on Irregular Decimation*. Springer Briefs in Mathematics. Springer International Publishing, 2019.

[10] Elena Dubrova and Martin Hell. Espresso: A stream cipher for 5g wireless communication systems. *Cryptography and Communications*, 9:273–289, 2017.

[11] Amparo Fúster-Sabater and Pino Caballero-Gil. Linear solutions for cryptographic nonlinear sequence generators. *Physics Letters A*, 369(5–6):432–437, 2007.

[12] Amparo Fúster-Sabater and Sara D. Cardell. Linear complexity of generalized sequences by comparison of PN-sequences. *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Ser. A. Matemáticas (RACSAM)*, 114(4):79–97, 2020.

[13] Solomon W Golomb and Guang Gong. *Signal design for good correlation for Wireless Communication, Cryptography, and Radar*. Cambridge University Press, 2005.

[14] Ana I Gómez, Domingo Gómez-Pérez, and Andrew Tirkel. Generalised gmw sequences. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 1806–1811. IEEE, 2021.

[15] Shabbir Hassan and Mohammad Ubaidullah Bokhari. Design of pseudo random number generator using linear feedback shift register. *International Journal of Engineering and Advanced Technology (IJEAT)*, 9(2):1956–1965, 2019.

[16] Yupu Hu and Guozhen Xiao. Generalized self-shrinking generator. *IEEE Trans on Information Theory*, 50(4):714–719, 2004.

[17] Ali Kanso. Modified self-shrinking generator. *Computers & Electrical Engineering*, 36(5):993–1001, 2010.

[18] Edwin L. Key. An analysis of the structure and complexity of nonlinear binary sequence generators. *IEEE Transactions on Information Theory*, 22(6):732–736, 1976.

[19] Willi Meier and Othmar Staffelbach. The self-shrinking generator. In Alfredo De Santis, editor, *Advances in Cryptology — EUROCRYPT'94*, pages 205–214, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

[20] Amalia Beatriz Orúe López, Luis Hernández Encinas, Agustín Martín Muñoz, and Fausto Montoya Vitini. A lightweight pseudorandom number generator for securing the internet of things. *IEEE Access*, 5:27800–27806, 2017.

[21] Orúe López, Amalia Beatriz, Luis Hernández Encinas, and Fausto Montoya Vitini. Trifork, a new pseudorandom number generator based on lagged Fibonacci maps. *Journal of Computer Science and Engineering*, 2(2):46–51, 2010.

[22] F. Pichler, editor. *Linear Complexity and Random Sequences*, volume 219 of *Lecture Notes in Computer Science*. Springer-Verlag, 1986.

[23] Hamed Rahimov, Majid Babaei, and Mohsen Farhadi. Cryptographic PRNG based on combination of LFSR and chaotic logistic map. *Applied Mathematics*, 2:1531–1534, 2011.

Keynote Talk: Recent Advances in Signal Design for Integrated Sensing & Communications

Pingzhi Fan

Southwest Jiaotong University, Chengdu, China

Abstract. Integrated Sensing and Communication (ISAC) combines sensing and communication systems to utilize wireless resources efficiently, realize wide area environment sensing, and even to pursue mutual benefits. It is anticipated that ISAC would be one of the key enablers of 5G Advanced (5GA) and 6G wireless networks for supporting a variety of emerging applications. Obviously, transmitting signal design plays an essential role in ISAC systems. This talk shall provide recent advances in ISAC signal designs, including coordinated signal design, communications signal-based design, radar signal-based design, and dedicated dual-function signal design. In particular, a new concept called low ambiguity zone (LAZ) and some theoretical bounds, as well as related LAZ signal designs, shall be presented.

Construction of Cross Z-complementary Sequence Set with Large CZC Ratio

Kai Liu *, Qinghai Xu, Xin Meng

School of Information Science and Engineering
Yanshan University
Qinhuangdao, China.

liukai@ysu.edu.cn

Abstract

Cross Z-complementary pairs/sequences (CZCPs/CZCSs) are widely used for training sequences in spatial modulation (SM) systems and can achieve superior channel estimation performance in frequency-selective channels, whose aperiodic correlation sums appear as zero correlation zones at both the front-end and back-end offsets of the sequences. Nevertheless, the ZCZ length of the binary CZCP is restricted to half of its length, while the CZCS can result in a larger increase in ZCZ length, and is suitable for SM systems against larger delay expansion. This paper proposes a class of optimal CZCS sets (CZCSSs) with flexible ZCZ length by employing CZCPs and Hadamard products. To improve the parameters of CZCPs, two novel classes of CZCPs are introduced through concatenation construction. The construction results yield new parameters and expand the pool of training sequences available for SM systems.

1 Introduction

Spatial modulation (SM) is a category of MIMO modulation techniques. Multiple transmit antenna (TA) elements are present in an SM system, but only one radio frequency (RF) chain. Within each time slot, the SM symbol can be divided into two parts: one part is called the "spatial symbol", which is responsible for selecting and activating TA elements, and the other part is called the "constellation symbol", which is selected from traditional PSK/QAM constellations and transmitted from active TA elements. "Single RF chain" of SM in principle doesn't permit the transmitter to transmit using the pilots on all TAs simultaneously, so the dense training sequence of conventional MIMO in [13]-[15] is not applicable to SM systems. For this reason, Liu proposed cross Z-complementary

*The authors are supported in part by the Natural Science Foundation of Hebei Province under Grant F2023203066, and in part by the Key Laboratory Project of Hebei Province, China under Grant 202250701010046.

pairs (CZCPs) that can be applied to SM training sequences [4]. The idea of CZCPs is derived from Golay complementary pairs (GCPs) [3] and Z-complementary pairs (ZCPs) [1], which have aperiodic auto-correlation sums (AACSs) for front-end and tail-end ZCZ, as well as aperiodic cross-correlation sums (ACCSs) for tail-end ZCZ. Liu also pointed out that the ZCZ length of CZCP cannot exceed $N/2$, where N is the sequence length. When the ZCZ length reaches half of the sequence length, it is called a perfect CZCP. Cross Z-complementary ratio (CZC_{ratio}) is defined in [5] as the ratio of ZCZ length Z to the maximum possible ZCZ width Z_{max}. When $CZC_{ratio} = 1$, it is referred to as the optimal CZCP. Multiple CZCPs with different CZC_{ratio} are constructed in [4], [5], [8]-[11]. Recently, CZCPs have been expanded to CZCSs[12] and CZCSSs[2].

In the literature, binanry quaternary and q-ary CZCPs have been developed. Adhikary used the insertion method to indirectly construct a number of binary CZCPs with larger CZC_{ratio} [5]. He also used Barker codes to construct a class of optimal binary CZCPs and extended the length of binary CZCPs through the Turyn method. Fan proposed several types of binary CZCPs with parameters $(10^{\beta}, 4 \times 10^{\beta-1})$,$(26^{\gamma}, 12 \times 26^{\gamma-1})$,$(10^{\beta}26^{\gamma}, 12 \times 10^{\beta}26^{\gamma-1})$[8], which are also GCPs. Huang used Boolean functions (BFs) to directly construct binary CZCPs, whose $CZC_{ratio} \approx 2/3$[9]. In [10], binary CZCPs of different lengths were constructed using ZCPs and the concatenation method, with the largest CZC_{ratio} being . Zhang searched for the optimal seed CZCP sequence by computer and then constructed binary CZCPs with a larger CZC_{ratio} by combining GCPs and Kronecker products [11]. In [10] and [18], binary CZCPs were mapped to quaternary CZCPs.Liu constructed an optimal q-ary CZCP with a length of $2^m (m \geq 4)$ based on generalized Boolean functions (GBFs) [4], whereas Adhikary constructed a non-optimal q-ary CZCP with a length of $2^{m-1} (m \geq 4)$ using GBFs [5].To extend the ZCZ length, the concept of CZCS is introduced as the extension of CZCP [4].Kumar directly constructed $(2^{n+1}, 2^{n+1}, 2^{m-1} + 2, 2^{\pi(m-3)} + 1)$-CZCSS using GBFs [2].In this paper, we also propose two methods for constructing CZCPs using concatenation techniques. Based on the literature and our constructed CZCPs, a class of indirect construction methods for CZCSS is proposed, where the set parameters can be optimized

The rest of this paper is organized as follows. In part two, the basic definitions of CZCP and CZCSS are introduced. In part three, two constructions of CZCPs are constructed and CZCSS, and the parameters of constructed results are compared to the literature. A conclusion will then be presented.

2 Basic Concepts

Let a and b be two complex sequences of length N, some notations are given as follows:

- $a \parallel b$ represents the concatenation of the sequences a and b;
- $\overleftarrow{a}$ represents the reverse of a;
- a^* represents the complex conjugate of a. Definition 1: Let $a = (a_0, a_1, \cdots, a_{N-1})$ and $b = (b_0, b_1, \cdots, b_{N-1})$ be two sequences of length N, and the aperiodic correlation

function of and is defined as

$$\rho_{a,b}(\tau)=\begin{cases}\sum_{i=0}^{N-1-\tau}a_ib_{i+\tau}^*, 0\le\tau\le N-1,\\ \sum_{i=0}^{N-1-\tau}a_{i-\tau}b_i^*, -(N-1)\le\tau<0,\\ 0, |\tau|\ge N.\end{cases}\tag{1}$$

If $a\neq b$, $\rho_{a,b}(\tau)$ is called the aperiodic cross-correlation function (ACCF) of a and b; if $a=b$, $\rho_{a,a}(\tau)$ is called the aperiodic auto-correlation function (AACF) of a, represented by $\rho_a(\tau)$.

Definition 2[3]: If the AACF sum of sequences a and b of length N satisfies $\rho_a(\tau)+\rho_b(\tau)=0$ for $1\le\tau\le N-1$, then (a,b) is called GCP.

Definition 3[6]: Let (a,b) and (c,d) be two GCPs of length N if $\rho_{a,c}(\tau)+\rho_{b,d}(\tau)=0$ for $0\le\tau\le N-1$, then (a,b) and (c,d) are referred to as mate each other.

Definition 4[2]: Given a set $S=\{S^0,S^1,\ldots,S^{K-1}\}$, where each element set S^p is composed of M sequences, namely $S^p=\{s_0^p,s_1^p,\ldots,s_{M-1}^p\}$, $s_l^p=(s_{l,t}^p,0\le t<N)$, where $0\le p\le K-1$, $0\le l\le M-1$. If the set S satisfies the following properties:

$$\begin{aligned}&P1:\sum_{i=0}^{M-1}\rho(s_i^p)(\tau)=0,\ |\tau|\in(V_1\cup V_2)\cap V;\\ &P2:\sum_{i=0}^{M-1}\rho(s_i^p,s_{i+1}^p)(\tau)=0,|\tau|\in V_2;\\ &P3:\sum_{i=0}^{M-1}\rho(s_i^p,s_i^{p'})(\tau)=0,|\tau|\in\{0\}\cup V_1\cup V_2;\\ &P4:\sum_{i=0}^{M-1}\rho(s_i^p,s_{i+1}^{p'})(\tau)=0,|\tau|\in\cup V_2\end{aligned}\tag{2}$$

It is called a (K,M,N,Z)-CZCSS, where $s_M^p=s_0^p$, $s_M^{p'}=s_0^{p'}$, $p\neq p'$, $V_1=\{1,2,\ldots,Z\}$, $V_2=\{N-Z,N-Z+1,\ldots,N-1\}$, $Z\le N$. If $K=1$, then S is reduced to a CZCS [12]. If $K=1$ and $M=2$, S is then converted to a CZCP.

According to Definition 4, P1 indicates that each CZCP needs to have two zero auto-correlation zones (ZACZs) when considering AACS. They are referred to in this paper as the "front-end ZACZ" and "tail-end ZACZ" with time-shift on V_1 and V_2, respectively. When evaluating ACCS, P2 indicates that each CZCP needs to have a "tail-end zero cross correlation zone (ZCCZ)".

Definition 5: Let (a_0,b_0) and (a_1,b_1) be two CZCPs of length N. If $\rho_{a_0,a_1}(\tau)+\rho_{b_0,b_1}(\tau)=0$ for $\forall\tau$ and $\rho_{a_0,b_1}(\tau)+\rho_{b_0,a_1}(\tau)=0$ for $\tau\in V_2$, they are called mate of CZCPs.

Definition 6[5]: Let (a,b) be a CZCP with length N and a ZCZ length of Z. If the maximum achievable length of Z is $Z_{\max}$, then define $CZC_{ratio}=Z/Z_{\max}$. When $CZC_{ratio}=1$, CZCP is deemed optimal.

When the length of binary CZCPs is $N=2^\alpha10^\beta26^\gamma$, Z is $N/2$, otherwise it is $N/2-1$[10].

Lemma 1[19]: For a (K,M,N,Z)-CZCSS $S=\{S^0,S^1,\ldots,S^{K-1}\}$, the upper bound on ZCZ width is given by

$$Z\le\tfrac{MN}{K}-1\tag{3}$$

For the binary CZCSS, we have

$$Z \leq \frac{MN}{2K} \tag{4}$$

A q-ary (K, M, N, Z)-CZCSSs is called optimal if $Z = (MN)/K - 1$ for $q > 2$ or $Z = (MN)/2K$ for $q = 2$.

3 The magical method

Step 1: Let (a_0, b_0) be a (N, Z)-CZCP and (a_1, b_1) be the mate of (a_0, b_0).

Step 2: Set $\alpha = \{x_i\}_{i=0}^{2^n-1}$, $\beta = \{y_i\}_{i=0}^{2^n-1}$, where $x_i = a_0$ or a_1, $y_i = \begin{cases} b_0, x_i = a_0 \\ b_1, x_i = a_1 \end{cases}$. $\overline{\alpha} = \{\overline{x_i}\}_{i=0}^{2^n-1}$, where $\overline{x_i} = \begin{cases} a_0, x_i = a_1 \\ a_1, x_i = a_0 \end{cases}$, similarly, $\overline{\beta} = \{\overline{y_i}\}_{i=0}^{2^n-1}$, where $\overline{y_i} = \begin{cases} b_0, x_i = a_1 \\ b_1, x_i = a_0 \end{cases}$ so there are the following equations:

$$\rho_{x_i}(\tau) + \rho_{y_i}(\tau) = 0, |\tau| \in V_1 \cup V_2 \tag{5}$$

$$\rho_{x_i,y_i}(\tau) + \rho_{y_i,x_i}(\tau) = 0, |\tau| \in V_2 \tag{6}$$

$$\rho_{x_i,\overline{x_i}}(\tau) + \rho_{y_i,\overline{y_i}}(\tau) = 0, \forall \tau \tag{7}$$

Step 3: Let $\mathrm{H} = [h_{i,j}]_{2^n \times 2^n}$ be a Hadamard matrix of order $2^n \times 2^n$, so that the matrix S

$$\mathrm{S} = \begin{bmatrix} \mathrm{H}\Theta\alpha & \mathrm{H}\Theta\beta \\ \mathrm{H}\Theta\overline{\alpha} & \mathrm{H}\Theta\overline{\beta} \end{bmatrix} \tag{8}$$

where Θ represents Hadamard product. Take the row vector of S to form the sequence set $S = \{S_\mu, 0 \leq \mu < 2^{n+1}\}$.

Theorem 1. *The sequence set S constructed from the above steps is a $(2^{n+1}, 2^{n+1}, N, Z)$-CZCSS.*

Until now, only [2] proposed a class of CZCSS, then the comparison of parameters is shown in Table 1. The direct GBF-based construction proposed in [2] and the indirect construction method proposed in **Theorem1** provide ideas for CZCSS design, despite the fact that the two constructions produce non-optimal CZCSSs. **Theorem1** uses Hadamard matrices and the CZCPs with larger CZC_{ratio} to construct the CZCSS with more flexible parameters, and when $Z = N/2$, CZCSS achieves optimal performance. Therefore, the CZCSS derived from **Theorem1** have a higher CZC ratio than that of [2].

Let (a, b) be a GCP of length N, then $(c, d) = (\overleftarrow{b^*}, \overleftarrow{-a^*})$ is the mate of (a, b). Perform the following two concatenation operations on (a, b) and (c, d):

$$ConstructionI \begin{array}{l} a_0 = (a \, \|c\| \, a \, \|b\| \, d \, \|b), \\ b_0 = (a \, \|c\| \, a \, \|-b\| - d \, \|-b); \end{array} \tag{9}$$

$$ConstructionII \begin{array}{l} a_0 = (a \, \|a\| - a \, \|c\| - a \, \|b\| \, b \, \|-b\| \, d \, \|-b), \\ b_0 = (a \, \|a\| - a \, \|c\| - a \, \|-b\| - b \, \|b\| - d \, \|b). \end{array} \tag{10}$$

Table 1: Parameter Comparison of CZCSSs

Ref	Sequence Set Parameters	Methods and constraints	Remarks
[2]	$(2^{n+1}, 2^{n+1}, 2^{m-1}+2, 2^{\pi(m-3)}+1)$	GBFs. $m > 4$	Non-optimal
Thm.2	$(2^{n+1}, 2^{n+1}, N, Z)$	Hadamard Matrix and the Hadamard Product of CZCP	when $Z = N/2$, optimal

Theorem 2. *(a_0, b_0) obtained from the above Construction I is a $(6N, 2N-1)$-CZCP, (a_0, b_0) obtained from the Construction II is a $(10N, 3N-1)$-CZCP.*

The comparison of CZCPs parameters is shown in Table 2. Compared to existing literature, **Theorem 2** uses GCPs and the concatenation operation to obtain CZCPs with larger CZC_{ratio} and new parameter combinations.

4 Proof

Proof of Theorem1. Due to $\rho_{x_i}(\tau) + \rho_{y_i}(\tau) = 0$ for $|\tau| \in V_1 \cup V_2$, $0 \le i < 2^n$, the AACF of S_μ is as follow

$$\rho_{S_\mu}(\tau) = \sum_{i=0}^{2^n-1} h^2_{\mu \bmod 2^n, i}(\rho_{x_i}(\tau) + \rho_{y_i}(\tau)) = 0, |\tau| \in V_1 \cup V_2 \tag{11}$$

Equation (11) satisfies the condition P1 of Definition 4.

$$\begin{aligned}\rho_{S^i_\mu, S^{i+1}_\mu}(\tau) = &\sum_{i=0}^{2^n-2} h_{\mu \bmod 2^n, i} h_{\mu \bmod 2^n, i+1}(\rho_{x_i, x_{i+1}}(\tau) + \rho_{y_i, y_{i+1}}(\tau)) + \\ &h_{\mu \bmod 2^n, 2^{n-1}} h_{\mu \bmod 2^n, 0}(\rho_{x_{2^n-1}, y_0}(\tau) + \rho_{y_{2^n-1}, x_0}(\tau))\end{aligned} \tag{12}$$

When $x_i = x_{i+1}$, $y_i = y_{i+1}$, obtained from $\rho_{x_i}(\tau) + \rho_{y_i}(\tau) = 0$, $|\tau| \in V_1 \cup V_2$ and $\rho_{x_0, y_0}(\tau) + \rho_{y_0, x_0}(\tau) = 0$, $|\tau| \in V_2$:

$$\rho_{S^i_\mu, S^{i+1}_\mu}(\tau) = 0 \tag{13}$$

When $x_i \neq x_{i+1}$, $y_i \neq y_{i+1}$, obtained from $\rho_{x_i, \overline{x_i}}(\tau) + \rho_{y_i, \overline{y_i}}(\tau) = 0$ for all τ and $\rho_{x_0, \overline{y_0}}(\tau) + \rho_{y_0, \overline{x_0}}(\tau) = 0$ for $|\tau| \in V_2$, so we have

$$\rho_{S^i_\mu, S^{i+1}_\mu}(\tau) = 0 \tag{14}$$

Equations (13) and (14) satisfy the condition P2 of Definition 4.

Table 2: The Comparison of CZCP Parameters

Ref	Parameters	CZC_{ratio}	Methods	Optimality
[4]	$(2N, N), N = 2^{\alpha}10^{\beta}26^{\gamma}$	1	GCPs	Yes
	$(2^m, 2^{m-1}), m \geq 2$	1	GBF	Yes
[5]	$\left(2^{m-1}+2, 2^{\pi(m-3)}+1\right), m \geq 4$	$\leq \frac{1}{2}$	GBF	No
	$(2N+2, N/2+1)$	$\leq \frac{1}{2}$	Insertion	No
	$(12, 5)\,(24, 11)$	1	Barker code	Yes
	$(12N, 5N), (24N, 11N)$	$\leq \frac{5}{6}, \leq \frac{11}{12}$	Kronecker product and GCPs	No
[8]	$\left(10^{\beta}, 4\times 10^{\beta-1}\right), \beta \geq 1$	$\frac{4}{5}$	Kronecker product and GCPs	No
	$(26^{\gamma}, 12\times 26^{\gamma-1}), \gamma \geq 1$	$\frac{12}{13}$		No
	$\left(10^{\beta}26^{\gamma}, 12\times 10^{\beta}26^{\gamma-1}\right), \gamma \geq 1$	$\frac{12}{13}$		No
[9]	$\left(2^{m-1}+2^{v+1}, 2^{\pi(v+1)-1}+2^{v}-1\right)$ $m \geq 4, 0 \leq v \leq m-3$	$\leq \frac{2}{3}$	BF	No
[10]	$(2^{m+2}+2^{m+1}, 2^{m+1}-1)$	$\leq \frac{2}{3}$	ZCPs and concatenation operation	No
	$(2^{m+4}+2^{m+3}+2^{m+2}, 2^{m+3}-1)$	$\leq \frac{4}{7}$		No
	$\left(2^{\alpha+2}10^{\beta}26^{\gamma}+4, 3\times 2^{\alpha-1}10^{\beta}26^{\gamma}\right)$	$\frac{3}{4}$		No
	$\left(7\times 2^{\alpha+2}10^{\beta}26^{\gamma}, 3\times 2^{\alpha+2}10^{\beta}26^{\gamma}-1\right)$	$\frac{6}{7}$		No
	$\left(3\times 2^{\alpha+2}10^{\beta}26^{\gamma}, 5\times 2^{\alpha+1}10^{\beta}26^{\gamma}-1\right)$	$\frac{5}{6}$		No
[11]	$(M, \frac{M}{2}-1), M \in \{6, 12, 24, 28, 48, 56\}$	1	Computer Search	Yes
	$(MN, (\frac{5M-6}{10})N), N = 10^{\beta+1}$	$\frac{5M-6}{5M}$	GCPs and Kronecker product	No
	$MN, (\frac{13M-14}{26})N, N = 26^{\gamma+1}$	$\frac{13M-14}{13M}$		No
	$(96, 47), (112, 55)$	1		Yes
	$(96N, 47N)$	$\leq \frac{27}{28}$		No
	$(112N, 55N)$	$\leq \frac{55}{56}$		No
Thm.1	$(6N, 2N-1)$	$\leq 2/3$	GCPs concatenation operation	No
	$(10N, 3N-1)$	$\leq 3/5$		No

Let S_e and S_f denote two different rows of S, when $0 \leq e, f < 2^n$ or $2^n \leq e, f < 2^{n+1}$,using the properties of the Hadamard matrix, we have

$$\rho_{S_e,S_f}(\tau) = \sum_{i=0}^{2^n-1} h_{e \bmod 2^n,i} h_{f \bmod 2^n,i}(\rho_{x_i}(\tau) + \rho_{y_i}(\tau)) = 0 \tag{15}$$

Where $|\tau| \in V_1 \cup V_2$.
When $0 \leq e < 2^n$, $2^n \leq f < 2^{n+1}$, $h_{e \bmod 2^n,i} = h_{f \bmod 2^n,i}$, then

$$\rho_{S_e,S_f}(\tau) = \sum_{i=0}^{2^n-1} h^2_{e \bmod 2^n,i}(\rho_{x_i,\overline{x_i}}(\tau) + \rho_{y_i,\overline{y_i}}(\tau)) = 0 \tag{16}$$

Where $0 \leq |\tau| < N$.

Equations (15) and (16) satisfy the condition P3 of Definition 4.

From equation (8), two different rows e, f,

$$\begin{aligned}\rho_{S_e^i,S_f^{i+1}}(\tau) = \sum_{i=0}^{2^n-2} h_{e \bmod 2^n,i} h_{f \bmod 2^n,i+1}(\rho_{x_i,x_{i+1}}(\tau) + \rho_{y_i,y_{i+1}}(\tau)) + \\ h_{e \bmod 2^n,2^{n-1}} h_{f \bmod 2^n,0} \rho_{x_{2^n-1},y_0}(\tau) + h_{e \bmod 2^n,2^{n-1}} h_{f \bmod 2^n,0} \rho_{y_{2^n-1},x_0}(\tau)\end{aligned} \tag{17}$$

Assuming $x_i = x_{i+1}$, $y_i = y_{i+1}$, then $\rho_{x_i}(\tau) + \rho_{y_i}(\tau) = 0$, $|\tau| \in V_1 \cup V_2$ and $\rho_{x_0,y_0}(\tau) + \rho_{y_0,x_0}(\tau) = 0$, $|\tau| \in V_2$, therefore

$$\rho_{S_e^i,S_f^{i+1}}(\tau) = 0 + \rho_{x_0,y_0}(\tau) + \rho_{y_0,x_0}(\tau) = 0 \tag{18}$$

Assuming $x_i \neq x_{i+1}$, $y_i \neq y_{i+1}$, $\rho_{x_i,\overline{x_i}}(\tau) + \rho_{y_i,\overline{y_i}}(\tau) = 0$ for $\forall\tau$, $\rho_{x_0,\overline{y_0}}(\tau) + \rho_{y_0,\overline{x_0}}(\tau) = 0$, $|\tau| \in V_2$, then

$$\rho_{S_e^i,S_f^{i+1}}(\tau) = 0 + \rho_{x_0,\overline{y_0}}(\tau) + \rho_{y_0,\overline{x_0}}(\tau) = 0 \tag{19}$$

Equations (18) and (19) satisfy the P4 condition of Definition 4. In summary, S is a $(2^{n+1}, 2^{n+1}, N, Z)$-CZCSS.This completes the proof of Theorem1. □

Proof of Theorem2. Firstly, let's prove Construction I.

For $\tau > 0$, according to Definitions 2 and 3, the AACFs of a_0 and b_0 are calculated in the following ways:

From Definition 2 and Definition 3, it can be concluded that:

$\rho_a(\tau)+\rho_b(\tau) = 0$, $1 \leq \tau \leq N-1$; $\rho_c(\tau)+\rho_d(\tau) = 0$, $1 \leq \tau \leq N-1$; $\rho^*_{a,c}(\tau)+\rho^*_{b,d}(\tau) = 0$, $0 \leq \tau \leq N-1$.

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

$$\begin{aligned}\rho_{a_0}(\tau) = 2\rho_a(\tau) + \rho_c(\tau) + 2\rho_b(\tau) + \rho_d(\tau) + \rho^*_{c,a}(N-\tau) + \rho^*_{a,c}(N-\tau) + \rho^*_{b,a}(N-\tau) + \\ \rho^*_{d,b}(N-\tau) + \rho^*_{b,d}(N-\tau)\end{aligned} \tag{20}$$

$$\begin{aligned}\rho_{b_0}(\tau) = 2\rho_a(\tau) + \rho_c(\tau) + 2\rho_b(\tau) + \rho_d(\tau) + \rho^*_{c,a}(N-\tau) + \rho^*_{a,c}(N-\tau) - \rho^*_{b,a}(N-\tau) + \\ \rho^*_{d,b}(N-\tau) + \rho^*_{b,d}(N-\tau)\end{aligned} \tag{21}$$

then

$$\begin{aligned}\rho_{a_0}(\tau) + \rho_{b_0}(\tau) = 4\rho_a(\tau) + 4\rho_b(\tau) + 2\rho_c(\tau) + 2\rho_d(\tau) + 2\rho^*_{c,a}(N-\tau) + 2\rho^*_{a,c}(N-\tau) + \\ 2\rho^*_{b,d}(N-\tau) + 2\rho^*_{d,b}(N-\tau) = 0\end{aligned} \tag{22}$$

Similarly,for $\tau = N$, we have

$$\rho_{a_0}(\tau) + \rho_{b_0}(\tau) = 2\rho^*_{a,c}(\tau-N) + 2\rho^*_{c,a}(\tau-N) + 2\rho^*_{b,d}(\tau-N) + 2\rho^*_{d,b}(\tau-N) = 0 \tag{23}$$

For $N+1 \leq \tau \leq 2N-1$, we have

$$\rho_{a_0}(\tau)+\rho_{b_0}(\tau)=2\rho_{a,c}(\tau-N)+2\rho_{c,a}(\tau-N)+2\rho_{b,d}(\tau-N)+2\rho_{d,b}(\tau-N)+ 2\rho_a^*(2N-\tau)+2\rho_b^*(2N-\tau)=0 \tag{24}$$

For $\tau = 2N$, we have

$$\rho_{a_0}(\tau)+\rho_{b_0}(\tau)=2\rho_a(\tau-2N)+2\rho_b(\tau-2N)=4N \tag{25}$$

For $2N+1 \leq \tau \leq 3N-1$, we have

$$\rho_{a_0}(\tau)+\rho_{b_0}(\tau)=2\rho_a(\tau-2N)+2\rho_b(\tau-2N)=0 \tag{26}$$

For $3N \leq \tau \leq 6N-1$, we have

$$\rho_{a_0}(\tau)+\rho_{b_0}(\tau)=0 \tag{27}$$

From the above, it can be obtained that

$$\rho_{a_0}(\tau)+\rho_{b_0}(\tau)=\begin{cases} 0, 0<\tau \leq 2N-1 \\ 4N, \tau = 2N \\ 0, 2N+1 \leq \tau \leq 6N-1 \end{cases} \tag{28}$$

Similarly, when $\tau < 0$, the conclusion also holds. Therefore, it can be concluded that

$$\rho_{a_0}(\tau)+\rho_{b_0}(\tau)=\begin{cases} 0, 0<|\tau| \leq 2N-1 \\ 4N, |\tau| = 2N \\ 0, 2N+1 \leq |\tau| \leq 6N-1 \end{cases} \tag{29}$$

The condition C1 of Definitions 4 is satisfied.

Next, the ACCFs of a_0 and b_0 are calculated as follows:

For $4N+1 \leq \tau \leq 6N-1$, we have

$$\rho_{a_0,b_0}(\tau)+\rho_{b_0,a_0}(\tau)=0 \tag{30}$$

Therefore, when $4N+1 \leq \tau \leq 6N-1$, $\rho_{a_0,b_0}(\tau)+\rho_{b_0,a_0}(\tau)=0$. Similarly, when $1-6N \leq \tau \leq -1-4N$, $\rho_{a_0,b_0}(\tau)+\rho_{b_0,a_0}(\tau)=0$. So (a_0,b_0) satisfies the condition C2 of *Definitions* 4 for $4N+1 \leq |\tau| \leq 6N-1$. In summary, (a_0,b_0) obtained from *Construction* I is a $(6N, 2N-1)$-CZCP.

Secondly, let's demonstrate *Construction* II. Similar to *Construction* I it can be concluded that

$$\rho_{a_0}(\tau)+\rho_{b_0}(\tau)=\begin{cases} 0, 1 \leq |\tau| \leq 3N-1 \\ -4N, |\tau| = 3N \\ 0, 3N+1 \leq |\tau| \leq 4N-1 \\ -4N, |\tau| = 4N \\ 0, 4N+1 \leq |\tau| \leq 10N-1 \end{cases} \tag{31}$$

For $7N+1 \leq |\tau| \leq 10N-1$, we have

$$\rho_{a_0,b_0}(\tau)+\rho_{b_0,a_0}(\tau)=0 \tag{32}$$

According to (31) and (32), the conditions C1 and C2 of Definitions 4 are satisfied, so (a_0,b_0) is a $(10N, 3N-1)$-CZCP. This completes the proof of Theorem2. □

5 Conclusion

This paper presents a class of optimal CZCSS methods based on CZCPs and their mates, utilizing Hadamard products. Furthermore, to enrich the base sequences, two types of CZCPs are constructed using the concatenation technique and GCPs, thus extending the parameter range of CZCPs. Currently, there are few results on the construction of CZCSSs, with only one type of direct construction method based on GBF proposed in [2]. The CZCSSs constructed in this article can achieve flexible sequence length and ZCZ length. The construction results of this article can provide more options for training sequences in SM systems.

References

[1] P. Fan, W. Yuan, and Y. Tu. Z-complementary binary sequences. *IEEE Signal Processing Letters*, vol. 14, no. 8, pp. 509–512, Aug. 2007

[2] P.Kumar, S.Majhi, S.Paul. A Direct Construction of Cross Z-Complementary Sequence Sets with Large Set Size. *Cryptogr. Commun.* https://doi.org/10.1007/s12095-024-00700-7. Feb. 2024.

[3] M. Golay. Complementary series. *IRE Transactions on Information Theory*, vol. 7, no. 2, pp. 82-87, Apr. 1961.

[4] Z. Liu, P. Yang, Y. L. Guan and P. Xiao. Cross Z-Complementary Pairs for Optimal Training in Spatial Modulation Over Frequency Selective Channels. *IEEE Transactions on Signal Processing*, vol. 68, pp. 1529-1543, Feb. 2020.

[5] A. R. Adhikary, Z. Zhou, Y. Yang and P. Fan. Constructions of Cross Z-Complementary Pairs With New Lengths. *IEEE Transactions on Signal Processing*, vol. 68, pp. 4700-4712, Aug. 2020.

[6] Chin-Chong Tseng and C. Liu. Complementary sets of sequences. *IEEE Transactions on Information Theory*, vol. 18, no. 5, pp. 644-652, Sep. 1972.

[7] Y. Zhou, Z. Zhou, Z. Liu, Y. Yang, P. Yang and P. Fan. Symmetrical Z-Complementary Code Sets for Optimal Training in Generalized Spatial Modulation. *2022 10th International Workshop on Signal Design and Its Applications in Communications (IWSDA)*, pp. 1-5, Feb. 2022.

[8] C. Fan, D. Zhang, and A. R. Adhikary. New sets of binary cross Z-complementary sequence pairs. *IEEE Communications Letters*, vol. 24, no. 8, pp. 1616–1620, Aug. 2020.

[9] Z. -M. Huang, C. –Y. Pai and C. -Y. Chen. Binary Cross Z-Complementary Pairs With Flexible Lengths From Boolean Functions. *IEEE Communications Letters*, vol. 25, no. 4, pp. 1057-1061, Apr. 2021.

[10] M. Yang, S. Tian, N. Li and A. R. Adhikary. New Sets of Quadriphase Cross Z-Complementary Pairs for Preamble Design in Spatial Modulation. *IEEE Signal Processing Letters*, vol. 28, pp. 1240-1244, May. 2021.

[11] H. Zhang, C. L. Fan, Y. Yang and S. Mesnager. New Binary Cross Z-Complementary Pairs With Large CZC Ratio. *IEEE Transactions on Information Theory*, vol. 69, no. 2, pp. 1328–1336, Feb.2023.

[12] Z. M. Huang, C.Y. Pai, and C. Y. Chen. Cross Z-Complementary Sets for Training Design in Spatial Modulation. *IEEE Transactions on Communications*, vol.70, no. 8, pp. 5030–5045, Aug. 2022.

[13] S. A. Yang and J. Wu. Optimal binary training sequence design for multiple-antenna systems over dispersive fading channels. *IEEE Transactions on Vehicular Technology*, vol. 51, no. 5, pp. 1271-1276, Sep. 2002.

[14] C. Fragouli, N. Al-Dhahir and W. Turin. Training-based channel estimation for multiple-antenna broadband transmissions. *IEEE Transactions on Wireless Communications*, vol. 2, no. 2, pp. 384-391, Mar. 2003.

[15] P. Fan and W. H. Mow. On optimal training sequence design for multiple-antenna systems over dispersive fading channels and its extensions. *IEEE Transactions on Vehicular Technology*, vol. 53, no. 5, pp. 1623-1626, Sep. 2004.

[16] P. Kumar, S. Majhi, S. Paul. A Direct Construction of Cross Z-Complementary Sets with Flexible Lengths and Large Zero Correlation Zone. 2022.[Online].Available: https://arxiv.org/abs/2207.11730v1.

[17] Z. -M. Huang, C. -Y. Pai and C. -Y. Chen. A Novel Construction of Optimal Cross Z-Complementary Sets Based on Generalized Boolean Functions. *IEEE International Symposium on Information Theory (ISIT)*, Espoo, Finland, pp. 1725-1730, Aug. 2022.

[18] F. Zeng, X. He, Z. Zhang and L. Yan. Quadriphase Cross Z-Complementary Pairs for Pilot Sequence Design in Spatial Modulation Systems. in *IEEE Signal Processing Letters*, vol. 29, pp. 508-512, Jan. 2022.

[19] Z. -M. Huang, C. -Y. Pai, Z. Liu and C. -Y. Chen. Enhanced Cross Z-Complementary Set and Its Application in Generalized Spatial Modulation. 2023.[Online].Available: https://doi.org/10.48550/arXiv.2311.18390.

A Construction of Optimal Z-Complementary Code Sets Based on Partially m-shift Orthogonal Complementary Codes

Tao Yu, Yang Yang, Avik Ranjan Adhikary

School of Mathematics
Southwest Jiaotong University
Chengdu, China

yutao_math@my.swjtu.edu.cn, {yang_data, avik.adhikary}@swjtu.edu.cn

Zhengchun Zhou

School of Information Science and Technology
Southwest Jiaotong University
Chengdu, China

zzc@swjtu.edu.cn

Abstract

Z-complementary code sets (ZCCSs) are widely used in multi-carrier code-division multiple access (MC-CDMA) and multiple-input multiple-output (MIMO) communication because of their ideal correlation properties within a certain region around the in-phase position named zero correlation zone (ZCZ). In this paper, we introduce the definition of a partially m-shifted orthogonal complementary code, and use it to construct an optimal ZCCS by combining complete complementary codes (CCCs). The resultant optimal ZCCSs have new parameters which have not been reported before.

1 Introduction

In 1951, Golay first proposed the concept of Golay complementary pairs (GCPs) while studying infrared multislit spectroscopy [1]. Ten years later, Golay presented the mathematical definition, properties and constructions of GCPs [2]. GCPs are a pair of sequences that satisfy the sum of aperiodic autocorrelation functions (AACFs) is a Dirac delta function [2]. Inspired by Golay's work, in 1972 Tseng and Liu extended the concept of GCPs to complementary sets (CSs) containing two or more constituent sequences [3]. CSs are a set of sequences that satisfy the sum of aperiodic autocorrelation functions (AACFs) is a Dirac delta function [3]. In addition, any two CSs with zero aperiodic cross-correlation sums (ACCSs) are called mutually orthogonal. Furthermore, a set of CSs that are mutually orthogonal to each other is referred to as a mutually orthogonal complementary

sequence sets (MOCSSs). Owing to the ideal correlation properties, MOCSSs have been applied in multi-carrier code division multiple access (MC-CDMA) systems [4], MIMO channel estimation [5] and suppressing the multiple access interference. An (M, N, L)-MOCSS is a family of M CSs, where M denotes the set size (i.e., the number of users), N denotes the flock size (i.e., the number of sub-carriers) and L denotes the sequence length [3]. It is worth noting that the set size of (M, N, L)-MOCSS is upper bounded by the flock size, i.e., $M \leq N$ [6]. When the set size equals the flock size, the MOCSS is called a complete complementary code (CCC) [6]. However, a significant limitation of CCC is that its set size (i.e., the number of users) is upper bounded by the flock size. To support a larger number of users in MC-CDMA systems, Z-complementary code sets (ZCCSs) were proposed by Fan *et al.* [7], which have ideal correlations within a zone around the in-phase position named the zero correlation zone (ZCZ).

In recent years, optimal ZCCSs have attracted a lot of research. For an (M, N, L, Z)-ZCCS, the upper bound of its set size is given by [8], i.e. $M \leq N\lfloor L/Z \rfloor$, where $\lfloor x \rfloor$ denotes the largest integer smaller than or equal to the real number x. When the equal sign holds, the ZCCS is said to optimal. At present, the systematic construction of optimal ZCCSs can be divided into two types: the direct construction methods based on generalized Boolean functions (GBFs) and the indirect construction methods based on base sequences.

First we review the direct constructions. In 2018, Wu *et al.* [9] first presented a construction of optimal ZCCSs based on generalized Boolean functions (GBFs), and discussed their peak-to-average power ratio (PAPR). In 2019, Sarkar *et al.* [10] constructed optimal ZCCSs from the second-order cosets of the q-ary generalization of the first-order Reed-Muller codes through a graphical representation. Later, in 2020, Sarkar *et al.* [11] proposed a construction of optimal ZCCSs with non-power-of-two lengths based on GBFs. And then in 2021, Sarkar *et al.* [12] also proposed a construction of optimal ZCCSs with non-power-of-two lengths based on Pseudo Boolean functions (PBFs). In addition, based on GBFs, Sarkar *et al.* [13] and Wu *et al.* [14] gave some optimal ZCCSs, respectively. Recently, based on GBFs, Ghosh *et al.* gave a construction of optimal ZCCSs with even lengths [15], and proposed three new classes of optimal binary ZCCSs [16]. Based on extended Boolean functions (EBFs), Shen *et al.* [17] proposed a construction of optimal ZCCSs, and Xiao *et al.* [18] obtained a new class of optimal ZCCSs.

Next, we review the indirect constructions. In [19], Das *et al.* presented a novel construction of optimal ZCCSs described in a z-domain framework by introducing the concept of Z-paraunitary (ZPU) matrices. In 2019, Adhikary *et al.* [20] proposed a construction of optimal ZCCSs based on the Hadamard matrix and Z-complementary pairs (ZCPs), which can obtain optimal ZCCSs of odd and even lengths. The ZCP has zero AACSs within a certain region around the in-phase position named zero correlation zone (ZCZ). A ZCP of length L and ZCZ width Z is abbreviated as (L, Z)-ZCP. Later, based on ZCPs and CCCs, Xie *et al.* [21] also obtained a family of optimal ZCCSs. Recently, combining optimal ZCCSs and CCCs, Yu *et al.* [22] designed two classes of optimal ZCCSs with enlarged parameters in terms of sequence lengths and set size. Based on orthogonal matrices, Cui *et al.* [23] proposed a novel construction of three classes of optimal ZCCSs with flexible lengths.

From the application perspective, modern communication systems require very flexible choices of set sizes, sequence lengths and large ZCZ width without any sacrifice of the desired correlation properties. So, this paper presents a construction of optimal ZCCSs with more flexible choices by introducing the concept of partially m-shift orthogonal complementary code. The partially m-shift orthogonal complementary code has zero autocorrelation and cross-correlation sums for each m time-shift within a certain region around the in-phase position. Based on partially m-shift orthogonal complementary code and CCCs, we get a class of optimal ZCCSs with sequence lengths which have not been reported before.

The remainder of the paper is organized as follows. In Section 2, we will show some basic notations, definitions, and a brief introduction of partially m-shift orthogonal complementary code. In Section 3, we will present the constructions of both ZCCSs and optimal ZCCSs based on partially m-shift orthogonal complementary code and CCCs. In Section 4, we will compare our results with existing ones. Finally, we will conclude our work in Section 5.

2 Preliminaries

In this section, we will present some basic notations, definitions, and a brief introduction of partially m-shift orthogonal complementary code.

- $\mathbf{a}$ and $\mathbf{b}$ denotes two unimodular complex valued sequences of length L, i.e., $\mathbf{a} = \big(a(0), a(1), \cdots, a(L-1)\big)$ and $\mathbf{b} = \big(b(0), b(1), \cdots, b(L-1)\big)$.
- $\mathbf{a}||\mathbf{b} = \big(a(0), \cdots, a(L-1), b(0), \cdots, b(L-1)\big)$ represents the concatenation of $\mathbf{a}$ and $\mathbf{b}$.
- intlv$(\mathbf{a}_0, \mathbf{a}_1, \cdots, \mathbf{a}_{N-1})$= $\big(a_0(0), a_1(0), \cdots, a_{N-1}(0), a_0(1), a_1(1), \cdots, a_{N-1}(1), \cdots, a_0(L-1), a_1(L-1), \cdots, a_{N-1}(L-1)\big)$ denotes the bit-interleaved sequences of $\{\mathbf{a}_0, \mathbf{a}_1, \cdots, \mathbf{a}_{N-1}\}$.
- $e\mathbf{a} = \big(ea(0), ea(1), \cdots, ea(L-1)\big)$, where e is a complex number. When $e = -1$, $e\mathbf{a}$ is written as $-\mathbf{a}$.
- x^* represents the complex conjugate of a complex number x.
- $\lfloor x \rfloor$ denotes the largest integer no more than the real number x. $\lceil x \rceil$ represents the smallest integer greater than or equal to x.
- $\langle k \rangle_N$ is the least non-negative integer of k modulo N, where k and N are two non-negative integers.

Given two complex valued sequences $\mathbf{a}$ and $\mathbf{b}$ of length L, the aperiodic correlation function of $\mathbf{a}$ and $\mathbf{b}$ at time-shift τ is defined as

$$\rho_{\mathbf{a},\mathbf{b}}(\tau) = \begin{cases} \sum_{n=0}^{L-1-\tau} a(n)b^*(n+\tau), & 0 \le \tau \le L-1, \\ 0, & \tau \ge L. \end{cases}$$

When $\mathbf{a} \neq \mathbf{b}$, $\rho_{\mathbf{a},\mathbf{b}}(\tau)$ is called the aperiodic cross-correlation function (ACCF); otherwise, it is called the aperiodic autocorrelation function (AACF) of $\mathbf{a}$. For simplicity, AACF of $\mathbf{a}$ will be denoted by $\rho_{\mathbf{a}}(\tau)$.

A sequence set $A^{(i)}(1 \leq i \leq M)$ contains N constituent sequences of length L, i.e., $A^{(i)} = \{\mathbf{a}_k^i : 0 \leq k < N\}$, where $\mathbf{a}_k^i = \big(a_k^i(0), a_k^i(1), \cdots, a_k^i(L-1)\big)$.The aperiodic cross-correlation function sum of $A^{(i)}$ and $A^{(j)}$ at time-shift τ is defined as

$$\rho_{A^{(i)},A^{(j)}}(\tau) = \sum_{k=0}^{N-1} \rho_{\mathbf{a}_k^i,\mathbf{a}_k^j}(\tau).$$

When $i = j$, $\rho_{A^{(i)},A^{(j)}}(\tau)$ is called the aperiodic autocorrelation function sum (AACFS), denoted by $\rho_{A^{(i)}}(\tau)$ for short.

Definition 1. Let $\mathcal{A} = \left\{A^{(0)}, A^{(1)}, \cdots, A^{(M-1)}\right\}$ be a set containing M sequence sets, where $A^{(i)}$ consists of N constituent sequences of length L. $\mathcal{A}$ is called an ZCCS, if the following equation holds:

$$\rho_{A^{(i)},A^{(j)}}(\tau) = \begin{cases} NL, & \tau = 0, i = j, \\ 0, & 0 < \tau < Z, i = j, \\ 0, & 0 \leq \tau < Z, i \neq j, \end{cases}$$

where Z is the ZCZ width. For simplicity, it is denoted by (M, N, L, Z)-ZCCS.

The following lemma gives a bound on the parameters of an (M, N, L, Z)-ZCCS.

Lemma 2 ([8])**.** *For any (M, N, L, Z)-ZCSS, we have*

$$M \leq N \left\lfloor \frac{L}{Z} \right\rfloor. \tag{1}$$

In this paper, an (M, N, L, Z)-ZCCS is said to be optimal if the equal sign in Eq. (1) holds, i.e., $M = N \left\lfloor \frac{L}{Z} \right\rfloor$. Moreover, when $N = 2$ and $L \neq 2^a 10^b 26^c$, one can have a tighter bound, i.e., $M \leq 2\lceil L/Z - 1 \rceil$ [7]. When the equal sign holds, the ZCCS is called optimal. When $Z = L$, the ZCCS is said an MOCSS, denoted by (M, N, L)-MOCSS; When $Z = L$ and $M = N$, the ZCCS is called a CCC, denoted by (M, M, L)-CCC.

In [24], the authors defined a partially E sequence and used it to construct a ZCP. Below, we will introduce a partially m-shift orthogonal complementary code for constructing ZCCSs.

Definition 3. Let $\mathcal{A} = \left\{A^{(0)}, A^{(1)}, \cdots, A^{(M-1)}\right\}$ be a set containing M sequence sets, where $A^{(i)}$ consists of N constituent sequences of length L. Set the integer m to satisfy $0 < m \leq Z \leq L$, then $\mathcal{A}$ is said to be a partially m-shift orthogonal complementary code if

$$\rho_{A^{(i)},A^{(j)}}(m\tau) = \begin{cases} NL, & \tau = 0, i = j, \\ 0, & 0 < \tau < \frac{Z}{m}, i = j, \\ 0, & 0 \leq \tau < \frac{Z}{m}, i \neq j, \end{cases}$$

where Z is the zone width around the in-phase position. For simplicity, it is denoted by (M, N, L, Z)-partially m-shift orthogonal complementary code.

When $m = 2$ and $M = N = 1$, the partially m-shift orthogonal complementary code is called a partially E sequence [24]; When $m = 2$, $M = 1$ and $Z = L$, the partially m-shift orthogonal complementary code is called an even-shift complementary sequence set (ESCSS) [25]; When $m = 1$, the partially m-shift orthogonal complementary code is called a ZCCS; When $m = 1$, $M = N$ and $Z = L$, the partially m-shift orthogonal complementary code is called a CCC [6]. An (M, N, L, Z)-partially m-shift orthogonal complementary code $\mathcal{A}$ contains M distinct partially m-shift complementary sequence sets, i.e. $\mathcal{A} = \left\{A^{(0)}, A^{(1)}, \cdots, A^{(M-1)}\right\}$, where $A^{(i)}$ satisfies $\rho_{A^{(i)}}(m\tau) = 0, 0 < \tau < \frac{Z}{m}$. In general, for any given (M, N, L, Z)-partially m-shift orthogonal complementary code, the maximum number M of different partially m-shift complementary sequence sets is bounded by

$$M \leq mN \left\lfloor \frac{L}{Z} \right\rfloor. \tag{2}$$

3 Construction of Optimal Z-complementary Codes Sets

In this section, based on partially m-shift orthogonal complementary code and CCC, we will present a construction of ZCCSs with more flexible lengths. Before we begin, let us first define an operator ϕ_m, which is useful for the construction of ZCCSs. Let $A = \{\mathbf{a}_k : 0 \leq k < m\}$ be a set of m constituent sequences of length L_1, where $\mathbf{a}_k = \big(a_k(0), a_k(1), \cdots, a_k(L_1 - 1)\big)$. Let $\mathbf{b} = \big(b(0), b(1), \cdots, b(L_2 - 1)\big)$ be a sequence of length L_2, then $\phi_m(\mathbf{b}, A)$ is a sequence of length $L_1 L_2$ defined as

$$\phi_m(\mathbf{b}, A) = b(0)\mathbf{a}_{\langle 0\rangle_m} || b(1)\mathbf{a}_{\langle 1\rangle_m} || \cdots || b(L_2 - 1)\mathbf{a}_{\langle L_2 - 1\rangle_m}.$$

For better understanding, we will give an example to describe.

Example 4. Let $A = \{\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_2\}$ be a set of 3 constituent sequences of length L and $C = \{\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$ be a set of 4 constituent sequences of length L. Also let $\mathbf{b} = (1, 1, -1, -1, 1, -1, -1)$ be a sequence of length 7, then

$$\begin{aligned}\phi_3(\mathbf{b}, A) &= \mathbf{a}_0 || \mathbf{a}_1 || - \mathbf{a}_2 || - \mathbf{a}_0 || \mathbf{a}_1 || - \mathbf{a}_2 || - \mathbf{a}_0;\\ \phi_4(\mathbf{b}, C) &= \mathbf{c}_0 || \mathbf{c}_1 || - \mathbf{c}_2 || - \mathbf{c}_3 || \mathbf{c}_0 || - \mathbf{c}_1 || - \mathbf{c}_2.\end{aligned}$$

In what follows, we will present the main results of this paper.

Lemma 5. *Let $\mathcal{A} = \{A^{(0)}, A^{(1)}, \cdots, A^{(M_1-1)}\}$ be an (M_1, N_1, L_1, Z_1)-partially m-shift orthogonal complementary code and $\mathcal{B} = \{B^{(0)}, B^{(1)}, \cdots, B^{(M_2-1)}\}$ be an (M_2, M_2, L_2)-CCC, where $A^{(i)} = \{\mathbf{a}_0^i, \mathbf{a}_1^i, \cdots, \mathbf{a}_{N_1-1}^i\}$, $\mathbf{a}_l^i = \big(a_l^i(0), a_l^i(1), \cdots, a_l^i(L_1 - 1)\big)$, $B^{(j)} = \{\mathbf{b}_0^j, \mathbf{b}_1^j, \cdots, \mathbf{b}_{M_2-1}^j\}$, $\mathbf{b}_k^j = \big(b_k^j(0), b_k^j(1), \cdots, b_k^j(L_2 - 1)\big)$, $0 \leq i \leq M_1 - 1$, $0 \leq j, k \leq M_2 - 1$, $0 \leq l \leq N_1 - 1$. Also set integer m to satisfy $m | M_2$, $C_k^t = \{\mathbf{b}_k^{mt}, \mathbf{b}_k^{mt+1}, \cdots, \mathbf{b}_k^{mt+m-1}\}$,*

where $0 \le t \le M_2/m - 1$. *Define* $\mathcal{S} = \{S^{0,0}, S^{0,1}, \cdots, S^{M_1-1,M_2/m-1}\}$, *where* $S^{i,t}$ *consists of* N_1M_2 *constituent sequences of length* L_1L_2, *i.e.,*

$$\begin{aligned} S^{i,t} = \big\{ & \phi_m(\mathbf{a}_0^i, C_0^t), \phi_m(\mathbf{a}_0^i, C_1^t), \cdots, \phi_m(\mathbf{a}_0^i, C_{M_2-1}^t), \\ & \phi_m(\mathbf{a}_1^i, C_0^t), \phi_m(\mathbf{a}_1^i, C_1^t), \cdots, \phi_m(\mathbf{a}_1^i, C_{M_2-1}^t), \\ & \cdots \\ & \phi_m(\mathbf{a}_{N_1-1}^i, C_0^t), \phi_m(\mathbf{a}_{N_1-1}^i, C_1^t), \cdots, \phi_m(\mathbf{a}_{N_1-1}^i, C_{M_2-1}^t) \big\}. \end{aligned}$$

Then $\mathcal{S}$ *is an* $(M_1M_2/m, N_1M_2, L_1L_2, Z_1L_2)$*-ZCCS.*

Proof. Let $S^{i,t}$ and $S^{i',t'}$ be two arbitrary sequence sets of $\mathcal{S}$. For any integer $\tau = qL_2 + r$, $n = lM_2 + k$, where $0 \le q \le L_1 - 1$, $0 \le r \le L_2 - 1$, $0 \le l \le N_1 - 1$, $0 \le k \le M_2 - 1$. We proceed with the proof considering the following cases.

- When $r = 0$, we have

$$\begin{aligned} \rho_{S^{i,t},S^{i',t'}}(\tau) &= \sum_{n=0}^{N_1M_2-1} \rho_{\phi_m(\mathbf{a}^i_{\lfloor \frac{n}{M_2} \rfloor}, C^t_{\langle n \rangle_{M_2}}),\ \phi_m(\mathbf{a}^{i'}_{\lfloor \frac{n}{M_2} \rfloor}, C^{t'}_{\langle n \rangle_{M_2}})}(\tau) \\ &= \sum_{l=0}^{N_1-1} \sum_{k=0}^{M_2-1} \Big[\sum_{h=0}^{L_1-1-q} a_l^i(h) a_l^{i'}(h+q) \cdot \rho_{\mathbf{b}_k^{mt+\langle h \rangle_m}, \mathbf{b}_k^{mt'+\langle h+q \rangle_m}}(0) \Big] \qquad (3) \\ &= \sum_{l=0}^{N_1-1} \sum_{h=0}^{L_1-1-q} a_l^i(h) a_l^{i'}(h+q) \cdot \rho_{B^{(mt+\langle h \rangle_m)}, B^{(mt'+\langle h+q \rangle_m)}}(0). \end{aligned}$$

  For the case $t \ne t'$, consider $0 \le \tau < Z_1L_2$ (i.e., $0 \le q \le Z_1 - 1$), since $\mathcal{B}$ is a CCC, $\rho_{B^{(mt+\langle h \rangle_m)}, B^{(mt'+\langle h+q \rangle_m)}}(0) = 0$, we have $\rho_{S^{i,t},S^{i',t'}}(\tau) = 0$.

  For the case $t = t'$, consider $0 \le \tau < Z_1L_2$ (i.e., $0 \le q \le Z_1 - 1$), when $\langle q \rangle_m \ne 0$, since $\mathcal{B}$ is a CCC, $\rho_{B^{(mt+\langle h \rangle_m)}, B^{(mt'+\langle h+q \rangle_m)}}(0) = 0$, one has $\rho_{S^{i,t},S^{i',t'}}(\tau) = 0$; when $\langle q \rangle_m = 0$, $\rho_{B^{(mt+\langle h \rangle_m)}, B^{(mt'+\langle h+q \rangle_m)}}(0) = M_2L_2$, then

$$\begin{aligned} \rho_{S^{i,t},S^{i',t'}}(\tau) &= \sum_{l=0}^{N_1-1} \sum_{h=0}^{L_1-1-q} a_l^i(h) a_l^{i'}(h+q) \cdot \rho_{B^{(mt+\langle h \rangle_m)}, B^{(mt'+\langle h+q \rangle_m)}}(0) \\ &= M_2L_2 \cdot \sum_{l=0}^{N_1-1} \sum_{h=0}^{L_1-1-q} a_l^i(h) a_l^{i'}(h+q) \\ &= M_2L_2 \cdot \rho_{A^{(i)}, A^{(i')}}(m\alpha) \end{aligned}$$

  where $0 \le \alpha < \frac{Z_1}{m}$. If $i \ne i'$, since $\mathcal{A}$ is an (M_1, N_1, L_1, Z_1)-partially m-shift orthogonal complementary code, $\rho_{A^{(i)}, A^{(i')}}(m\alpha) = 0$, then $\rho_{S^{i,t},S^{i',t'}}(\tau) = 0$. If $i = i'$, when $\tau = 0$, $\rho_{S^{i,t},S^{i',t'}}(\tau) = M_2L_2N_1L_1$; when $1 \le \tau < Z_1L_2$ (i.e., $1 \le q \le Z_1 - 1$, $1 \le \alpha < \frac{Z_1}{m}$), since $\mathcal{A}$ is an (M_1, N_1, L_1, Z_1)-partially m-shift orthogonal complementary code, we have $\rho_{A^{(i)}, A^{(i')}}(m\alpha) = 0$ and then $\rho_{S^{i,t},S^{i',t'}}(\tau) = 0$.

- When $r \neq 0$, we have

$$\begin{aligned}
\rho_{S^{i,t},S^{i',t'}}(\tau) &= \sum_{n=0}^{N_1M_2-1} \rho_{\phi_m(\mathbf{a}^i_{\lfloor \frac{n}{M_2} \rfloor}, C^t_{\langle n \rangle_{M_2}}),\ \phi_m(\mathbf{a}^{i'}_{\lfloor \frac{n}{M_2} \rfloor}, C^{t'}_{\langle n \rangle_{M_2}})}(\tau) \\
&= \sum_{l=0}^{N_1-1} \sum_{k=0}^{M_2-1} \Bigg[\sum_{h=0}^{L_1-1-q} a^i_l(h) a^{i'}_l(h+q) \cdot \rho_{\mathbf{b}^{mt+\langle h \rangle_m}_k, \mathbf{b}^{mt'+\langle h+q \rangle_m}_k}(r) \\
&\quad + \sum_{h=0}^{L_1-2-q} a^i_l(h) a^{i'}_l(h+q+1) \cdot \rho_{\mathbf{b}^{mt+\langle h \rangle_m}_k, \mathbf{b}^{mt'+\langle h+q+1 \rangle_m}_k}(r-L_2) \Bigg] \\
&= \sum_{l=0}^{N_1-1} \Bigg[\sum_{h=0}^{L_1-1-q} a^i_l(h) a^{i'}_l(h+q) \cdot \rho_{B^{(mt+\langle h \rangle_m)}, B^{(mt'+\langle h+q \rangle_m)}}(r) \\
&\quad + \sum_{h=0}^{L_1-2-q} a^i_l(h) a^{i'}_l(h+q+1) \cdot \rho_{B^{(mt+\langle h \rangle_m)}, B^{(mt'+\langle h+q+1 \rangle_m)}}(r-L_2) \Bigg].
\end{aligned}$$

The case that $r \neq 0$ can be similarly discussed.

According to the discussion above, $\mathcal{S}$ is an $(M_1M_2/m, N_1M_2, L_1L_2, Z_1L_2)$-ZCCS. This completes the proof. □

By Lemma 5, we have the following theorem for the construction of optimal ZCCSs.

Theorem 6. *Let $\mathcal{A} = \{A^{(0)}, \cdots, A^{(M_1-1)}\}$ be an (M_1, N_1, L_1, Z_1)-partially m-shift orthogonal complementary code and satisfy $M_1 = mN_1\lfloor \frac{L_1}{Z_1} \rfloor$. If $\mathcal{B} = \{B^{(0)}, B^{(1)}, \cdots, B^{(M_2-1)}\}$ is an (M_2, M_2, L_2)-CCC, then $\mathcal{S}$ given by Lemma 5 is an optimal $(M_1M_2/m, N_1M_2, L_1L_2, Z_1L_2)$-ZCCS.*

Proof. The proof is analog to that of Lemma 5, so we only need to prove that $\mathcal{S}$ is an optimal $(M_1M_2/m, N_1M_2, L_1L_2, Z_1L_2)$-ZCCS. Since $M_1 = mN_1\lfloor \frac{L_1}{Z_1} \rfloor$, the set size of ZCCS $\mathcal{S}$ comes up to the theoretical bound in Lemma 2, that is, $M_1M_2/m = N_1M_2\lfloor \frac{L_1}{Z_1} \rfloor = N_1M_2\lfloor \frac{L_1L_2}{Z_1L_2} \rfloor$. Therefore, $\mathcal{S}$ is an optimal $(M_1M_2/m, N_1M_2, L_1L_2, Z_1L_2)$-ZCCS. This completes the proof. □

Below, we will show how to obtain flexible partially m-shifted orthogonal complementary codes for generating optimal ZCCSs with new parameters.

The partially m-shift orthogonal complementary code can be obtained by the computer search, in addition, it can be obtained from the ZCCS by bit-interleaving. For example, $\mathcal{A} = \{A^{(0)}, A^{(1)}\}$ is a $(2, 2, 17, 9)$-ZCCS, i.e.,

$$\begin{aligned}
A^{(0)} = \{\mathbf{a}^0_0, \mathbf{a}^0_1\} = \{&(-1,-1,-1,-1,-1,-1,-1,1,-1,1,1,1,-1,-1,-1,1,1), \\
&(-1,-1,1,-1,1,1,-1,-1,1,1,-1,1,-1,1,-1,-1,1)\},
\end{aligned}$$

$$\begin{aligned}
A^{(1)} = \{\mathbf{a}^1_0, \mathbf{a}^1_1\} = \{&(1,-1,-1,1,-1,1,-1,1,1,-1,-1,1,1,-1,1,-1,-1), \\
&(-1,-1,1,1,1,-1,-1,-1,1,-1,1,1,1,1,1,1,1)\}.
\end{aligned}$$

Then by bit-interleaving, we get a $(2, 1, 34, 18)$-partially 2-shift orthogonal complementary code $\{\mathbf{b}_0^0, \mathbf{b}_0^1\}$, i.e.,

$$\begin{aligned}\mathbf{b}_0^0 = intlv(\mathbf{a}_0^0, \mathbf{a}_1^0) = (&-1,-1,-1,-1,-1,1,-1,-1,-1,1,-1,1,-1,-1,1,-1,-1,\\ &1,1,1,1,-1,1,1,-1,-1,-1,1,-1,-1,1,-1,1,1),\\ \mathbf{b}_0^1 = intlv(\mathbf{a}_0^1, \mathbf{a}_1^1) = (&1,-1,-1,-1,-1,1,1,1,-1,1,1,-1,-1,-1,1,-1,1,\\ &1,-1,-1,-1,1,1,1,1,1,-1,1,1,1,-1,1,-1,1).\end{aligned} \tag{4}$$

And we have $\rho_{\mathbf{b}_0^0}(2) = \rho_{\mathbf{b}_0^0}(4) = \cdots = \rho_{\mathbf{b}_0^0}(16) = 0, \rho_{\mathbf{b}_0^0}(18) = 2$, $\rho_{\mathbf{b}_0^1}(2) = \rho_{\mathbf{b}_0^1}(4) = \cdots = \rho_{\mathbf{b}_0^1}(16) = 0, \rho_{\mathbf{b}_0^1}(18) = 2$ and $\rho_{\mathbf{b}_0^0,\mathbf{b}_0^1}(0) = \rho_{\mathbf{b}_0^0,\mathbf{b}_0^1}(2) = \cdots = \rho_{\mathbf{b}_0^0,\mathbf{b}_0^1}(32) = 0$, $\rho_{\mathbf{b}_0^1,\mathbf{b}_0^0}(0) = \rho_{\mathbf{b}_0^1,\mathbf{b}_0^0}(2) = \cdots = \rho_{\mathbf{b}_0^1,\mathbf{b}_0^0}(32) = 0$. Similarly, based on $(4, 4, 17, 9)$-ZCCS, we can obtain $(4, 1, 68, 36)$-partially 4-shift orthogonal complementary code and $(4, 2, 34, 18)$-partially 2-shift orthogonal complementary code using bit-interleaving, respectively. Thus, a partially m-shift orthogonal complementary code with more flexible parameters can be obtained. Then by Theorem 6, we can offer more flexible choices of optimal ZCCS parameters.

Now, we give some examples of optimal ZCCS to illustrate the result of Theorem 6.

Table 1: Binary $(8, 2, 32, 16)$-partially 2-shift orthogonal complementary code

$\begin{pmatrix}\mathbf{a}_0^0\\ \mathbf{a}_1^0\end{pmatrix}$	$\begin{pmatrix}+&+&+&+&+&-&-&+&+&+&+&+&+&-&-&+&+&+&+&+&-&-&+&-&-&-&-&-&+&+&-\\ -&-&-&-&-&+&+&-&+&+&+&+&-&-&+&-&-&-&-&-&+&+&-&-&-&-&-&-&+&+&-\end{pmatrix}$
$\begin{pmatrix}\mathbf{a}_0^1\\ \mathbf{a}_1^1\end{pmatrix}$	$\begin{pmatrix}+&+&-&-&+&-&+&-&+&+&-&-&+&-&+&-&+&+&-&-&+&-&+&-&-&-&+&+&-&+&-&+\\ -&-&+&+&-&+&-&+&+&+&-&-&+&-&+&-&-&-&+&+&-&+&-&+&-&-&+&+&-&+&-&+\end{pmatrix}$
$\begin{pmatrix}\mathbf{a}_0^2\\ \mathbf{a}_1^2\end{pmatrix}$	$\begin{pmatrix}+&+&+&+&+&+&-&-&+&+&+&+&+&+&-&-&+&-&-&-&-&-&+&+&-&+&+&+&+&+&-&+\\ -&-&-&-&-&+&+&-&+&+&+&+&+&+&-&-&+&+&+&+&+&+&-&-&+&+&+&+&+&+&-&+\end{pmatrix}$
$\begin{pmatrix}\mathbf{a}_0^3\\ \mathbf{a}_1^3\end{pmatrix}$	$\begin{pmatrix}+&+&-&-&+&-&+&-&+&+&-&-&+&-&+&-&-&-&+&+&-&+&-&+&+&+&-&-&+&-&+&-\\ -&-&+&+&-&+&-&+&+&+&-&-&+&-&+&-&+&+&-&-&+&-&+&-&+&+&-&-&+&-&+&-\end{pmatrix}$
$\begin{pmatrix}\mathbf{a}_0^4\\ \mathbf{a}_1^4\end{pmatrix}$	$\begin{pmatrix}+&+&+&+&+&+&-&-&+&-&-&-&-&-&+&+&-&+&+&+&+&+&-&-&+&+&+&+&+&+&-&+\\ -&-&-&-&-&+&+&-&-&-&-&-&-&-&+&+&-&-&-&-&-&-&+&+&-&+&+&+&+&+&-&+\end{pmatrix}$
$\begin{pmatrix}\mathbf{a}_0^5\\ \mathbf{a}_1^5\end{pmatrix}$	$\begin{pmatrix}+&+&-&-&+&-&+&-&-&-&+&+&-&+&-&+&+&+&-&-&+&-&+&-&+&+&-&-&+&-&+&-\\ -&-&+&+&-&+&-&+&-&-&+&+&-&+&-&+&-&-&+&+&-&+&-&+&+&+&-&-&+&-&+&-\end{pmatrix}$
$\begin{pmatrix}\mathbf{a}_0^6\\ \mathbf{a}_1^6\end{pmatrix}$	$\begin{pmatrix}+&+&+&+&+&+&-&-&+&-&-&-&-&-&+&+&-&-&-&-&-&-&+&+&-&-&-&-&-&+&+&-\\ -&-&-&-&-&+&+&-&-&-&-&-&-&-&+&+&-&+&+&+&+&+&-&-&+&-&-&-&-&-&+&-\end{pmatrix}$
$\begin{pmatrix}\mathbf{a}_0^7\\ \mathbf{a}_1^7\end{pmatrix}$	$\begin{pmatrix}+&+&-&-&+&-&+&-&-&-&+&+&-&+&-&+&-&-&+&+&-&+&-&+&-&-&+&+&-&+&-&+\\ -&-&+&+&-&+&-&+&-&-&+&+&-&+&-&+&+&+&-&-&+&-&+&-&+&+&-&-&+&-&+&+\end{pmatrix}$

where 1 and -1 are denoted by $+$ and $-$, respectively.

Example 7. Let $\mathcal{A}$ be a binary $(2, 1, 34, 18)$-partially 2-shift orthogonal complementary code given by (4) and satisfy the equal sign in Eq. (2). Let $\mathcal{B}$ be a binary $(4, 4, 3)$-CCC from [22, Table III]. Then we can get an optimal binary $(4, 4, 102, 54)$-ZCCS $\mathcal{S}$ from Theorem 6, which is new optimal ZCCSs not presented in previous work.

Example 8. Let $\mathcal{A}$ be a binary $(8, 2, 32, 16)$-partially 2-shift orthogonal complementary code, as shown in Table 1, and satisfy the equal sign in Eq. (2). Let $\mathcal{B}$ be a binary $(4, 4, 3)$-CCC from [22, Table III]. Then we can get an optimal binary $(16, 8, 96, 48)$-ZCCS $\mathcal{S}$ from Theorem 6.

4 Comparison with the Previous Works

In Table 2, we list the parameters of our proposed optimal ZCCSs with that of the previous works. Compared with the previous construction methods, our proposed construction is different in the following ways:

- In [9, 10, 11, 12, 13, 14, 15, 17, 18, 21], the constructions are based on GBFs, PBFs and EBFs. Hence, for the binary optimal ZCCSs, the parameters are of the form of power of two. Compared to that, we can obtain optimal ZCCSs with non-power-of-two lengths. For example, we get an optimal binary $(4, 4, 102, 54)$-ZCCS, which can not be generated by [9, 10, 11, 12, 13, 14, 15, 17, 18, 21]. In [16], the authors offered optimal binary ZCCS with both power-of-two and non-power-of-two lengths through GBF. However, we can obtain an optimal binary $(4, 4, 102, 54)$-ZCCS, which can not be constructed by [16].

- In [20], Adhikary *et al.* constructed optimal $(2^{n+1}, 2^{n+1}, L, Z)$-ZCCS by using (L, Z)-ZCP and Hadamard matrix, where $Z > \frac{L}{2}$. In addition, in [21], using (L, Z)-ZCP and $(2^{k+1}, 2^{k+1}, 2^m)$-CCC, the authors constructed an optimal $(2^{k+2}, 2^{k+2}, 2^m \cdot L, 2^m \cdot Z)$-ZCCS. Note that, here the flock size and set size are same. However, we can design an optimal ZCCS with a different set size and flock size and a large ZCZ width according to the practical application. For example, we can obtain an optimal binary $(16, 8, 96, 48)$-ZCCS, which can not be constructed by [20, 21].

- In [19], Das *et al.* constructed optimal ZCCSs, based on ZPU matrices. In [22], based on optimal ZCCSs and CCCs, the authors derived optimal ZCCSs with enlarged parameters by using the Kronecker product. Note that, if we represent ZCCSs in [22] as matrices of polynomials as in [19], the same ZCCSs can be obtained by a different approach in [19]. However, based on (M_1, N_1, L_1, Z_1)-partially m-shift orthogonal complementary code and (M_2, M_2, L_2)-CCC, we can generate an optimal $(M_1M_2/m, N_1M_2, L_1L_2, Z_1L_2)$-ZCCS with flexible parameters. In fact, the results of [22] are our special case. For example, when $m = 1$, the parameters of the optimal ZCCS generated by us are the same as the result of [22, Th.1]. In addition, we can obtain an optimal binary $(4, 4, 102, 54)$-ZCCS, which can not be constructed by [19, 22]. In [23], based on $L \times L$ orthogonal matrices and $N \times N$ orthogonal matrices, Cui *et al.* constructed optimal (HL, N, L, Z)-ZCCSs, where $Z|L, N = HZ$. It should be noted that the length of these optimal ZCCSs is limited by the order of the orthogonal matrices. For example, we can get an optimal binary $(4, 4, 102, 54)$-ZCCS, which can not be derived by [23], since the Hadamard matrix of order 102 does not exist.

5 Conclusion

In this paper, we introduced a new concept called partially m-shift orthogonal complementary code. Based on partially m-shift orthogonal complementary code and CCC, we

Table 2: Summary of Existing Optimal ZCCSs

Ref.	Based on	Parameters	Conditions
[9, Th. 2]	GBF	$(M, N, 2^m, 2^m N/M)$	$M = 2^{k+v}, N = 2^k, m \geq 3,$ $v \leq m, k \leq m - v$
[10, Th. 2]	GBF	$(M, N, 2^m, 2^m N/M)$	$M = 2^{k+p+1},$ $N = 2^{k+1}, k + p \leq m$
[11, Th. 2]	GBF	$(M, M, 2^{m-1} + 2,$ $2^{m-2} + 2^{\pi(m-3)} + 1)$	$M = 2^{n+1}, m \geq 3$
[12, Th. 1]	PBF	$(M, N, 2^m M/N, 2^m)$	$M = p \cdot 2^{k+1}, N = 2^{k+1},$ $m \geq 2$, p is prime
[13, Th. 1]	GBF	$(M, N, 2^m, 2^m N/M)$	$M = 2^{n+p}, N = 2^n, p \leq m$
[14, Th. 3]	GBF	$(M, N, 2^m, 2^m N/M)$	$M = 2^{k+v}, N = 2^k,$ $v \leq m, k \leq m - v$
[15, Th. 1]	GBF	$(M, N, 2^m M/N, 2^m)$	$M = k \cdot 2^{n+1}, N = 2^{n+1},$ $k, m, n \in \mathbb{Z}^+$
[16, Th. 1]	GBF	$(M, N, \gamma \cdot M/N, \gamma)$	$M = R \cdot 2^{k+1}, N = 2^{k+1},$ $k \geq 1, m \geq 5,$ $\gamma = 5 \cdot 2^{m-3}$, R is even
[16, Th. 3]	GBF	$(M, M, 3 \cdot \gamma, 2 \cdot \gamma)$	$M = 2^{k+1}, k \geq 1,$ $m \geq 5, \gamma = 5 \cdot 2^{m-3}$
[17, Th. 2]	EBF	$(M, N, q^m, q^m N/M)$	$M = q^{v+1}, N = q,$ $m \geq 2,\ v \leq m$
[18, Th. 4.2]	EBF	$(M, N, q^m, q^m N/M)$	$M = q^{v+d}, N = q^d, q \geq 2,$ $v \leq m, d \leq m - v$
[21, Th. 1]	GBF	$(M, M, 3 \cdot 2^m, 2^{m+1})$	$M = 2^{k+1}, k, m \geq 1$
[21, Th. 3]	ZCP and CCC	$(M, M, L \cdot 2^m, Z \cdot 2^m)$	(L, Z)-ZCP, $M = 2^{k+2}, Z > \frac{L}{2},$ $(2^{k+1}, 2^{k+1}, 2^m)$-CCC
[19, Th. 1]	Butson-type Hadamard Matrices	(M, N, M, N)	$M, N \geq 2$
[19, Th. 2]	Optimal ZPU Matrices and Butson-type Hadamard Matrices	$(M, N, M \cdot N^n, N^{n+1})$	$M, N \geq 2,\ n \geq 0$
[20, Con. 1]	ZCP and Hadamard Matrices	(M, M, L, Z)	(L, Z)-ZCP, $M = 2^{n+1}, Z \geq \lceil \frac{L}{2} \rceil$
[22, Th.1]	Optimal ZCCS and CCC	$(M_1 M_2, N_1 M_2, L_1 L_2, Z_1 L_2)$	(M_2, M_2, L_2)-CCC and Optimal (M_1, N_1, L_1, Z_1)-ZCCS
[22, Th.2]	Optimal ZCCS and CCC	$(M_1, N_1, L_1 L_2 N_1, Z_1 L_2 N_1)$	(N_1, N_1, L_2)-CCC and Optimal (M_1, N_1, L_1, Z_1)-ZCCS
[23, Th.1]	$L \times L$ and $N \times N$ Orthogonal matrices	$(M, N, L, NL/M)$	$M = HL, N = HZ, Z \mid L$
[23, Th.2]	$L \times L$ and $N \times N$ Orthogonal matrices	(M, N, L, Z)	$M = HL, H = \lfloor \frac{N}{Z} \rfloor,$ $\lfloor \frac{L}{Z} \rfloor \cdot (N \mod Z) =$ $(L \mod Z) \lfloor \frac{N}{Z} \rfloor$
Th. 6	CCC and partially m-shift orthogonal complementary code	$(\frac{M_1 M_2}{m}, N_1 M_2, L_1 L_2, Z_1 L_2)$	(M_2, M_2, L_2)-CCC and (M_1, N_1, L_1, Z_1)-partially m-shift orthogonal complementary code satisfying the equal sign in Eq. (2)

presented a construction which can lead to new optimal ZCCSs with sequence lengths. Since the proposed construction depends on the availability of the partially m-shift orthogonal complementary code, the properties of partially m-shift orthogonal complementary code as well as some new constructions can be considered in the future work.

References

[1] M. J. E. Golay. Static multislit spectrometry and its application to the panoramic display of infrared spectra. *J. Opt. Soc. Am.*, 41(7): 468–472, 1951.

[2] M. J. E. Golay. Complementary series. *IRE Trans. Inf. Theory*, 7(2): 82–87, 1961.

[3] C. C. Tseng, C. L. Liu. Complementary sets of sequences. *IEEE Trans. Inf. Theory*, 18(5): 644–652, 1972.

[4] Z. L. Liu, Y. L. Guan, U. Parampalli. New complete complementary codes for peak-to-mean power control in multi-carrier CDMA. *IEEE Trans. Commun.*, 62(3): 1105–1113, 2014.

[5] S. Wang, A. Abdi. MIMO ISI channel estimation using uncorrelated golay complementary sets of polyphase sequences. *IEEE Trans. Veh. Technol.*, 56(5): 3024–3039, 2007.

[6] N. Suehiro, M. Hatori. N-shift cross-orthogonal sequences. *IEEE Trans. Inf. Theory*, 34(1): 143–146, 1988.

[7] P. Z. Fan, W. N. Yuan, Y. F. Tu. Z-complementary binary sequences. *IEEE Signal Process. Lett.*, 14(8): 509–512, 2007.

[8] L. F. Feng, P. Z. Fan, X. Zhou. Lower bounds on correlation of Z-complementary code sets. *Wireless Pers. Commun.*, 72(2): 1475–1488, 2013.

[9] S. W. Wu, C. Y. Chen. Optimal Z-complementary sequence sets with good peak-to-average power-ratio property. *IEEE Signal Process. Lett.*, 25(10): 1500–1504, 2018.

[10] P. Sarkar, S. Majhi, Z. L. Liu. Optimal Z-complementary code set from generalized Reed-Muller codes. *IEEE Trans. Commun.*, 67(3): 1783–1796, 2019.

[11] P. Sarkar, A. Roy, S. Majhi. Construction of Z-complementary code sets with non-power-of-two lengths based on generalized Boolean functions. *IEEE Commun. Lett.*, 24(8): 1607–1611, 2020.

[12] P. Sarkar, S. Majhi, Z. L. Liu. Pseudo-boolean functions for optimal Z-complementary code sets with flexible lengths. *IEEE Signal Process. Lett.*, 28: 1350–1354, 2021.

[13] P. Sarkar, S. Majhi. A direct construction of optimal ZCCS with maximum column sequence PMEPR two for MC-CDMA system. *IEEE Commun. Lett.*, 25(2): 337–341, 2021.

[14] S. W. Wu, A. Sahin, Z. M. Huang, C. Y. Chen. Z-complementary code sets with flexible lengths from generalized Boolean functions. *IEEE Access*, 9: 4642–4652, 2021.

[15] G. Ghosh, S. Majhi, P. Sarkar, A. K. Upadhaya. Direct construction of optimal z-complementary code sets with even lengths by using generalized Boolean functions. *IEEE Signal Process. Lett.*, 29: 872–876, 2022.

[16] G. Ghosh, S. Majhi, S. Paul. Construction of optimal binary Z-complementary code sets with new lengths using generalized Boolean function. *Cryptogr. Commun.*, 15(5): 979–993, 2023.

[17] B. S. Shen, H. Meng, Y. Yang, Z. C. Zhou. New construction of Z-complementary code sets and mutually orthogonal complementary sequence sets. *Des. Codes Cryptogr.*, 91(2): 353–371, 2023.

[18] H. Y. Xiao, X. W. Cao. New constructions of mutually orthogonal complementary sets and Z-complementary code sets based on extended Boolean functions. *Cryptogr. Commun.*, 16(1): 167–184, 2024.

[19] S. Das, U. Parampalli, S. Majhi, Z. L. Liu, S. Budišin. New optimal Z-complementary code sets based on generalized paraunitary matrices. *IEEE Trans. Signal Process.*, 68: 5546–5558, 2020.

[20] A. R. Adhikary, S. Majhi. New construction of optimal aperiodic Z-complementary sequence sets of odd-lengths. *Electronics Lett.*, 55(19): 1043–1045, 2019.

[21] C. L. Xie, Y. Sun, Y. Ming. Constructions of optimal binary Z-complementary sequence sets with large zero correlation zone. *IEEE Signal Process. Lett.*, 28: 1694–1698, 2021.

[22] T. Yu, A. R. Adhikary, Y. Y. Wang, Y. Yang. New class of optimal Z-complementary code sets. *IEEE Signal Process. Lett.*, 29: 1477–1481, 2022.

[23] L. Cui, X. Y. Chen. Two constructions for optimal Z-complementary sequence sets. *Adv. Math. Commun.*, 2022.

[24] C. L. Xie, Y. Sun. Constructions of even-period binary Z-complementary pairs with large ZCZs. *IEEE Signal Process. Lett.*, 25(8): 1141–1145, 2018.

[25] B. S. Shen, Y. Yang, Y. H. Feng, Z. C. Zhou. A generalized construction of mutually orthogonal complementary sequence sets with non-power-of-two lengths. *IEEE Trans. Commun.*, 69(7): 4247–4253, 2021.

On Average Zero-Correlation Zone of Golay Complementary Pairs

Dian Li, Chunlei Li
University of Bergen, Bergen, Norway
{dian.li, chunlei.li}@uib.no

Zilong Liu
University of Essex, Colchester, UK
zilong.liu@essex.ac.uk

Abstract

Understanding the average zero-correlation zone (ZCZ) width of sequence sets is of strong interest for enhanced spread-spectrum systems whereby multiple users are deployed in a randomly distributed manner. For the first time in the literature, we study the average ZCZ of Golay-Davis-Jedwab (GDJ) complementary pairs. For a certain set of GDJ pairs, we show that its average ZCZ is dependent on the associated permutation and identify the permutation yielding the largest ZCZ width.

1 Introduction

A pair of sequences whose out-of phase aperiodic autocorrelation sums are all zero is known as the Golay complementary pair [1]. GCPs and their generalization, complementary codes, have been employed in various fields including radar waveform design, channel estimation, peak-to-average power ratio reduction, multi-carrier code-division multiple access (MC-CDMA), etc. It is noted that the number of mutually orthogonal GCPs or complementary codes is upper bounded by that of the constituent sequences. For a larger set size, multiple sequence sets with low inter-set correlation property were introduced in [2]. Almost at the same time, Z-complementary code set (ZCCS) was proposed in [3]. In a ZCCS, every code (which can be regarded as a two-dimensional matrix through proper arranging) exhibits a zero-correlation zone (ZCZ) for the aperiodic autocorrelation sums. Likewise, every pair of two distinct codes exhibits a zero cross-correlation zone. In practice, a ZCCS can be deployed to mitigate the multiuser interference due to quasi-synchronous transmission of MC-CDMA signals. Since then, a number of constructions on various types of sequence sets with ZCZ or low-correlation zone (LCZ) properties have been proposed [4–10].

It is noted that the existing constructions are mostly focused on enlarging the minimum ZCZ width. Due to the statistical nature of multiuser transmission, we argue that it is equally important to maximize the average ZCZ width of sequence sets. As the first initiative on this problem, we aim to investigate the average ZCZ width of a large set of

GCPs. Based on the GCP construction in [11] by Davis and Jedwab, also known as Golay-Davis-Jedwab (GDJ) pairs, we characterize the pairwise ZCZ within a set of GDJ pairs. We show that the ZCZ width of two different GDJ pairs is related to the permutation and linear terms in the corresponding generalized Boolean functions. Further, we prove that under the permutation σ_m (as given in Proposition 15), the largest average ZCZ can be achieved.

The remainder of this paper is outlined as follows. In Section 2, we introduce the notations and definitions that will be used throughout this paper. In Section 3, we investigate the ZCZ width between two GDJ pairs. In Section 4, we demonstrate that the largest average ZCZ width can be achieved by certain permutation.

2 Preliminaries

Throughout this paper, $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$ is the set of integers modulo a positive integer q and $\xi = e^{2\pi\sqrt{-1}/q}$ denotes a q-th primitive root of unity.

Let $\mathbf{a} = (a_0, a_1, \ldots, a_{L-1})$, $\mathbf{b} = (b_0, b_1, \ldots, b_{L-1})$ be two length-L sequences over $\mathbb{Z}_q$. The aperiodic cross-correlation function between $\mathbf{a}$ and $\mathbf{b}$ at displacement u is given by

$$\rho(\mathbf{a}, \mathbf{b})(u) = \begin{cases} \sum_{i=0}^{L-1-u} \xi^{a_i - b_{i+u}}, & 0 \le u < L, \\ \sum_{i=0}^{L+u-1} \xi^{a_{i-u} - b_i}, & -L < u < 0. \end{cases}$$

If $\mathbf{a} = \mathbf{b}$, then $\rho(\mathbf{a}, \mathbf{b})(u)$ represents the aperiodic autocorrelation of $\mathbf{a}$ and is denoted as $\rho(\mathbf{a})(u)$. Next, we introduce the concept of ZCZ sequences below.

Let $\mathbf{S} = \{\mathbf{s}_1, \mathbf{s}_2, \ldots, \ldots, \mathbf{s}_K\}$ be a set of K sequences where $\mathbf{s}_k = (s_{k,0}, s_{k,1}, \ldots, s_{k,L-1})$ for $1 \le k \le K$. $\mathbf{S}$ is called a Z-complementary set with ZCZ width Z if

$$\sum_{k=1}^{K} \rho(\mathbf{s}_k)(u) = \begin{cases} KL, & u = 0, \\ 0, & 1 \le |u| < Z. \end{cases} \tag{1}$$

If $Z = L$, a conventional complementary set is defined.

Definition 1. A set $\mathcal{C} = \{\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_M\}$, where $\mathbf{C}_i$ is a set of K sequences of length L, is called an (M, K, L, Z)-ZCCS if

$$\rho(\mathbf{C}_i, \mathbf{C}_j)(u) = \sum_{k=1}^{K} \rho(\mathbf{s}_k^i, \mathbf{s}_k^j)(u) = \begin{cases} KL, & u = 0, i = j, \\ 0, & 0 < |u| < Z, i = j, \\ 0, & |u| < Z, i \ne j, \end{cases} \tag{2}$$

where Z denotes the ZCZ width and each $\mathbf{C}_i = \{\mathbf{c}_0^i, \mathbf{c}_1^i, \ldots, \mathbf{c}_{K-1}^i\}$ consists of K length-L sequences for $1 \le i \le M$.

In an (M, K, L, Z)-ZCCS, any two Z-complementary codes are called a Z-complementary mate. If $Z = L$, a Z-complementary mate becomes the conventional complementary mate. It is shown that the maximum number of distinct Z-complementary mates is upper bounded by $K\lfloor L/Z \rfloor$ which is greater than the number K of conventional complementary mates. When a Z-complementary code set achieves the bound, it is said to be optimal [12].

Definition 2. Consider $\mathcal{C} = \{\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_M\}$, where each $\mathbf{C}_i$ is a set of K complementary sequences of length L. Denote by $Z(\mathbf{C}_i, \mathbf{C}_j)$ the mutual ZCZ width between $\mathbf{C}_i$ and $\mathbf{C}_j$ for $1 \le i, j \le M$. The average ZCZ of the set $\mathcal{C}$ is defined as follows:

$$\overline{Z} = \frac{\sum_{i=1}^{M} \sum_{j=1}^{M} Z(\mathbf{C}_i, \mathbf{C}_j)}{M^2}. \tag{3}$$

In general, it is challenging to explicitly determine the average ZCZ width for a set $\mathcal{C}$ as in Definition 2. In this paper we will investigate this problem for a set of binary complementary pairs from generalized Boolean functions.

Recall that generalized Boolean function (GBF) f of the m variables $x_1, x_2, \ldots, x_m$ is a mapping from $\mathbb{Z}_2^m$ to $\mathbb{Z}_q$. The monomial of degree r is a product of r variables of the form $x_{j_1} x_{j_2} \ldots x_{j_r}$ where $1 \le j_1 < j_2 < \cdots < j_r \le m$. A GBF f can be uniquely expressed as a linear combination of these 2^m monomials $1, x_1, \ldots, x_m, \ldots, x_1 x_2 \cdots x_m$, where the coefficient of each monomial belongs to $\mathbb{Z}_q$. For a GBF f, we define a sequence $\mathbf{f} = (\xi^{f_0}, \xi^{f_1}, \ldots, \xi^{f_{2^m-1}})$ of length 2^m corresponding to f where $f_i = f(i_1, i_2, \ldots, i_m)$ and $(i_1, i_2, \ldots, i_m)$ is the binary representation of the integer $i = \sum_{j=1}^{m} i_j 2^{j-1}$.

Davis and Jedwab in [11] established the connection between binary GCPs with Boolean functions and studied q-ary GCPs with length 2^m using the tool of GBFs, where q is a power of 2. We recall their constructed GDJ pairs as follows:

Theorem 3. *[11] Let m be a positive integer and π a permutation of the symbols $\{1, 2, \cdots, m\}$. Let f be a GBF given by*

$$f(x_1, x_2, \cdots, x_m) = \frac{q}{2} \sum_{k=1}^{m-1} x_{\pi(k)} x_{\pi(k+1)} + \sum_{k=1}^{m} c_{\pi(k)} x_{\pi(k)}, \tag{4}$$

where q is a power of 2 and $c_{\pi(k)} \in \mathbb{Z}_q$. Then, for any choice $d, d' \in \mathbb{Z}_q$, the sequence pair

$$(\mathbf{a}_0, \mathbf{a}_1) = (\mathbf{f} + d, \mathbf{f} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d') \tag{5}$$

is a complementary pair over $\mathbb{Z}_q$ of length 2^m.

The work was later generalized in [13] where those GBFs have co-domain $\mathbb{Z}_q$ for any positive even integer q. In this paper, we consider the GBFs with co-domain $\mathbb{Z}_q$ where q is even.

3 ZCZ of two GDJ pairs

This section studies the ZCZ width for GDJ pairs constructed by GBFs.

Theorem 4. *Let m be a positive integer and π a permutation of the symbols $\{1, 2, \cdots, m\}$. Let f be a GBF as in (4) and g be a GBF given by*

$$g(x_1, x_2, \cdots, x_m) = \frac{q}{2} \sum_{k=1}^{m-1} x_{\pi(k)} x_{\pi(k+1)} + \sum_{k=1}^{m} c'_{\pi(k)} x_{\pi(k)}, \tag{6}$$

where the first position that $(c'_{\pi(1)}, \ldots, c'_{\pi(m)})$ *and* $(c_{\pi(1)}, \ldots, c_{\pi(m)})$ *differ is at the index* t, $1 \le t \le m$, *and* $c_{\pi(t)} - c_{\pi(t)'} = q/2$. *Then, the GDJ pairs*

$$(\mathbf{a}_0, \mathbf{a}_1) = (\mathbf{f} + d, \mathbf{f} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d'), \quad (\mathbf{b_0}, \mathbf{b_1}) = (\mathbf{g} + d, \mathbf{g} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d')$$

form a Z-complementary mate of ZCZ width

$$Z = \frac{1}{2}\Big(2^{\pi(t+1)} - \sum_{\substack{k=t+2 \\ \pi(k)<\pi(t+1)}}^{m} 2^{\pi(k)}\Big), \tag{7}$$

where the summation is deemed as zero when $t = m - 1$.

Proof. Note $\rho(\mathbf{a}, \mathbf{b})(u) = \rho^*(\mathbf{a}, \mathbf{b})(-u)$ for $(\mathbf{a}, \mathbf{b}) \in \{(\mathbf{a}_0, \mathbf{b}_0), (\mathbf{a}_1, \mathbf{b}_1)\}$. To demonstrate pairs $(\mathbf{a}_0, \mathbf{a}_1)$ and $(\mathbf{b}_0, \mathbf{b}_1)$ have the ZCZ width Z, below we will investigate the value of

$$\begin{aligned} \rho(\mathbf{a}_0, \mathbf{b}_0)(u) + \rho(\mathbf{a}_1, \mathbf{b}_1)(u) &= \sum_{i=0}^{L-1-u} \xi^{a_{0,i} - b_{0,i+u}} + \sum_{i=0}^{L-1-u} \xi^{a_{1,i} - b_{1,i+u}} \\ &= \sum_{i=0}^{L-1-u} (\xi^{a_{0,i} - b_{0,i+u}} + \xi^{a_{1,i} - b_{1,i+u}}). \end{aligned} \tag{8}$$

For a given integer i, let $j = i + u$; also let $(i_1, i_2, \ldots, i_m)$ and $(j_1, j_2, \ldots, j_m)$ be the binary representations of i and j, respectively. Denoted by $v(i, j)$ the integer v such that

$$i_{\pi(v)} \ne j_{\pi(v)} \text{ and } i_{\pi(k)} = j_{\pi(k)}, \quad \forall\, 1 \le k < v. \tag{9}$$

We will simply denote $v(i, j)$ as v whenever there is no ambiguity. Then we consider four cases to show that for each (i, j) pair, either we have $\xi^{a_{0,i} - b_{0,j}} + \xi^{a_{1,i} - b_{1,j}} = 0$ or there exist integers $i' \le L - 1 - u$ and $j' = i' + u \le L - 1$ such that

$$\xi^{a_{0,i} - b_{0,j}} + \xi^{a_{1,i} - b_{1,j}} + \xi^{a_{0,i'} - b_{0,j'}} + \xi^{a_{1,i'} - b_{1,j'}} = 0.$$

Below we will divide our discussion into four cases.

Case 1 : When $v = 1$ which means $j_{\pi(1)} \ne i_{\pi(1)}$, we have

$$a_{0,i} - a_{1,i} - (b_{0,j} - b_{1,j}) = \frac{q}{2}(j_{\pi(1)} - i_{\pi(1)}). \tag{10}$$

Since $j_{\pi(1)} \ne i_{\pi(1)}$, from (10) we get $\frac{\xi^{a_{0,i} - a_{1,j}}}{\xi^{b_{0,i} - b_{1,j}}} = -1$, which implies $\xi^{a_{0,i} - b_{0,j}} + \xi^{a_{1,i} - b_{1,j}} = 0$.

Case 2 : When $1 < v \le t$, let $i' = (i_1, i_2, \ldots, 1 - i_{\pi(v-1)}, \ldots, i_m)$ and $j' = (j_1, j_2, \ldots, 1 - j_{\pi(v-1)}, \ldots, j_m)$ whose binary representations are different from i and j only at the position $\pi(v - 1)$ respectively. It is clear that $j' = i' + u$. Then we have

$$a_{0,i'} - a_{0,i} = \frac{q}{2} i_{\pi(v-2)} + \frac{q}{2} i_{\pi(v)} + c_{\pi(v-1)} - 2 i_{\pi(v-1)} c_{\pi(v-1)}. \tag{11}$$

According to $i_{\pi(v-1)} = j_{\pi(v-1)}$ and $i_{\pi(v-2)} = j_{\pi(v-2)}$, we have

$$\begin{aligned} a_{0,i} - a_{0,i'} - (b_{0,j} - b_{0,j'}) =& -\frac{q}{2} i_{\pi(v-2)} - \frac{q}{2} i_{\pi(v)} - c_{\pi(v-1)} + 2 i_{\pi(v-1)} c_{\pi(v-1)} \\ &+ \frac{q}{2} j_{\pi(v-2)} + \frac{q}{2} j_{\pi(v)} + c'_{\pi(v-1)} - 2 j_{\pi(v-1)} c'_{\pi(v-1)} \\ =& \frac{q}{2}(j_{\pi(v-2)} - i_{\pi(v-2)}) + \frac{q}{2}(j_{\pi(v)} - i_{\pi(v)}) + (c'_{\pi(v-1)} - c_{\pi(v-1)}) \\ &+ 2(c_{\pi(v-1)} i_{\pi(v-1)} - c'_{\pi(v-1)} j_{\pi(v-1)}) \\ \equiv& \frac{q}{2} + (2 i_{\pi(v-1)} - 1)(c_{\pi(v-1)} - c'_{\pi(v-1)}) \pmod q. \end{aligned}$$

Since $c_{\pi(v-1)} = c'_{\pi(v-1)}$ we have

$$a_{0,i} - a_{0,i'} - (b_{0,j} - b_{0,j'}) \equiv \frac{q}{2} \pmod q. \tag{12}$$

Similarly,

$$a_{1,i} - a_{1,i'} - (b_{1,j} - b_{1,j'}) \equiv \frac{q}{2} \pmod q. \tag{13}$$

Hence, for a pair $(i, j = i + u)$, if $v(i, j) \le t$, from (12) (13) we can derive $\frac{\xi^{a_{0,i} - b_{0,j}}}{\xi^{a_{0,i'} - b_{0,j'}}} = -1$ and $\frac{\xi^{a_{1,i} - b_{1,j}}}{\xi^{a_{1,i'} - b_{1,j'}}} = -1$. Thus,

$$\xi^{a_{0,i} - b_{0,j}} + \xi^{a_{1,i} - b_{1,j}} + \xi^{a_{0,i'} - b_{0,j'}} + \xi^{a_{1,i'} - b_{1,j'}} = 0, \tag{14}$$

which implies $\rho(\mathbf{a}_0, \mathbf{b}_0)(u) + \rho(\mathbf{a}_1, \mathbf{b}_1)(u) = 0$.

Case 3 : When $v = t + 1$, we have $c'_{\pi(v-1)} - c_{\pi(v-1)} = c'_{\pi(t)} - c_{\pi(t)} = q/2$ by assumption. Arguing as in *Case* 2, from (3) we can obtain

$$a_{0,i} - a_{0,i'} - (b_{0,j} - b_{0,j'}) \equiv 0 \pmod q$$

and

$$a_{1,i} - a_{1,i'} - (b_{1,j} - b_{1,j'}) \equiv 0 \pmod q.$$

Then we can derive $\xi^{a_{0,i} - b_{0,j}} = \xi^{a_{0,i'} - b_{0,j'}}$ and $\xi^{a_{1,i} - b_{1,j}} = \xi^{a_{1,i'} - b_{1,j'}}$. In this case, it is possible that

$$|\rho(\mathbf{a}_0, \mathbf{b_0})(u) + \rho(\mathbf{a}_1, \mathbf{b}_1)(u)| \ge 0.$$

Case 4 : When $v > t + 1$, let i'', j'' be two integers different from i, j in the position $\pi(t)$, i.e. $i'' = (i_1, i_2, \ldots, 1 - i_{\pi(t)}, \ldots, i_m)$. Then we have

$$a_{0,i''} - a_{0,i} = \frac{q}{2} i_{\pi(t-1)} + \frac{q}{2} i_{\pi(t+1)} + c_{\pi(t)} - 2 i_{\pi(t)} c_{\pi(t)}.$$

Therefore,

$$\begin{aligned} a_{0,i} - a_{0,i''} - (b_{0,j} - b_{0,j''}) =& -\frac{q}{2} i_{\pi(t-1)} - \frac{q}{2} i_{\pi(t+1)} - c_{\pi(t)} + 2 i_{\pi(t)} c_{\pi(t)} \\ &+ \frac{q}{2} j_{\pi(t-1)} + \frac{q}{2} j_{\pi(t+1)} + c'_{\pi(t)} - 2 j_{\pi(t)} c'_{\pi(t)} \\ =& \frac{q}{2}(j_{\pi(t-1)} - i_{\pi(t-1)}) + \frac{q}{2}(j_{\pi(t+1)} - i_{\pi(t+1)}) + (c'_{\pi(t)} - c_{\pi(t)}) \\ &+ 2(c_{\pi(t)} i_{\pi(t)} - c'_{\pi(t)} j_{\pi(t)}) \\ \equiv& (2 i_{\pi(t)} - 1)(c_{\pi(t)} - c'_{\pi(t)}) \pmod q. \end{aligned}$$

By the assumption that $c_{\pi(t)} - c'_{\pi(t)} = q/2$, we have

$$a_{0,i} - a_{0,i''} - (b_{0,j} - b_{0,j''}) \equiv \frac{q}{2} \pmod q \tag{15}$$

and

$$a_{1,i} - a_{1,i''} - (b_{1,j} - b_{1,j''}) \equiv \frac{q}{2} \pmod q. \tag{16}$$

As discussed above, for a integer u, if $v(i,j) > t$, where $j = i + u$, then $\rho(\mathbf{a}_0, \mathbf{b}_0)(u) + \rho(\mathbf{a}_1, \mathbf{b}_1)(u) = 0$. Based on the discussion for Cases 1-4, we see that $|\rho(\mathbf{a}_0, \mathbf{b}_0)(u) + \rho(\mathbf{a}_1, \mathbf{b}_1)(u)| > 0$ can only occur in Case 3, namely, the integers i and $j = i + u$ satisfy that

$$i_{\pi(t+1)} = j_{\pi(t+1)} \text{ and } i_{\pi(k)} = j_{\pi(k)}, \quad \forall\, 1 \le k \le t, \tag{17}$$

which implies

$$u = j - i = \sum_{k=v+2}^{m} 2^{\pi(k)-1}(j_{\pi(k)} - i_{\pi(k)}). \tag{18}$$

Next we discuss the minimum value of $|u|$, which corresponds to the ZCZ width, for possible values of u of the above form. Denote $w_k = j_{\pi(k)} - i_{\pi(k)}$, which takes values from $\{0, \pm 1\}$. From (18) we have

$$\begin{aligned} |u| &= \left| 2^{\pi(t+1)-1} w_{t+1} + \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-1} w_k + \sum_{\substack{k=t+2 \\ \pi(k)<\pi(t+1)}}^{m} 2^{\pi(k)-1} w_k \right| \\ &\ge \left| 2^{\pi(t+1)-1} w_{t+1} + \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-1} w_k \right| - \left| \sum_{\substack{k=t+2 \\ \pi(k)<\pi(t+1)}}^{m} 2^{\pi(k)-1} w_k \right| \\ &\ge \left| 2^{\pi(t+1)-1} w_{t+1} + \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-1} w_k \right| - \sum_{\substack{k=t+2 \\ \pi(k)<\pi(t+1)}}^{m} 2^{\pi(k)-1}, \end{aligned} \tag{19}$$

where the last inequality holds due to the fact that $w_k \in \{0, \pm 1\}$. Furthermore, by the fact that $w_{t+1} = j_{\pi(t+1)} - i_{\pi(t+1)} \neq 0$ we have

$$2^{\pi(t+1)-1} w_{t+1} + \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-1} w_k = w_{t+1} 2^{\pi(t+1)-1} \left(1 + \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-\pi(t+1)} \frac{w_k}{w_{t+1}} \right).$$

It is readily seen that

$$\left| 1 + \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-\pi(t+1)} \frac{w_k}{w_{t+1}} \right| \ge 1,$$

which implies

$$\left| 2^{\pi(t+1)-1} w_{t+1} + \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-1} w_k \right| \ge 2^{\pi(t+1)-1}.$$

This together with (19) shows that for any u such that i, $j = i + u$ satisfying (17), one has

$$|u| \geq Z = 2^{\pi(t+1)-1} - \sum_{\substack{k=t+2 \\ \pi(k)>\pi(t+1)}}^{m} 2^{\pi(k)-1}.$$

That is to say, for any $0 < |u| < Z$, we have $\rho(\mathbf{a}_0, \mathbf{b}_0)(u) + \rho(\mathbf{a}_1, \mathbf{b}_1)(u) = 0$. □

Remark 5. As in many works [5] [14], the ZCZ width in Theorem 4 is essentially a lower bound of the actual ZCZ width of GDJ pairs. While it is not certain whether $|\rho(\mathbf{a}_0, \mathbf{b}_0)(Z) + \rho(\mathbf{a}_1, \mathbf{b}_1)(Z)| > 0$ in Case 3, experiment results show that Z in Theorem 4 is indeed the actual ZCZ width of GDJ pairs for most permutations.

Remark 6. Suppose in Theorem 4 we choose functions f and g differing at $c_{\pi(m)}, c'_{\pi(m)}$, namely, $c_{\pi(m)} - c'_{\pi(m)} = \frac{q}{2}$, and $c_{\pi(i)} = c'_{\pi(i)}$ for $1 \leq i \leq m-1$. It is easy to see that we don't need to discuss Cases 3 and 4 in the proof of Theorem 4. That is to say, for any $0 < |u| < L$, Cases 1 and 2 imply that $\rho(\mathbf{a}_0, \mathbf{b}_0)(u) + \rho(\mathbf{a}_1, \mathbf{b}_1)(u) = 0$. This corresponds to the conventional Golay complementary mates.

From Theorem 4, we can easily obtain the following results.

Corollary 7. *Let* $(\mathbf{a}_0, \mathbf{a}_1) = (\mathbf{f} + d, \mathbf{f} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d')$ *and* $(\mathbf{b}_0, \mathbf{b}_1) = (\mathbf{g} + d, \mathbf{g} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d')$ *be GDJ pairs as in Theorem 4. Suppose that in* f *and* g, $c_{\pi(m-1)} - c'_{\pi(m-1)} = \frac{q}{2}$, *and* $c_{\pi(i)} = c'_{\pi(i)}$ *for* $1 \leq i \leq m-2$. *Then* $(\mathbf{a}_0, \mathbf{a}_1)$ *and* $(\mathbf{b}_0, \mathbf{b}_1)$ *have* ZCZ *of width* $2^{\pi(m)-1}$.

Corollary 8. *Let* $(\mathbf{a}_0, \mathbf{a}_1) = (\mathbf{f} + d, \mathbf{f} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d')$ *and* $(\mathbf{b}_0, \mathbf{b}_1) = (\mathbf{g} + d, \mathbf{g} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d')$ *be GDJ paris as defined in Theorem 4. Suppose that in the functions* f *and* g, $c_{\pi(m-2)} - c'_{\pi(m-2)} = \frac{q}{2}$, *and* $c_{\pi(i)} = c'_{\pi(i)}$ *for* $1 \leq i < m-2$. *Then the pairs* $(\mathbf{a}_0, \mathbf{a}_1)$ *and* $(\mathbf{b}_0, \mathbf{b}_1)$ *have* ZCZ *width* $\left|2^{\pi(m-1)-1} - 2^{\pi(m)-1}\right|$.

Proof. Substituting $t = m-2$ in Theorem 4, when $\pi(m) > \pi(m-1)$ we can derive $Z = 2^{\pi(m-1)-1}$ from (7). Similarly, if $\pi(m) < \pi(m-1)$ then $Z = 2^{\pi(m-1)-1} - 2^{\pi(m)-1}$. Therefore, the pairs $(\mathbf{a}_0, \mathbf{a}_1)$ and $(\mathbf{b}_0, \mathbf{b}_1)$ have ZCZ width $Z = \left|2^{\pi(m-1)-1} - 2^{\pi(m)-1}\right|$. □

The characterization on the ZCZ width of GDJ pairs in Theorem 4 motivates us to consider the average ZCZ width of a set of GDJ pairs. In Theorem 4 we have the condition $c_{\pi(t)} - c'_{\pi(t)} = q/2$. In next section we will consider the average ZCZ width of a set of binary GDJ pairs.

4 Average ZCZ widths for certain permutations

In this section we will investigate the average ZCZ property of a set of binary GDJ pairs. As shown in Theorem 3, we can denote by $f_{\mathbf{c},\pi}$ the m-variate Boolean function associated with the coefficient vector $\mathbf{c} \in \mathbb{Z}_2^m$ and the permutation π. Define a set

$$\mathcal{C}_\pi = \{\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_M\}, \tag{20}$$

where $\mathbf{C}_i = (\mathbf{f}_{\mathbf{c}_i,\pi} + d, \mathbf{f}_{\mathbf{c}_i,\pi} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d')$ is a binary GDJ pair generated by the function $f_{\mathbf{c}_i,\pi}$ as described in Theorem 3 and $\mathbf{c}_i \in \mathbb{Z}_2^m$. It is clear that $M = 2^m$. We will investigate the average ZCZ width of $\mathcal{C}_\pi$, denoted as $\overline{Z_\pi}$, for different permutations π on $\{1, 2, \ldots, m\}$.

We first give an auxiliary result, which will be frequently used to explicitly calculate the average ZCZ witdh of $\mathcal{C}_\pi$ for some permutations π.

Lemma 9. *Let $\mathbf{C}_i$ be a binary GDJ pair in $\mathcal{C}_\pi = \{\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_M\}$ as defined above, and $Z_{\pi,t}$ be given by as in (7) for integers t with $1 \le t \le m-1$. Then we have*

$$\#\{\mathbf{C}_j \in \mathcal{C}_\pi \mid Z(\mathbf{C}_i, \mathbf{C}_j) = Z_{\pi,t}\} = 2^{m-t},$$

where $Z(\mathbf{C}_i, \mathbf{C}_j)$ is the ZCZ width of $\mathbf{C}_i$ and $\mathbf{C}_j$.

Proof. Since $\mathbf{C}_i, \mathbf{C}_j$ are GDJ pairs which corresponding to $f_{\mathbf{c}_i,\pi}$ and $f_{\mathbf{c}_j,\pi}$ respectively. Given $f_{\mathbf{c}_i,\pi}$ where $\mathbf{c}_i = (c_{i,0}, \ldots, c_{i,k}, \ldots, c_{i,m})$, for $f_{\mathbf{c}_j,\pi}$ where $\mathbf{c}_j = (c_{j,0}, \ldots, c_{j,k}, \ldots, c_{j,m})$, if $c_{i,k}{=}c_{j,k}$ for $0 \le k < t$ then $Z(\mathbf{C}_i, \mathbf{C}_j) = Z_{\pi,t}$. As $(\mathbf{c}_{j,t+1}, \ldots, \mathbf{c}_{j,m}) \in \mathbb{Z}_2^{m-t}$ which means there are 2^{m-t} pairs $\mathbf{C}_j$ satisfying $Z(\mathbf{C}_i, \mathbf{C}_j) = Z_{\pi,t}$. □

Lemma 9 facilitates the calculation of $\overline{Z_\pi}$ in this section. Based on Theorem 4 and this lemma, for any permutation π on $\{1, 2, \ldots, m\}$, we have

$$\begin{aligned}
\overline{Z_\pi} &= \frac{\sum_{i=1}^{2^m}\sum_{j=1}^{2^m} Z(\mathbf{C}_i, \mathbf{C}_j)}{2^{2m}} = \frac{2^m(\sum_{t=1}^{m-1} 2^{m-t} Z_{\pi,t} + 2 \cdot 2^m)}{2^{2m}} \\
&= 2^{-m}\sum_{t=1}^{m-1} 2^{m-t}\Big(2^{\pi(t+1)-1} - \sum_{\substack{t+2\le u\le m \\ \pi(u)<\pi(t+1)}} 2^{\pi(u)-1}\Big) + 2 \\
&= \sum_{j=2}^{m} \frac{1}{2^j}\Big(2^{\pi(j)} - \sum_{\substack{j+1\le u\le m \\ \pi(u)<\pi(j)}} 2^{\pi(u)}\Big) + 2 \\
&= \Psi_\pi + 1,
\end{aligned} \tag{21}$$

where the second equality contains $2 \cdot 2^m$ corresponding to $\mathbf{C}_i, \mathbf{C}_j$ being the same and complementary mate, the third equality follows from the form of $Z_{\pi,t}$ in (7), and

$$\Psi_\pi = \sum_{j=1}^{m} \Psi_\pi(j) = \sum_{j=1}^{m} \frac{1}{2^j}\Big(2^{\pi(j)} - \sum_{\substack{u=j+1 \\ \pi(u)<\pi(j)}}^{m} 2^{\pi(u)}\Big), \tag{22}$$

where $\Psi_\pi(1) = \frac{1}{2}\Big(2^{\pi(1)} - \sum_{\substack{u=2 \\ \pi(u)<\pi(1)}}^{m} 2^{\pi(u)}\Big) = \frac{1}{2}\Big(2^{\pi(1)} - (2^{\pi(1)-1} + 2^{\pi(1)-2} + \cdots + 2)\Big) = 1.$

Below we first determine the average ZCZ with $\overline{Z_\pi}$ for certain special permutations π.

Proposition 10. *Let $\pi_k = (k, \ldots, m, 1, \ldots, k-1)$ be the permutation on $\{1, 2, \ldots, m\}$, where $1 \le k \le m$. Then we have*

$$\overline{Z_{\pi_k}} = \frac{1}{2}\Big(2^k(m-k-1) + 2^{k-m}(2^k + k - 3) + 6\Big).$$

Proof. According to the definition of π_k, we have that $\pi_k(m-k+1)=m$ and

$$\sum_{\substack{j+1\le u\le m\\ \pi_k(u)<\pi_k(j)}} 2^{\pi_k(u)-1}=\begin{cases}\sum\limits_{u=m-k+2}^{m} 2^{\pi_k(u)-1}, & 1\le j\le m-k+1;\\ 0, & m-k+2\le j\le m.\end{cases}$$

Then it follows from (21) that

$$\begin{aligned}\overline{Z_{\pi_k}}&=\sum_{j=1}^{m-k+1}2^{-j}\left(2^{\pi_k(j)}-\sum_{u=m-k+2}^{m}2^{\pi_k(u)}\right)+\sum_{j=m-k+2}^{m}2^{\pi_k(j)-j}+1\\ &=\sum_{j=1}^{m}2^{-j}\cdot 2^{\pi_k(j)}-\sum_{j=1}^{m-k+1}2^{-j}\left(\sum_{u=m-k+2}^{m}2^{\pi_k(u)}\right)+1\\ &=(m-(k-1))2^{k-1}+(k-1)2^{k-m-1}+(2^k-2)(2^{-(m-k+1)}-1)+1\\ &=2^{k-1}(m-k-1)+2^{k-m}(2^{k-1}+\frac{k-3}{2})+3.\end{aligned}$$

This completes the proof. □

In the following, we will identify the permutation on $\{1,2,\ldots,m\}$ such that the corresponding set $\mathcal{C}=\{\mathbf{C}_1,\ldots,\mathbf{C}_M\}$, where $M=2^m$, has the maximum average ZCZ width. To this end, we first introduce some notations for presentation simplicity.

Denote by Π the set of all permutations on $\{1,2,\ldots,m\}$. For a permutation $\pi\in\Pi$, we denote by $\pi^{-1}(t)$ the pre-image of t, where $1\le t\le m$, under π, i.e., $\pi(\pi^{-1}(t))=t$. Define sets

$$\begin{aligned}\Pi_1&=\{\pi\in\Pi\,|\,\pi^{-1}(m)>\pi^{-1}(m-1)\},\\ \Pi_2&=\{\pi\in\Pi\,|\,\pi^{-1}(m)<\pi^{-1}(m-1)\},\end{aligned}\tag{23}$$

and sets

$$\begin{aligned}\Pi_{1,1}&=\{\pi\in\Pi\,|\,\pi^{-1}(m)-\pi^{-1}(m-1)=1\},\\ \Pi_{1,2}&=\{\pi\in\Pi\,|\,\pi^{-1}(m)-\pi^{-1}(m-1)>1\}.\end{aligned}\tag{24}$$

Clearly, $\Pi=\Pi_1\sqcup\Pi_2$ and $\Pi_1=\Pi_{1,1}\sqcup\Pi_{1,2}$.

To identify the permutation that gives the largest average ZCZ width, we need the following lemmas, which give auxiliary results for proving the main theorem.

Lemma 11. *Given a permutation $\rho\in\Pi_2$ with $s=\rho^{-1}(m)$ and $t=\rho^{-1}(m-1)$, choose $\pi\in\Pi_1$ such that $\pi(s)=m-1,\pi(t)=m$ and $\pi(j)=\rho(j)$ for $j\neq s,t$. Then $\overline{Z_\pi}\ge\overline{Z_\rho}$.*

Proof. Since $\pi(j)=\rho(j)$ for $j\neq s,t$, it's easy to see that $\Psi_\pi(j)=\Psi_\rho(j)$ for $j\in\{1,2,\ldots,m\}\setminus\{s,t\}$. Hence, we have

$$\overline{Z_\pi}-\overline{Z_\rho}=\Psi_\pi(s)+\Psi_\pi(t)-\Psi_\rho(s)-\Psi_\rho(t)\tag{25}$$

and if $s = 1$ clearly, $\Psi_\pi(s) - \Psi_\rho(s) = 0$. By $\pi(s) = m$ and $\rho(t) = m - 1$ we have

$$\begin{aligned}\Psi_\pi(s) - \Psi_\rho(s) &= 2^{-s}\left(2^{m-1} - \sum_{\substack{s+1\le u\le m\\ \pi(u)<m-1}} 2^{\pi(u)} - (2^m - \sum_{s+1\le u\le m} 2^{\rho(u)})\right)\\ &= 2^{-s}\left(-2^{m-1} + 2^{\rho(t)} - \sum_{\substack{s+1\le u\le m\\ u\neq t}} 2^{\pi(u)} + \sum_{\substack{s+1\le u\le m\\ u\neq t}} 2^{\rho(u)}\right)\\ &= 0\end{aligned} \tag{26}$$

since $\pi(u) = \rho(u)$ for $s + 1 \le u \le m$ and $u \neq t$. Similarly, by $\pi(t) = m$ and $\rho(t) = m - 1$ we have

$$\begin{aligned}\Psi_\pi(t) - \Psi_\rho(t) &= 2^{-t}\left(2^m - \sum_{t+1\le u\le m} 2^{\pi(u)} - (2^{m-1} - \sum_{t+1\le u\le m} 2^{\rho(u)})\right)\\ &= 2^{-t}\left(2^{m-1} - \sum_{\substack{s+1\le u\le m\\ u\neq t}} 2^{\pi(u)} + \sum_{\substack{s+1\le u\le m\\ u\neq t}} 2^{\rho(u)}\right)\\ &= 2^{m-t-1}.\end{aligned} \tag{27}$$

Thus, $\overline{Z_\pi} - \overline{Z_\rho} > 0$. □

Lemma 12. *Given a permutation $\rho \in \Pi_{1,2}$ with $s = \rho^{-1}(m-1)$ and $t = \rho^{-1}(m)$, where $t \ge s + 2$, choose a permutation $\pi \in \Pi_{1,1}$ such that $\pi(s+1) = m, \pi(t) = \rho(s+1)$, and $\pi(j) = \rho(j)$ for $j \neq s+1, t$. Then $\overline{Z_\pi} \ge \overline{Z_\rho}$.*

Proof. Since $\pi(j) = \rho(j)$ for $j \in \{1, \dots, m\} \setminus \{s+1, t\}$, it is easy to see that

$$\Psi_\pi(j) = \Psi_\rho(j) \text{ for } j = 2, \dots, s, \text{ and } j = t+1, \dots, m,$$

where $\Psi_\pi(j)$, $\Psi_\rho(j)$ are given as in (22). Hence we have

$$\overline{Z_\pi} - \overline{Z_\rho} = \sum_{j=2}^{m} (\Psi_\pi(j) - \Psi_\rho(j)) = \sum_{j=s+1}^{t} (\Psi_\pi(j) - \Psi_\rho(j)).$$

By $\pi(s+1) = m$ and $\rho(t) = m$, we have

$$\begin{aligned}\Psi_\pi(s+1) - \Psi_\rho(s+1) &= 2^{-(s+1)}\left((2^m - \sum_{u=s+2}^{m} 2^{\pi(u)}) - (2^{\rho(s+1)} - \sum_{\substack{u=s+2\\ \rho(u)<\rho(s+1)}}^{m} 2^{\rho(u)})\right)\\ &= 2^{-(s+1)}\left(2^m - 2^{\rho(s+1)} - \sum_{\substack{u=s+2\\ \pi(u)\ge\rho(s+1)}}^{m} 2^{\pi(u)}\right)\end{aligned} \tag{28}$$

and

$$\begin{aligned}\Psi_\pi(t) - \Psi_\rho(t) &= 2^{-t}\left((2^{\pi(t)} - \sum_{\substack{u=t+1\\ \pi(u)<\pi(t)}}^{m} 2^{\pi(u)}) - (2^m - \sum_{u=t+1}^{m} 2^{\rho(u)})\right)\\ &= 2^{-t}\left(2^{\pi(t)} - 2^m + \sum_{\substack{u=t+1\\ \pi(u)\geq\pi(t)}}^{m} 2^{\pi(u)}\right),\end{aligned}$$

since $\pi(u) = \rho(u)$ for $u = t+1, \ldots, m$.

For $s+2 \leq j \leq t-1$, we have

$$\begin{aligned}\Psi_\pi(j) - \Psi_\rho(j) =& 2^{-j}\left((2^{\pi(j)} - \sum_{\substack{u=j+1\\ \pi(u)<\pi(j)}}^{m} 2^{\pi(u)}) - (2^{\rho(j)} - \sum_{\substack{u=j+1\\ \rho(u)<\rho(j)}}^{m} 2^{\rho(u)})\right)\\ =& \begin{cases} -2^{\pi(t)-j}, & \text{if } \pi(t) < \pi(j),\\ 0, & \text{otherwise,}\end{cases}\end{aligned}$$

which implies

$$\sum_{j=s+2}^{t-1}(\Psi_\pi(j) - \Psi_\rho(j)) = \begin{cases} 0, & \text{if } \pi(t) = m-2,\\ \sum_{\substack{j=s+2\\ \pi(j)>\pi(t)}}^{t-1} -2^{\pi(t)-j}, & \text{if otherwise.}\end{cases} \tag{29}$$

Thus, if $\pi(t) = \rho(s+1) = m-2$ then

$$\begin{aligned}\sum_{j=s+1}^{t}(\Psi_\pi(j) - \Psi_\rho(j)) &= 2^{-(s+1)}(2^m - 2^{\rho(s+1)}) + 2^{-t}\left(2^{\rho(s+1)} - 2^m\right)\\ &> 0,\end{aligned}$$

since $t \geq s+2$ and $\sum_{\pi(u)\geq\rho(s+1)}^{m}{}_{u=s+2} 2^{\pi(u)} = \sum_{\pi(u)\geq\pi(t)}^{m}{}_{u=t+1} 2^{\pi(u)} = 0$. Otherwise, from (29) we have

$$\sum_{\substack{j=s+2\\ \pi(j)>\pi(t)}}^{t-1} -2^{\pi(t)-j} \geq -2^{\pi(t)}(2^{-(s+2)} + \cdots + 2^{-(t-1)}) = -2^{\rho(s+1)}(2^{-(s+1)} - 2^{-(t-1)}),$$

then

$$\begin{aligned}\sum_{j=s+1}^{t}(\Psi_\pi(j) - \Psi_\rho(j)) &\geq 2^{-(s+1)}\left(2^m - 2^{\rho(s+1)} - \sum_{\substack{u=s+2\\ \pi(u)\geq\rho(s+1)}}^{m} 2^{\pi(u)}\right) + 2^{-t}\left(2^{\rho(s+1)} - 2^m\right) - 2^{\rho(s+1)}2^{-(s+1)}\\ &\geq 2^{-(s+1)}\left(2^m - 3\cdot 2^{\rho(s+1)} + 2^{\rho(s+1)-(t-s-1)} - 2^{m-(t-s-1)}\right) > 0,\end{aligned}$$

since $\rho(s+1) \leq m-3$. Thus, it shows $\overline{Z_\pi} \geq \overline{Z_\rho}$. □

For any permutation $\pi \in \Pi_{1,1}$, define sets

$$\begin{aligned} P_1 &= \{\pi \in \Pi_{1,1} \,|\, \pi^{-1}(m-2) = 1, \pi^{-1}(m-1) = 2\}, \\ P_2 &= \{\pi \in \Pi_{1,1} \,|\, \pi^{-1}(m-2) < \pi^{-1}(m-1)\}, \\ P_3 &= \{\pi \in \Pi_{1,1} \,|\, \pi^{-1}(m-2) > \pi^{-1}(m)\}. \end{aligned} \tag{30}$$

Clearly, $\Pi_{1,1} = P_2 \sqcup P_3$, for these sets we have the following lemmas:

Lemma 13. *Given a permutation $\rho \in P_3$ with $s = \rho^{-1}(m-1)$ and $t = \rho^{-1}(m-2)$ where $s \geq 2$, choose a permutation $\pi \in P_2$ such that $\pi(s) = m-1, \pi(s-1) = m-2$ and $\pi(j) = \rho(j)$ for $j \neq s-1, t$. Then $\overline{Z_\pi} \geq \overline{Z_\rho}$.*

Proof. Since $\pi(j) = \rho(j)$ for $j \neq s-1, t$, we can derive that $\pi(t) = \rho(s-1)$ and $\pi(t) < m-2$. Then from 22, we have

$$\overline{Z_\pi} - \overline{Z_\rho} = \sum_{j=s-1}^{t} (\Psi_{\pi(j)} - \Psi_{\rho(j)}) \tag{31}$$

In (31), for $j = s-1$,

$$\begin{aligned} \Psi_{\pi(s-1)} - \Psi_{\rho(s-1)} &= 2^{-(s-1)} \left(2^{\pi(s-1)} - 2^{\rho(s-1)} - \sum_{\substack{u=s \\ \pi(u)<\pi(s-1)}}^{m} 2^{\pi(u)} + \sum_{\substack{u=s \\ \rho(u)<\rho(s-1)}}^{m} 2^{\rho(u)} \right) \\ &= 2^{-(s-1)} \left(2^{m-2} - 2 \cdot 2^{\pi(t)} - \sum_{\substack{u=s+2 \\ \pi(u)>\pi(t)}}^{m} 2^{\pi(u)} \right) \geq 0. \end{aligned}$$

For $s \leq j \leq t$, we have

$$\begin{aligned} \sum_{j=s}^{t} (\Psi_{\pi(j)} - \Psi_{\rho(j)}) &= (2^{-s} + 2^{-(s+1)})(2^{m-2} - 2^{\pi(t)}) - 2^{-j} \sum_{\substack{j=s+2 \\ \pi(j)>\pi(t)}}^{t-1} 2^{\pi(t)} - 2^{-t}(2^{m-2} - 2^{\pi(t)}) \\ &> (2^{-s} + 2^{-(s+1)})(2^{m-2} - 2^{\pi(t)}) - 2^{-(s+1)} 2^{\pi(t)} - 2^{-t}(2^{m-2} - 2^{\pi(t)}) > 0. \end{aligned}$$

Thus, we can derive that $\sum_{j=s-1}^{t} (\Psi_{\pi(j)} - \Psi_{\rho(j)}) > 0$ which implies $\overline{Z_\pi} > \overline{Z_\rho}$. □

Lemma 14. *For any permutation $\rho \in \Pi_{1,1} \setminus P_1$ and $\pi \in P_1$ with $\pi(1) = m-2$ and $\pi(2) = m-1$. Then $\overline{Z_\pi} \geq \overline{Z_\rho}$.*

Proof. Since $\pi \in P_1$ then we have

$$\overline{Z_\pi} = 2^{-2}(2^{m-2} + 2) + 2^{-3}(3 \cdot 2^{m-2} + 2) + \sum_{j=4}^{m} \Psi_\pi(j) + 2.$$

Suppose $\rho(s) = m-1$, there are three cases as below.

Case $1: s = 1$, By assumption $\rho(1) = m-1$ and $\rho(2) = m$. Clearly $\rho^{-1}(m-2) \geq 2$. Suppose $\rho(t) = m-2$, when $t = 3$, chose $\pi \in P_1$ such that $\pi(j) = \rho(j)$ for $4 \leq j \leq m$ then

$$\overline{Z_\rho} = 2^{-2}(2^m - (2^{m-1} - 2)) + 2^{-2} + \sum_{j=4}^{m} \Psi_\rho(j) + 2.$$

Hence, we have

$$\overline{Z_\pi} - \overline{Z_\rho} = \sum_{j=2}^{m} (\Psi_\pi(j) - \Psi_\rho(j)) = 2^{-3} \cdot 2^{m-2} > 0 \quad , \tag{32}$$

since $\Psi_\pi(j) = \Psi_\rho(j)$ for $4 \leq j \leq m$. When $t > 3$, let $\pi(t) = \rho(3)$ and $\pi(j) = \rho(j)$ for $3 \leq j \leq m$ and $j \neq t$, then

$$\begin{aligned}
\overline{Z_\pi} - \overline{Z_\rho} &= 2^{-3}(2^{m-2} + 2) + \sum_{j=4}^{m} \Psi_\pi(j) - \sum_{j=3}^{m} \Psi_\rho(j) \\
&= 2^{-3}(2^{m-2} + 2) + \sum_{j=4}^{t} \Psi_\pi(j) - \sum_{j=3}^{t-1} \Psi_\rho(j) - \Psi_\rho(t) \\
&= 2^{-3}(2^{m-2} + 2) - 2^{-3}(2^{\rho(3)} - \sum_{\substack{u=4 \\ \rho(u)<\rho(3)}}^{m} 2^{\rho(u)}) - \sum_{\substack{j=4 \\ \pi(j)>\pi(t)}}^{t-1} 2^{-j}(2^{\pi(t)}) + (2^{\pi(t)} - 2^{m-2}) \\
&\geq \left(\frac{5}{3} \cdot 2^{m-6} - 2^{m-2-t} + 2^{m-2t+1} - 2^{-t} + \frac{2^{m-2t}}{3} \right) \\
&> 0.
\end{aligned}$$

Case $2: s = 2$, It can be derived from Lemma 13 directly that $\overline{Z_\pi} - \overline{Z_\rho} > 0$.

Case $3: s \geq 3$, According to Lemma 13, it's sufficient to consider the permutation ρ such that $\rho^{-1}(m-2) < s$. Thus there exists $\pi \in P_1$ such that $\pi(j) = \rho(j)$ for $s+2 \leq j \leq m$, then we have

$$\begin{aligned}
\overline{Z_\pi} - \overline{Z_\rho} = 2^{-2}(2^{m-2} + 2)) + 2^{-3}(3 \cdot 2^{m-2} + 2) + \sum_{j=4}^{s+1} \Psi_\pi(j) \\
- \sum_{j=2}^{s-1} \Psi_\rho(j) - 2^{-s} \left(2^{m-1} - \sum_{\substack{u=s+1 \\ \rho(u)<m-1}}^{m} 2^{\rho(u)} \right) + 2^{-(s+1)} \left(2^m - \sum_{\substack{u=s+2 \\ \rho(u)<m}}^{m} 2^{\rho(u)} \right),
\end{aligned}$$

When $s = 3$,

$$\overline{Z_\pi} - \overline{Z_\rho} > (2^{m-3} + 2^{-1} + 2^{m-5} + 2^{-2}) - 2^{-2}\left(2^{m-3} - 2\right) + 2^{-3}2^{m-1} + 2^{-4}2^m > 0,$$

and when $s > 3$,

$$\overline{Z_\pi} - \overline{Z_\rho} > (2^{m-3} + 2^{-1} + 2^{m-5} + 2^{-2}) - 2^{-2}(2^{m-1} + 2) + 2^{-3}(2^{m-3}) + 2^{-4}2^{m-2} > 0.$$

From the discussion above we show that $\overline{Z_\pi} > \overline{Z_\rho}$. □

Proposition 15. *Let $\sigma_1 = (1)$, $\sigma_2 = (1,2)$ and $\sigma_3 = (1,2,3)$, and for $m \geq 3$, let*

$$\sigma_m = \begin{cases} (m-2, m-1, m)||\ldots||\sigma_1, & \text{if } m \equiv 1 \mod 3, \\ (m-2, m-1, m)||\ldots||\sigma_2, & \text{if } m \equiv 2 \mod 3, \\ (m-2, m-1, m)||\ldots||\sigma_3, & \text{if } m \equiv 3 \mod 3. \end{cases} \tag{33}$$

Then for any permutation $\pi \in \Pi_{1,1}$ with $(\pi(1), \pi(2), \pi(3)) = (m-2, m-1, m)$, we have $\overline{Z_{\sigma_m}} \geq \overline{Z_\pi}$.

Theorem 16. *Let Π be the set of permutations on $\{1, 2, \ldots, m\}$ and $\sigma_m \in \Pi$ be the permutation as given in (33). Then, among all permutations π in Π, the maximum average ZCZ width of $\mathcal{C}_\pi = \{\mathbf{C}_1, \ldots, \mathbf{C}_M\}$ is given by $\overline{Z_{\sigma_m}} = \Psi_{\sigma_m} + 1$, where*

$$\Psi_{\sigma_m} = \frac{1}{2^3}(5 \cdot 2^{m-2} + 14 + \Psi_{\sigma_{m-3}}),$$

and $\Psi_{\sigma_t} = t$ for $t \in \{1, 2, 3\}$; or equivalently,

$$\Psi_{\sigma_m} = 5 \cdot 2^{m-5} \cdot \frac{1 - 2^{-6m_1}}{1 - 2^{-6}} + \frac{14}{8} \cdot \frac{1 - 2^{-3m_1}}{1 - 2^{-3}} + \frac{t}{2^{3m_1}}, \tag{34}$$

where $m = 3m_1 + t$ with $t \in \{1, 2, 3\}$.

Proof. Recall that $\Pi = \Pi_1 \sqcup \Pi_2$, $\Pi_1 = \Pi_{1,1} \sqcup \Pi_{1,2}$ and $\Pi_1 = P_1 \sqcup P_2$, where $\sqcup$ denotes the union of disjoint sets. Suppose π is the permutation in Π such that the corresponding $\overline{Z_\pi}$. Lemmas 11 and 12 shows that π belongs to $\Pi_{1,1}$. Furthermore, by Proposition 15, we see that $\pi = \sigma_m$ is the permutation with the maximum average ZCZ width. According to (3) and (22), it suffices to consider Ψ_{σ_m} and we have

$$\begin{aligned}
\Psi_{\sigma_m} =& \sum_{j=1}^{m} \frac{1}{2^j}\Big(2^{\sigma_m(j)} - \sum_{\substack{u=j+1 \\ \sigma_m(u)<\sigma_m(j)}}^{m} 2^{\sigma_m(u)}\Big) \\
=& \frac{1}{2}\big(2^{m-2} - (2^{m-2} - 2)\big) + \frac{1}{2^2}\big(2^{m-1} - (2^{m-2} - 2)\big) \\
&+ \frac{1}{2^3}\big(2^m - (2^{m-2} - 2)\big) + \sum_{j=4}^{m} \frac{1}{2^j}\Big(2^{\sigma_m(j)} - \sum_{\substack{u=j+1 \\ \sigma_m(u)<\sigma_m(j)}}^{m} 2^{\sigma_m(u)}\Big) \\
=& \frac{1}{2^3}(5 \cdot 2^{m-2} + 14) + \frac{1}{2^3}\sum_{j=1}^{m-3} \frac{1}{2^j}\Big(2^{\sigma_{m-3}(j)} - \sum_{\substack{u=j+1 \\ \sigma_{m-3}(u)<\sigma_{m-3}(j)}}^{m-3} 2^{\sigma_{m-3}(u)}\Big) \\
=& \frac{1}{2^3}(5 \cdot 2^{m-2} + 14 + \Psi_{\sigma_{m-3}}).
\end{aligned}$$

Following the above recursive relation, the expression in (34) can be easily obtained. □

Below we list the maximum average ZCZ width for the Z-complementary set defined in (20) for small integers m with $3 \leq m \leq 10$.

m	3	4	5	6	7	8	9	10
$\overline{Z}_{\max}$	4	$\frac{43}{8}$	8	$\frac{105}{8}$	$\frac{1491}{64}$	$\frac{349}{8}$	$\frac{5393}{64}$	$\frac{84744}{512}$

We show the average ZCZ width of a set composed by all possible GDJ pairs generated by different GBFs. Now we show that according to the algorithm below we can construct a set with optimal average ZCZ width.

5 Conclusion

This paper focused on understanding the average ZCZ of complementary sequence sets motivated by their random deployment nature in practical spread-spectrum communication systems.

We have first derived a lower bound of their ZCZ width for two GDJ pairs, showing that the width is associated with the difference in linear coefficients and permutations within the corresponding GBF. Based on this finding, we have then studied the average ZCZ width of a set of GDJ pairs and provided the expression for a class of cyclic permutations. By comparing the average ZCZ width across different permutations, it is found that that the largest average ZCZ can be achieved by certain permutation family.

References

[1] M. Golay, "Complementary series," *IRE Transactions on Information Theory*, vol. 7, no. 2, pp. 82–87, 1961.

[2] G. Gong, "Constructions of multiple shift-distinct signal sets with low correlation," in *2007 IEEE International Symposium on Information Theory*. IEEE, 2007, pp. 2306–2310.

[3] P. Fan, W. Yuan, and Y. Tu, "Z-complementary binary sequences," *IEEE Signal Processing Letters*, vol. 14, no. 8, pp. 509–512, 2007.

[4] P. Sarkar, C. Li, S. Majhi, and Z. Liu, "New correlation bound and construction of quasi-complementary sequence sets," *IEEE Transactions on Information Theory*, 2024.

[5] P. Sarkar, S. Majhi, and Z. Liu, "Optimal Z-complementary code set from generalized Reed-Muller codes," *IEEE Transactions on Communications*, vol. 67, no. 3, pp. 1783–1796, 2019.

[6] Z. Liu, U. Parampalli, Y. L. Guan, and S. Boztas, "Constructions of optimal and near-optimal quasi-complementary sequence sets from Singer difference sets," *IEEE Wireless Communications Letters*, vol. 2, no. 5, pp. 487–490, 2013.

[7] S. Das, U. Parampalli, S. Majhi, Z. Liu, and S. Budišin, "New optimal Z-complementary code sets based on generalized paraunitary matrices," *IEEE Transactions on Signal Processing*, vol. 68, pp. 5546–5558, 2020.

[8] H. Xiao and X. Cao, "New constructions of mutually orthogonal complementary sets and Z-complementary code sets based on extended Boolean functions," *Cryptography and Communications*, vol. 16, no. 1, pp. 167–184, 2024.

[9] T. Yu, A. R. Adhikary, Y. Wang, and Y. Yang, "New class of optimal Z-complementary code sets," *IEEE Signal Processing Letters*, vol. 29, pp. 1477–1481, 2022.

[10] X. Tang, P. Fan, and J. Lindner, "Multiple binary ZCZ sequence sets with good cross-correlation property based on complementary sequence sets," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 4038–4045, 2010.

[11] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes," *IEEE Transactions on information theory*, vol. 45, no. 7, pp. 2397–2417, 1999.

[12] L. Feng, P. Fan, and X. Zhou, "Lower bounds on correlation of Z-complementary code sets," *Wireless personal communications*, vol. 72, no. 2, pp. 1475–1488, 2013.

[13] K. Paterson, "Generalized Reed-Muller codes and power control in OFDM modulation," *IEEE Transactions on Information Theory*, vol. 46, no. 1, pp. 104–120, 2000.

[14] P. Sarkar and S. Majhi, "A direct construction of optimal ZCCS with maximum column sequence PMEPR two for MC-CDMA system," *IEEE Communications Letters*, vol. 25, no. 2, pp. 337–341, 2020.

New Constructions of Two-Dimensional Binary Z-Complementary Array Pairs

Kai Liu *, Fanfei Meng, Mohan Xiang

School of Information Science and Engineering
Yanshan University
Qinhuangdao, China.

liukai@ysu.edu.cn

Abstract

The Z-complementary array pair (ZCAP) is a two-dimensional extension of the Z-complementary sequence pair, applied to radar waveform design, spatial synchronization, and two-dimensional multi-carrier CDMA systems. We suggest optimal binary Type-I and Type-II ZCAPs using concatenation, interleaving, and iteration techniques to further ZCAP research. The zero correlation zone (ZCZ) ratio of the constructed ZCAPs approaches 1. Our constructions provide new design methods for ZCAPs and improve the flexibility and adaptability of ZCAP parameters beyond the current literature.

Key words:Z-complementary array pair, Z-complementary sequence pair, zero correlation zone.

1 Introduction

In 1951, while investigating an optical problem in multislit spectroscopy, M.J.E. Golay introduced the concept of complementary sequence pairs, i.e., pairs of sequences with zero aperiodic autocorrelation and zero in each nonzero time shift, known as Golay complementary pairs (GCPs) [1]. However, available lengths for GCPs are very limited. For instance, the length of a binary GCP exists exclusively in the form$2^{\alpha}10^{\beta}26^{\gamma}$[2], where α, β, and γ are nonnegative integers. To obtain flexible sequence length, Fan et al. introduced the concept of "zero correlation zone (ZCZ)" in 2007 [3], which defines an aperiodic Z-complementary pair (ZCP) by specifying that the aperiodic autocorrelation sum of sequence pairs is zero only in a segment of intervals. The Golay complementary array pair (GCAP) is a two-dimensional extended form of GCP [4], with row length and column

*The authors are supported in part by the Natural Science Foundation of Hebei Province under Grant F2023203066, and in part by the Key Laboratory Project of Hebei Province, China under Grant 202250701010046.

length of $2^{\alpha}10^{\beta}26^{\gamma}$. The Z-complementary array pair (ZCAP) as the extension of GCAP can provide flexible row and column lengths [5], which can be applied to two-dimensional radars [6], two-dimensional synchronization [7], and two-dimensional multi-carrier CDMA systems [8]. ZCAPs possess the two-dimensional ZCZ property where in the sum of the aperiodic autocorrelation functions of consistent arrays is zero in a specific area. Similar to ZCPs, ZCAPs have an extremely wide parameter range and are divided into Type-I ZCAPs and Type-II ZCAPs according to different positions of ZCZ in the array [9].

In contrast to the extensively studied ZCPs over many years [10-21], there are comparatively fewer research methods and results available for the ZCAPs. In general, ZCAP construction approaches include the direct methods and the indirect methods. Two-dimensional Boolean functions are an effective tool for directly generating ZCAPs. By designing different kinds of two-dimensional Boolean functions, Pai obtained ZCAPs with array size $2^n \times \sum_{\alpha=t+1}^{m-1} d_\alpha 2^{\alpha-1} + 2^v$[22], Abhishek Roy constructed ZCAPs with array size $(2^{m_1-1} + 2^{n+1}) \times (2^{m_2} + 4)$[23], and Zhang constructed ZCAPs with array size $14 \cdot 2^{n-4} \times 2^m$[24]. Accordingly, the direct methods yield limited results in terms of array size and ZCZ size. To enlarge the parameter range, the indirect methods play a key role. Based on the existing ZCPs and ZCAPs, Pai et al. utilized the Kronecker product, concatenation operation, and interleaving operation to obtain Type-I ZCAPs with varying array sizes. Besides, as Type-II ZCAP can suppress asynchronous interference in MC-CDMA system, Pai et al. also proposed a design for Type-II ZCAPs, but the parameters remained constrained[9]. Consequently, in this paper, we generate four class of two-dimensional ZCAPs with new parameters, including optimal Type-I ZCAPs and Type-II ZCAPs by employing concatenation, interleaving, and interation techniques.

The rest of the paper is organized as follows. In Section 2, some basic notations and definitions are provided. In Section 3, several construction methods of Type-I ZCAPs, including optimal ZCAPs, are presented using the concatenation, Kronecker product, and interleaving methods, and the construction results of various parameters are obtained. In Section 4, Type-II ZCAPs are designed based on the iteration method. In Section 5, the parameters of the constructed ZCAPs are analyzed and compared to the literature. Section 6 concludes this paper.

2 Preliminaries

Let $\boldsymbol{C}$ be a binary array of size $L_1 \times L_2$, $\boldsymbol{C} = (c_{i,j}, 0 \le i < L_1, 0 \le j < L_2)$, where $(c_{i,j}) \in \{+1, -1\}$. For convenience, let " $+$ " and " $-$ " denote "1" and "-1", respectively.

- x^* stands for the conjugate of the complex number x.
- $(\cdot)^T$ denotes the transposition of $(\cdot)$, where $(\cdot)$ can represent a sequence or an array.
- Let $\boldsymbol{D} = (d_{i,j}, 0 \le i < L_1, 0 \le j < L_2)$ be also an array of size $L_1 \times L_2$. c_j and d_j denote the respective column vectors of arrays $\boldsymbol{C}$ and $\boldsymbol{D}$. The concatenation operation of arrays $\boldsymbol{C}$ and $\boldsymbol{D}$ is expressed as

$$\boldsymbol{C} \parallel \boldsymbol{D} = (c_0, c_1, \ldots, c_{L_2-1}, d_0, d_1, \ldots, d_{L_2-1}), \tag{1}$$

where "$\|$" stands for concatenation operator.

• $\odot$ represents the interleaving operation, and the interleaving of arrays $\boldsymbol{C}$ and $\boldsymbol{D}$ is expressed as follows

$$\boldsymbol{C} \odot \boldsymbol{D} = (c_0, d_0, c_1, d_1 \ldots, c_{L_2-1}, d_{L_2-1}), \tag{2}$$

where c_j and d_j denote the column vectors of arrays $\boldsymbol{C}$ and $\boldsymbol{D}$, respectively.

Definition 1. The two-dimensional aperiodic cross-correlation function (ACCF) of arrays $\boldsymbol{C}$ and $\boldsymbol{D}$ at the shift (u_1, u_2) is defined as

$$\rho(\boldsymbol{C}, \boldsymbol{D}; u_1, u_2) = \sum_{i=0}^{L_1-1-u_1} \sum_{i=0}^{L_2-1-u_2} c_{i,j} d_{i+u_1, j+u_2}, \tag{3}$$

where $0 \le u_1 < L_1, 0 \le u_2 < L_2$. When $\boldsymbol{C} = \boldsymbol{D}$, $\rho(\boldsymbol{C}, \boldsymbol{C}; u_1, u_2)$ is called the aperiodic autocorrelation function (AACF), denoted by $\rho(\boldsymbol{C}; u_1, u_2)$. If $L_1 = 1$, the array $\boldsymbol{C}$ becomes a sequence $\boldsymbol{C} = (c_j, j = 0, 1, \ldots, L_2 - 1)$, then the AACF of the sequence $\boldsymbol{C}$ can be expressed as

$$\rho(\boldsymbol{C}; u) = \sum_{j=0}^{L_2-1-u} c_j c_{j+u}, \tag{4}$$

Definition 2. [3] If a pair of sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ of length L satisfies

$$\rho(\boldsymbol{a}; u) + \rho(\boldsymbol{b}; u) = \begin{cases} 2L, u = 0 \\ 0, -Z < u < Z, u \ne 0 \end{cases} \tag{5}$$

where Z represents the ZCZ width, then the sequence pair $(\boldsymbol{a}, \boldsymbol{b})$ is called a Z-complementary pairs, denoted as $(L, Z) - \text{ZCP}$.

Definition 3. [3] If two $(L, Z) - \text{ZCPs}$ $(\boldsymbol{a}, \boldsymbol{b})$ and $(\boldsymbol{c}, \boldsymbol{d})$ satisfy

$$\rho(a, c; u) + \rho(b, d; u) = 0, \ \textit{where } 0 \le u < Z \tag{6}$$

then $(\boldsymbol{a}, \boldsymbol{b})$ and $(\boldsymbol{c}, \boldsymbol{d})$ are said to be mates to each other.

Definition 4. [4] If the AACF sum of arrays $\boldsymbol{C}$ and $\boldsymbol{D}$ of size $L_1 \times L_2$ satisfies

$$\rho(\boldsymbol{C}; u_1, u_2) + \rho(\boldsymbol{D}; u_1, u_2) = \begin{cases} 2L_1L_2, (u_1, u_2) = (0, 0) \\ 0, 0 \le |u_1| < Z_1, 0 \le |u_2| < Z_2, (u_1, u_2) \ne (0, 0) \end{cases} \tag{7}$$

then $(\boldsymbol{C}, \boldsymbol{D})$ is called a Type-I ZCZ complementary array pair (ZCAP), denoted as Type-I $((L_1, L_2), (Z_1, Z_2)) - \text{ZCAP}$.

In particular, the proof of ZCAPs in the following theorems of this paper is given only for $u_1 \ge 0$ and $u_2 \ge 0$. The proof process for $u_1 \le 0$ and $u_2 \le 0$ is similar, so it is omitted.

Definition 5. [5] If the AACF sum of arrays $\boldsymbol{C}$ and $\boldsymbol{D}$ of size $L_1 \times L_2$ satisfies

$$\rho(\boldsymbol{C}; u_1, u_2) + \rho(\boldsymbol{D}; u_1, u_2) = 0, L_1 - Z_1 < |u_1| < L_1 \text{ or } L_2 - Z_2 < |u_2| < L_2 \tag{8}$$

then $(\boldsymbol{C}, \boldsymbol{D})$ is referred to as a Type-II $((L_1, L_2)(Z_1, Z_2)) - \text{ZCAP}$.

Definition 6. [22] The ZCZ ratio of $((L_1, L_2)(Z_1, Z_2)) - \text{ZCAP}$ is defined as

$$ZCZ_{ratio} = \frac{Z_1 Z_2}{L_1 L_2} \tag{9}$$

Definition 7. [10] A binary odd-length $(L, Z) - \text{ZCP}$ $(\boldsymbol{a}, \boldsymbol{b})$ is said to be Z-optimal if the parameters satisfy $Z = \frac{L+1}{2}$, and a binary even-length $(L, Z) - \text{ZCP}$ is said to be Z-optimal if the parameters satisfy $Z = L - 2$.

Definition 8. [9] Let $(\boldsymbol{A}, \boldsymbol{B})$ be a binary $((L_1, L_2)(Z_1, Z_2)) - \text{ZCAP}$, where L_1 and L_2 are odd. If $Z_1 Z_2 = \left(\frac{L_1+1}{2}\right)\left(\frac{L_2+1}{2}\right)$, then $(\boldsymbol{A}, \boldsymbol{B})$ is said to be Z-optimal. For an binary $((L_3, L_4)(Z_3, Z_4)) - \text{ZCAP}$, if one of its dimensions is odd and the other is even, then it is called an optimal ZCAP when $Z_1 Z_2 \leq \max((L_3 - 1) L_4, L_3 (L_4 - 1))$.

3 Construction of Type-I ZCAPs

In this section, two classes of ZCAPs are constructed by the concatenation operation and interleaving methods based ZCPs and ZCAPs. By utilizing the optimal odd-length ZCP as the base sequence in Theorem 1, we can optimize the resulting two-dimensional ZCAP.

Theorem 1. *Let* $(\boldsymbol{a}, \boldsymbol{b})$ *be an* $(L, Z) - \text{ZCP}$ *and* $(\boldsymbol{c}, \boldsymbol{d}) = \left(\overleftarrow{\boldsymbol{b}}, -\overleftarrow{\boldsymbol{a}}\right)$ *be a mate of* $(\boldsymbol{a}, \boldsymbol{b})$*, where* $\overleftarrow{\boldsymbol{a}}$ *and* $\overleftarrow{\boldsymbol{b}}$ *represents the reverse of* $\boldsymbol{a}$ *and* $\boldsymbol{b}$*, respectively. The array pairs* $(\boldsymbol{M}, \boldsymbol{N})$ *are constructed by the following operations.*

I. $\boldsymbol{M} = (\boldsymbol{a}^T \parallel \boldsymbol{c}^T \parallel \boldsymbol{a}^T), N = (\boldsymbol{b}^T \parallel \boldsymbol{d}^T \parallel \boldsymbol{b}^T)$;

II. $\boldsymbol{M} = \left(\boldsymbol{a}^T \parallel \boldsymbol{a}^T \parallel -\boldsymbol{a}^T \parallel \boldsymbol{c}^T \parallel -\boldsymbol{a}^T\right), \boldsymbol{N} = \left(\boldsymbol{b}^T \parallel \boldsymbol{b}^T \parallel -\boldsymbol{b}^T \parallel \boldsymbol{d}^T \parallel -\boldsymbol{b}^T\right)$;

III. $\boldsymbol{M} = \left(\boldsymbol{a}^T \parallel \boldsymbol{a}^T \parallel \boldsymbol{c}^T \parallel -\boldsymbol{c}^T \parallel \boldsymbol{a}^T \parallel -\boldsymbol{c}^T \parallel -\boldsymbol{a}^T\right)$,
$\boldsymbol{N} = \left(\boldsymbol{b}^T \parallel \boldsymbol{b}^T \parallel \boldsymbol{d}^T \parallel -\boldsymbol{d}^T \parallel \boldsymbol{b}^T \parallel -\boldsymbol{d}^T \parallel -\boldsymbol{b}^T\right)$;

IV. $\boldsymbol{M} = \left(\boldsymbol{a}^T \parallel \boldsymbol{a}^T \parallel \boldsymbol{c}^T \parallel \boldsymbol{a}^T \parallel -\boldsymbol{a}^T \parallel -\boldsymbol{c}^T \parallel \boldsymbol{a}^T \parallel -\boldsymbol{c}^T \parallel -\boldsymbol{a}^T\right)$,
$\boldsymbol{N} = \left(\boldsymbol{b}^T \parallel \boldsymbol{b}^T \parallel \boldsymbol{d}^T \parallel \boldsymbol{b}^T \parallel -\boldsymbol{b}^T \parallel -\boldsymbol{d}^T \parallel \boldsymbol{b}^T \parallel -\boldsymbol{d}^T \parallel -\boldsymbol{b}^T\right)$;

V. $\boldsymbol{M} = \left(\boldsymbol{a}^T \parallel \boldsymbol{a}^T \parallel \boldsymbol{c}^T \parallel \boldsymbol{a}^T \parallel \boldsymbol{c}^T \parallel -\boldsymbol{c}^T \parallel \boldsymbol{a}^T \parallel -\boldsymbol{c}^T \parallel -\boldsymbol{a}^T \parallel \boldsymbol{c}^T \parallel \boldsymbol{a}^T\right)$,
$\boldsymbol{N} = \left(\boldsymbol{b}^T \parallel \boldsymbol{b}^T \parallel \boldsymbol{d}^T \parallel \boldsymbol{b}^T \parallel \boldsymbol{d}^T \parallel -\boldsymbol{d}^T \parallel \boldsymbol{b}^T \parallel -\boldsymbol{d}^T \parallel -\boldsymbol{b}^T \parallel \boldsymbol{d}^T \parallel \boldsymbol{b}^T\right)$;

VI. $\boldsymbol{M} = \left(\boldsymbol{a}^T \parallel \boldsymbol{a}^T \parallel \boldsymbol{a}^T \parallel \boldsymbol{a}^T \parallel -\boldsymbol{a}^T \parallel \boldsymbol{a}^T \parallel -\boldsymbol{a}^T \parallel \boldsymbol{c}^T \parallel \boldsymbol{c}^T \parallel -\boldsymbol{c}^T \parallel -\boldsymbol{c}^T \parallel \boldsymbol{c}^T \parallel -\boldsymbol{a}^T\right)$,
$\boldsymbol{N} = \left(\boldsymbol{b}^T \parallel \boldsymbol{b}^T \parallel \boldsymbol{b}^T \parallel \boldsymbol{b}^T \parallel -\boldsymbol{b}^T \parallel -\boldsymbol{b}^T \parallel -\boldsymbol{b}^T \parallel \boldsymbol{d}^T \parallel \boldsymbol{d}^T \parallel -\boldsymbol{d}^T \parallel \boldsymbol{d}^T \parallel \boldsymbol{d}^T \parallel -\boldsymbol{b}^T\right)$.

The array pairs are $((L, 3), (Z, 2)) - \text{ZCAP}$, $((L, 5), (Z, 3)) - \text{ZCAP}$, $((L, 7), (Z, 4)) - \text{ZCAP}$, $((L, 9), (Z, 5)) - \text{ZCAP}$, $((L, 11), (Z, 6)) - \text{ZCAP}$, $((L, 13), (Z, 7)) - \text{ZCAP}$ *respectively.*

Proof. Initially, we illustrate the conclusion with Construction I as an example. For $0 \leq u_1 < Z$, consider the three cases below.

1) For $u_2 = 0$,

$$\rho(\boldsymbol{M}; u_1, 0) = 2\rho(\boldsymbol{a}; u_1) + \rho(\boldsymbol{c}; u_1), \tag{10}$$

$$\rho(\boldsymbol{N}; u_1, 0) = 2\rho(\boldsymbol{b}; u_1) + \rho(\boldsymbol{d}; u_1), \tag{11}$$

we have

$$\rho(\boldsymbol{M}; u_1, 0) + \rho(\boldsymbol{N}; u_1, 0) = 2(\rho(\boldsymbol{a}; u_1) + \rho(\boldsymbol{b}; u_1)) + \rho(\boldsymbol{c}; u_1) + \rho(\boldsymbol{d}; u_1) = 0 \tag{12}$$

2) For $u_2 = 1$,

$$\rho(\boldsymbol{M}; u_1, 1) = \rho(\boldsymbol{a}, \boldsymbol{c}; u_1) + \rho(\boldsymbol{c}, \boldsymbol{a}; u_1), \tag{13}$$

$$\rho(\boldsymbol{N}; u_1, 1) = \rho(\boldsymbol{b}, \boldsymbol{d}; u_1) + \rho(\boldsymbol{d}, \boldsymbol{b}; u_1), \tag{14}$$

Since $(\boldsymbol{a}, \boldsymbol{b})$ and $(\boldsymbol{c}, \boldsymbol{d})$ are mates to each other, we have

$$\rho(\boldsymbol{M}; u_1, 1) + \rho(\boldsymbol{N}; u_1, 1) = 0 \tag{15}$$

3) For $u_2 = 2$,

$$\rho(\boldsymbol{M}; u_1, 2) = \rho(\boldsymbol{a}; u_1), \tag{16}$$

$$\rho(\boldsymbol{N}; u_1, 2) = \rho(\boldsymbol{c}; u_1), \tag{17}$$

When $u_1 = 0$, we have

$$\rho(\boldsymbol{M}; 0, 2) + \rho(\boldsymbol{N}; 0, 2) = 2L. \tag{18}$$

From the above, it is clear that $(\boldsymbol{M}, \boldsymbol{N})$ is an $((L, 3), (Z, 2)) - \text{ZCAP}$. The proof processes of other constructions are comparable to Construction I, so we omitted them. □

Remark 1. If $(\boldsymbol{a}, \boldsymbol{b})$ is an odd-length Z-optimal ZCP, then by Definition 7 $Z = \frac{L+1}{2}$ holds. To verify the optimality of the ZCAPs, we incorporate the ZCAP parameters into the equation $Z_1 Z_2 = \left(\frac{L_1+1}{2}\right)\left(\frac{L_2+1}{2}\right)$ in Definition 8 to calculate them independently, and it can be observed that the ZCAPs produced by Theorem 1 are Z-optimal, these optimal ZCAPs are not mentioned in the previous literature. In recent years, researchers have investigated and produced abundant results on odd-length Z-optimal ZCPs [10], which facilitates the generation of odd-dimension Z-optimal ZCAPs using our methods.

Example 1. Take a Z-optimal $(3, 2) - \text{ZCP}(\boldsymbol{a}, \boldsymbol{b}) = (+++, +-+)$, then the mate of $(\boldsymbol{a}, \boldsymbol{b})$ is $(\boldsymbol{c}, \boldsymbol{d}) = (+--, ---)$. By Construction I, we can obtain that $\boldsymbol{M} = \left(\boldsymbol{a}^T \parallel \boldsymbol{c}^T \parallel \boldsymbol{a}^T\right) = \begin{pmatrix} +++ \\ +-+ \\ +++ \end{pmatrix}$ and $\boldsymbol{N} = \left(\boldsymbol{b}^T \parallel \boldsymbol{d}^T \parallel \boldsymbol{b}^T\right) = \begin{pmatrix} +-+ \\ --- \\ +-+ \end{pmatrix}$. The AACF sum of $\boldsymbol{M}$ and $\boldsymbol{N}$ is $\begin{bmatrix} 2 & 0 & 6 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 18 & 0 & 6 \\ 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 6 & 0 & 2 \end{bmatrix}$, so $(\boldsymbol{M}, \boldsymbol{N})$ is a $((3, 3), (2, 2)) - \text{ZCAP}$. Since $Z_1 Z_2 = \left(\frac{L_1+1}{2}\right)\left(\frac{L_2+1}{2}\right) = 4$, according to Definition 8, then $(\boldsymbol{M}, \boldsymbol{N})$ is an optimal ZCAP.

Theorem 2. *Let $(\boldsymbol{A}, \boldsymbol{B})$ be an $((L_1, L_2), (Z_1, Z_2)) - \text{ZCAP}$, then the two operations on $\boldsymbol{A}$ and $\boldsymbol{B}$ are performed as below.*

Construction I (Interleaving):

$$\boldsymbol{M}^1 = (\boldsymbol{A} \odot \boldsymbol{B}) = (U_{\boldsymbol{A},1} U_{\boldsymbol{B},1} U_{\boldsymbol{A},2} U_{\boldsymbol{B},2} \cdots U_{\boldsymbol{A},L_2} U_{\boldsymbol{B},L_2}), \tag{19}$$

$$\boldsymbol{N}^1 = (\boldsymbol{A} \odot (-\boldsymbol{B})) = (U_{\boldsymbol{A},1} (-U_{\boldsymbol{B},1}) U_{\boldsymbol{A},2} (-U_{\boldsymbol{B},2}) \cdots U_{\boldsymbol{A},L_2} (-U_{\boldsymbol{B},L_2})), \tag{20}$$

or

$$\boldsymbol{M}^1 = \begin{pmatrix} \boldsymbol{A} \\ \odot \\ \boldsymbol{B} \end{pmatrix} = \begin{pmatrix} V_{\boldsymbol{A},1} \\ V_{\boldsymbol{B},1} \\ V_{\boldsymbol{A},2} \\ V_{\boldsymbol{B},2} \\ \vdots \\ V_{\boldsymbol{A},L_1} \\ V_{\boldsymbol{B},L_1} \end{pmatrix}, \boldsymbol{N}^1 = \begin{pmatrix} \boldsymbol{A} \\ \odot \\ -\boldsymbol{B} \end{pmatrix} = \begin{pmatrix} V_{\boldsymbol{A},1} \\ -V_{\boldsymbol{B},1} \\ V_{\boldsymbol{A},2} \\ -V_{\boldsymbol{B},2} \\ \vdots \\ V_{\boldsymbol{A},L_1} \\ -V_{\boldsymbol{B},L_1} \end{pmatrix} \tag{21}$$

where $U_{\boldsymbol{A},r}$ and $U_{\boldsymbol{B},r}$ denote the rth column of the arrays $\boldsymbol{A}$ and $\boldsymbol{B}$, respectively, and $V_{\boldsymbol{A},r}$ and $V_{\boldsymbol{B},r}$ denote the rth row of the arrays $\boldsymbol{A}$ and $\boldsymbol{B}$, respectively, then (M^1, N^1) is the $(L_1, 2L_2), (Z_1, 2Z_2) - ZCAP$ or $(2L_1, L_2), (2Z_1, Z_2) - ZCAP$.

Construction II (Iteration):

Let $\left(\boldsymbol{M}^1, \boldsymbol{N}^1\right) = \left((\boldsymbol{A} \odot \boldsymbol{B}), (\boldsymbol{A} \odot -\boldsymbol{B})\right)$ *and* $\left(\overline{\boldsymbol{M}^1}, \overline{\boldsymbol{N}^1}\right) = \left(\begin{pmatrix} \boldsymbol{A} \\ \odot \\ \boldsymbol{B} \end{pmatrix}, \begin{pmatrix} \boldsymbol{A} \\ \odot \\ -\boldsymbol{B} \end{pmatrix}\right)$.

Take $\left(\boldsymbol{M}^1, \boldsymbol{N}^1\right)$ and $\left(\overline{\boldsymbol{M}^1}, \overline{\boldsymbol{N}^1}\right)$ as seeds for subsequent interleaving iteration operations, the interleaving iteration expressions are as follows,

$$\boldsymbol{M}^k = \boldsymbol{M}^{k-1} \odot \boldsymbol{N}^{k-1}, \boldsymbol{N}^k = \boldsymbol{M}^{k-1} \odot \left(-\boldsymbol{N}^{k-1}\right). \tag{22}$$

$$\overline{\boldsymbol{M}^k} = \left(\overline{\boldsymbol{M}^{k-1}} \odot \overline{\boldsymbol{N}^{k-1}}\right), \overline{\boldsymbol{N}^k} = \left(\overline{\boldsymbol{M}^{k-1}} \odot \overline{-\boldsymbol{N}^{k-1}}\right). \tag{23}$$

Then, $\left(\boldsymbol{M}^k, \boldsymbol{N}^k\right)$ obtained after k interleaving iterations is a $\left(\left(L_1, 2^k L_2\right), \left(Z_1, 2^k Z_2\right)\right) - ZCAP$, and $\left(\overline{\boldsymbol{M}^k}, \overline{\boldsymbol{N}^k}\right)$ is a $\left(\left(2^k L_1, L_2\right), \left(2^k Z_1, Z_2\right)\right) - ZCAP$.

Proof. For Construction I in Theorem 2, take the column interleaving method as an example, then $\boldsymbol{M}^1 = (\boldsymbol{A} \odot \boldsymbol{B}), \boldsymbol{N}^1 = (\boldsymbol{A} \odot (-\boldsymbol{B}))$, when $0 \le u_1 < L_1, 0 \le u_2 < L_2$, we can obtain the following equations.

$$\rho\left(\boldsymbol{M}^1; u_1, 2u_2\right) = \rho\left(\boldsymbol{A}; u_1, u_2\right) + \rho\left(\boldsymbol{B}; u_1, u_2\right), \tag{24}$$

$$\rho\left(\boldsymbol{N}^1; u_1, 2u_2\right) = \rho\left(\boldsymbol{A}; u_1, u_2\right) + \rho\left(\boldsymbol{B}; u_1, u_2\right), \tag{25}$$

$$\rho\left(\boldsymbol{M}^1; u_1, 2u_2 + 1\right) = \rho\left(\boldsymbol{A}, \boldsymbol{B}; u_1, u_2\right) + \rho\left(\boldsymbol{B}, \boldsymbol{A}; u_1, u_2 + 1\right), \tag{26}$$

$$\rho\left(\boldsymbol{N}^1; u_1, 2u_2 + 1\right) = -\rho\left(\boldsymbol{A}, \boldsymbol{B}; u_1, u_2\right) - \rho\left(\boldsymbol{B}, \boldsymbol{A}; u_1, u_2 + 1\right). \tag{27}$$

According to Definition 4, we can get

$$\rho\left(\boldsymbol{M}^1; u_1, 2u_2\right) + \rho\left(\boldsymbol{N}^1; u_1, 2u_2\right) = 2\left(\rho\left(\boldsymbol{A}; u_1, u_2\right) + \rho\left(\boldsymbol{B}; u_1, u_2\right)\right) = 0, \tag{28}$$

$$\rho\left(\boldsymbol{M}^1; u_1, 2u_2 + 1\right) + \rho\left(\boldsymbol{N}^1; u_1, 2u_2 + 1\right) = 0, \tag{29}$$

Let $0 < t_2 < 2Z_2$, when $0 < u_1 < Z_1, 0 < t_2 < 2Z_2$,

$$\rho\left(\boldsymbol{M}^1; u_1, t_2\right) + \rho\left(\boldsymbol{N}^1; u_1, t_2\right) = 0. \tag{30}$$

Therefore $\left(\boldsymbol{M}^1, \boldsymbol{N}^1\right)$ is $\left(\left(L_1, 2L_2\right), \left(Z_1, 2Z_2\right)\right) -$ ZCAP. The proof of the row interleaving is similar to that of the column interleaving, so it is omitted. Moreover, Construction II's proof procedure of is analogous to that of Construction I, so it is omitted. □

Figure 1: The ACCF sum of $(\boldsymbol{M}^1, \boldsymbol{N}^1)$

Figure 2: The ACCF sum of $(\boldsymbol{M}^2, \boldsymbol{N}^2)$

Example 2. $(\boldsymbol{A}, \boldsymbol{B}) = \left(\begin{pmatrix} +++ \\ +-+ \\ +++ \end{pmatrix}, \begin{pmatrix} +-+ \\ --- \\ +-+ \end{pmatrix}\right)$ is a $((3,3),(2,2)) - \text{ZCAP}$, then by Construction I, we can get $\boldsymbol{M}^1 = (\boldsymbol{A} \odot \boldsymbol{B}) = \begin{pmatrix} +++-++ \\ +---+- \\ +++-++ \end{pmatrix}$, $\boldsymbol{N}^1 = (\boldsymbol{A} \odot -\boldsymbol{B}) = \begin{pmatrix} +-++-+ \\ ++-+++ \\ +-++-+ \end{pmatrix}$. Take $\boldsymbol{M}^2 = \begin{pmatrix} \boldsymbol{M}^1 \\ \odot \\ \boldsymbol{N}^1 \end{pmatrix} = \begin{pmatrix} +++-++ \\ +-++-+ \\ +---+- \\ ++-+++ \\ +++-++ \\ +-++-+ \end{pmatrix}$, $\boldsymbol{N}^2 = \begin{pmatrix} \boldsymbol{M}^1 \\ \odot \\ -\boldsymbol{N}^1 \end{pmatrix} = \begin{pmatrix} +++-++ \\ -+--+- \\ +---+- \\ --+--- \\ +++-++ \\ -+--+- \end{pmatrix}$, the AACF sum of $\left(\boldsymbol{M}^1, \boldsymbol{N}^1\right)$ is shown in Figure 1 and the AACF sum of $\left(\boldsymbol{M}^2, \boldsymbol{N}^2\right)$ is shown in Figure 2, so $\left(\boldsymbol{M}^1, \boldsymbol{N}^1\right)$ is a $((3,6)(2,4)) - \text{ZCAP}$, $\left(\boldsymbol{M}^2, \boldsymbol{N}^2\right)$ is a $((6,6)(4,4)) - \text{ZCAP}$.

4 Constructions of Type-II ZCAPs

There are very few Type-II ZCAP constructions in the existing literature. Type-II ZCAPs were achieved by using one-dimensional Type-II ZCP for the Kronecker product and concatenation operation in [9]. However, how to obtain Type-II ZCAP with flexible size is still an open question. In this section, we first use two arbitrary arrays with the same row number to construct a class of Type-II ZCAPs by concatenation operation. Subsequently, we extend the ZCAP parameters by iteration operation.

Theorem 3. *Let A be an array of size $L \times N_1$ and B be an array of size $L \times N_2$. Perform the following concatenation operation on A and B,*

$$C^0 = A \parallel B, D^0 = A \parallel -B, \tag{31}$$

then the array pair (C^0, D^0) is a Type-II $((L, N_1 + N_2)(L, \min(N_1, N_2) + 1)) - \text{ZCAP}$.

Proof. Let us discuss the following two cases for $0 < u_1 < L$. Case 1: When $N_1 \leq N_2$, the following three intervals are discussed: For $0 < u_2 \leq N_1$, we have

$$\rho(C^0; u_1, u_2) = \rho(A; u_1, u_2) + \rho(B; u_1, u_2) + \rho(A, B; u_1, N_1 - u_2), \tag{32}$$

$$\rho(D^0; u_1, u_2) = \rho(A; u_1, u_2) + \rho(B; u_1, u_2) - \rho(A, B; u_1, N_1 - u_2), \tag{33}$$

thus,

$$\rho(C^0; u_1, u_2) + \rho(D^0; u_1, u_2) = 2\left(\rho(A; u_1, u_2) + \rho(B; u_1, u_2)\right) \tag{34}$$

For $N_1 < u_2 \leq N_2$,

$$\rho(C^0; u_1, u_2) = \rho(B; u_1, u_2) + \rho(A, B; u_1, u_2 - N_1), \tag{35}$$

$$\rho(D^0; u_1, u_2) = \rho(B; u_1, u_2) - \rho(A, B; u_1, u_2 - N_1) \tag{36}$$

then

$$\rho(C^0; u_1, u_2) + \rho(D^0; u_1, u_2) = 2\rho(B; u_1, u_2). \tag{37}$$

Figure 3: The ACCF sum of $(\boldsymbol{C}^0, \boldsymbol{D}^0)$

For $N_2 < u_2 \leq N_1 + N_2$,

$$\rho(C^0; u_1, u_2) + \rho(D^0; u_1, u_2) = \rho(A, B; u_1, u_2 - N_2) - \rho(A, B; u_1, u_2 - N_2) = 0 \tag{38}$$

To sum up, when $N_1 \leq N_2$, we have

$$\rho(C^0; u_1, u_2) + \rho(D^0; u_1, u_2) = \begin{cases} 2\left(\rho(A; u_1, u_2) + \rho(B; u_1, u_2)\right), 0 < u_2 \leq N_1, \\ 2\rho(B; u_1, u_2), N_1 < u_2 \leq N_2, \\ 0, N_2 < u_2 \leq N_1 + N_2. \end{cases} \tag{39}$$

Therefore, (C^0, D^0) is a Type- II $((L, N_1 + N_2)\,(L, N_1 + 1)) - \text{ZCAP}$.

Case 2: When $N_1 > N_2$, for $0 < u_2 \leq N_1$, we have

$$\rho(C^0; u_1, u_2) = \rho(A; u_1, u_2) + \rho(B; u_1, u_2) + \rho(A, B; u_1, N_1 - u_2) \tag{40}$$

$$\rho(D^0; u_1, u_2) = \rho(A; u_1, u_2) + \rho(B; u_1, u_2) - \rho(A, B; u_1, N_1 - u_2) \tag{41}$$

For $N_1 < u_2 \leq N_1 + N_2$,

$$\rho(C^0; u_1, u_2) + \rho(D^0; u_1, u_2) = \rho(A, B; u_1, u_2 - N_1) - \rho(A, B; u_1, u_2 - N_1) = 0. \tag{42}$$

Consequently, it is clear that when $N_1 > N_2$,

$$\rho(C^0; u_1, u_2) + \rho(D^0; u_1, u_2) = \begin{cases} 2\left(\rho(A; u_1, u_2) + \rho(B; u_1, u_2)\right), 0 < u_2 \leq N_1, \\ \\ 0, N_1 < u_2 \leq N_1 + N_2. \end{cases} \tag{43}$$

then (C^0, D^0) is an $((L, N_1 + N_2)\,(L, N_2 + 1)) - \text{ZCAP}$. From the above, it is clear that (C^0, D^0) is a Type-II $((L, N_1 + N_2)\,(L, \min(N_1, N_2) + 1)) - ZCAP$. □

Example 3. Let $A = \begin{pmatrix} +-++ \\ ++-+ \\ +++- \end{pmatrix}$ and $B = \begin{pmatrix} +- \\ +- \\ ++ \end{pmatrix}$. According to Theorem 3, we can obtain $C^0 = A \parallel B = \begin{pmatrix} +-+++- \\ ++-++- \\ +++-++ \end{pmatrix}$ and $D^0 = A \parallel -B = \begin{pmatrix} +--+-+ \\ ++-+-+ \\ +++--- \end{pmatrix}$. The AACF sum of C^0 and D^0 is shown in Figure 3, then it can be seen that (C^0, D^0) is a Type-II $((2, 5)\,(2, 3)) - \text{ZCAP}$.

Remark 2 : Since the order of the basis matrix selected by Theorem 3 is arbitrary, the parameters of the ZCAP constructed by Theorem 3 are very flexible. In fact, Theorem 3 can yield optimal Type-II odd-dimensional ZCAP. For example, when $L = 7, N_1 = 3, N_2 = 10$, an odd-dimensional Type-II $((7, 13)\,(7, 4)) - -\text{ZCAP}$ is obtained. According to Definition 9, $((7, 13)\,(7, 4)) - \text{ZCAP}$ is an optimal Type-II ZCAP. Besides, In addition, the optimal Type-II ZCAP with parameters such as Type-II $((7, 13)\,(7, 4)) - \text{ZCAP}$ and Type-II $((9, 17)\,(9, 5)) - \text{ZCAP}$ can be generated.

Theorem 4. *Using* (C^0, D^0) *obtained from Theorem 3 as the initial array, after* k *iterations, we obtain* $\left(C^k, D^k\right)$*, where*

$$C^k = C^{k-1} \parallel D^{k-1}, D^k = C^{k-1} \parallel -D^{k-1} \tag{44}$$

then $\left(C^k, D^k\right)$ *is a Type-II* $\left(L, 2^k\left(N_1+N_2\right), \left(L, 2^k\left(N_1+N_2\right) - \min\left(N_1, N_2\right)+1\right)\right)-$ZCAP*.*

Proof. This proof is akin to Theorem 3 and can be derived through mathematical induction, hence it is omitted. □

Remark 3 : The ZCZ ratio of the Type-II ZCAPs can be calculated according to Definition 7. In Theorem 4, the ZCZ ratio of the constructed ZCAP is that

$$ZCZ_{ratio} = \frac{Z_1 Z_2}{L_1 L_2} = \frac{2^k L\left(N_1+N_2\right)}{2^k L\left(N_1+N_2\right) - \min\left(N_1, N_2\right)+1} = 1 - \frac{\min\left(N_1, N_2\right)-1}{2^k\left(N_1+N_2\right)} \tag{45}$$

According to Eq. (45), when the number of iteration k is large enough, the ZCZ ratio of the Type-II ZCAPs is close 1.

5 Comparison of ZCAP parameters

Until now, the construction methods and outcomes of ZCAPs are relatively inadequate. We compare the parameters of the ZCAPs constructed in this paper with those in existing literature in Table 1. Type- I ZCAPs were directly constructed by Boolean functions in [22]-[24]. [5] and [9] provided more Type-I and Type-II ZCAPs by indirect methods. Although ZCAPs in [9] can exist all array size, many ZCZ size cannot be obtained. Table 1 indicates that the parameters of proposed ZCAPs cannot be produced by the previous constructions, such as optimal Type-I $\left(\left(3,9\right),\left(2,5\right)\right)-$ ZCAP, Type-I $\left(\left(6,6\right),\left(4,4\right)\right)-ZCAP$, Type-II $\left(\left(2,24\right)\left(2,21\right)\right)-$ ZCAP, optimal Type-II $\left(\left(7,13\right)\left(7,4\right)\right)-$ ZCAP.

6 Conclusions

In this paper, Type-I and Type-II ZCAPs with new parameters are proposed by indirect construction methods. For Type-I ZCAPs, Theorem 1 involves concatenating ZCPs to construct Type-I ZCAPs with multiple parameters, including optimal binary ZCAPs. In Theorem 2, interleaving and iteration procedures are performed on binary ZCAPs with small sizes to obtain binary ZCAPs with large sizes. For Type-II ZCAPs, we employ arbitrary two arrays and apply concatenation and iteration operations to achieve optimal Type-II ZCAPs. The outstanding advantage of the method is the absence of initial array restrictions, making the parameters of Type-II ZCAPs flexible, with the ZCZ ratio approaching 1 as the number of iterations increases.

Table 1: Comparison of ZCAPs

Ref.	ZCAP Parameters	Types of ZCAPs	ZCZ_{ratio}	Optimality (Y/N)	Methods
[22]	$\left(\begin{array}{c}\left(2^n, 2^{m-1}+\sum_{\alpha=t+1}^{m-1} d_\alpha 2^{\alpha-1}+2^v\right),\\ \left(2^n, 2^{t-1}+2^v\right)\end{array}\right)$	Type-I	$\frac{2^{t-1}+2^v}{2^{m-1}+\sum_{\alpha=t+1}^{m-1} d_\alpha 2^{\alpha-1}+2^v}$	N	Boolean function
[23]	$\left(\begin{array}{c}\left(2^{m_1-1}+2^{n+1}, 2^{m_2}+4\right),\\ \left(2^{\pi(n+1)}+2^{n+1}, 2^{m_2-2}+2^{\varphi(m_2-3)}+1\right)\end{array}\right)$	Type-I	$\frac{\left(2^{\pi(n+1)}+2^{n+1}\right)\left(2^{m_2-2}+2^{\varphi(m_2-3)}+1\right)}{\left(2^{m_1-1}+2^{n+1}\right)\left(2^{m_2}+4\right)}$	N	Boolean function
[24]	$\left(\left(14\cdot 2^{n-4}, 2^m\right), \left(12\cdot 2^{n-4}, 2^m\right)\right)$	Type-I	$6/7$	N	Boolean function
	$\left((14, 2^m), (12, 2^m)\right)$		$6/7$	N	
[5]	$\left((4, L), (4, Z)\right)$	Type-I	Z/L	N	Concatenation
	$\left((2^m, 2^n L), (2^m, Z)\right)$		$Z/2^n L$	N	
	$\left((2L_1, L_2), (L_1, Z)\right)$		$Z/2L_2$	N	Kronecker product
[9]	$\left((L_1, 2L_2), (Z_1, Z_2)\right)$	Type-I	$\frac{Z_1 Z_2}{2L_1 L_2}$	N	Kronecker product and concatenation
	$\left((L_1, 2L_2), (Z_1, 2L_2)\right)$		Z_1/L_1	N	
	$\left((L_1, 2L_2+1), (Z_1, Z_2)\right)$		$\frac{Z_1 Z_2}{L_1(2L_2+1)}$	N	
	$\left((L_1, 2L_2+1), (Z_1, L_2+1)\right)$		$\frac{Z_1(L_2+1)}{L_1(2L_2+1)}$	Y	
	$\left((L_1, 2L_2+2), (Z_1, L_2+1)\right)$		$Z_1/2L_1$	N	Concatenation
	$\left((L_1, 2L_2), (Z_1, 2Z_2)\right)$		$\frac{Z_1 Z_2}{L_1 L_2}$	N	Kronecker product and interleaving
	$\left((L_1 L_3, L_2 L_4), (Z_1, Z_2)\right)$		$\frac{Z_1 Z_2}{L_1 L_2 L_3 L_4}$	N	Kronecker product
	$\left((L_1, 2L_2), (Z_1, L_2+1)\right)$	Type-II	$\frac{Z_1(L_2+1)}{2L_1 L_2}$	N	Kronecker product and concatenation
	$\left((L_1, 2L_2), (Z_1, 2L_2)\right)$		Z_1/L_1	N	
	$\left((L_1, 2L_2+1), (Z_1, L_2+1)\right)$		$\frac{Z_1(L_2+1)}{L_1(2L_2+1)}$	N	
Thm. 1	$\left((L, 3), (Z, 2)\right)$	Type-I	$2Z/3L$	Y	Concatenation
	$\left((L, 5), (Z, 3)\right)$		$3Z/5L$		
	$\left((L, 7), (Z, 4)\right)$		$4Z/7L$		
	$\left((L, 9), (Z, 5)\right)$		$5Z/9L$		
	$\left((L, 11), (Z, 6)\right)$		$6Z/11L$		
	$\left((L, 13), (Z, 7)\right)$		$7Z/13L$		
Thm. 2	$\left(\left(L_1, 2^k L_2\right), \left(Z_1, 2^k Z_2\right)\right)$	Type-I	$\frac{Z_1 Z_2}{L_1 L_2}$	N	Interleaving and iteration
	$\left(\left(2^k L_1, L_2\right), \left(2^k Z_1, Z_2\right)\right)$		$\frac{Z_1 Z_2}{L_1 L_2}$		
Thm. 3	$\left((L, N_1+N_2), (L, \min(N_1, N_2)+1)\right)$	Type-II	$\frac{\min(N_1, N_2)+1}{N_1+N_2}$	Y	Concatenation
Thm. 4	$\left(\begin{array}{c}\left(L, 2^k(N_1+N_2)\right),\\ \left(L, 2^k(N_1+N_2)-\min(N_1, N_2)+1\right)\end{array}\right)$		$1-\frac{\min(N_1, N_2)-1}{2^k(N_1+N_2)}$	N	Iteration

References

[1] M. Golay. Transactions on Information Theory. *J. Major Results*, 7(2):82–87, 1961.

[2] P. B. Borwein and R. A. Ferguson. A complete description of Golay pairs for lengths up to 100. *J. Mathematics Of Computation*, 73(246):967–985, 2003.

[3] P. Fan, W. Yuan, and Y. Tu. Z-complementary Binary Sequences. *J. Signal Processing Letters*, 14(8):509–512, 2007.

[4] S. Matsufuji, R. Shigemitsu, Y. Tanada, and N. Kuroyanagi. : Construction of complementary arrays. *C. Joint 1st Workshop on Mobile Future and Symposium on Trends in Communications*, 78-81, 2004.

[5] C.-Y. Pai, Y.-T. Ni, Y.-C. Liu, M.-H. Kuo, and C.-Y. Chen. : Constructions of Two-Dimensional Binary Z-Complementary Array Pairs. *C. International Symposium on Information Theory*, 2264-2268, 2019.

[6] G. Weathers and E. M. Holliday. Group-Complementary Array Coding for Radar Clutter Rejection. *J. Transactions on Aerospace and Electronic Systems*, 19(3): 369-379, 1983.

[7] S. Golomb and H. Taylor. Two-dimensional synchronization patterns for minimum ambiguity. *J. Transactions on Information Theory*, 28(4): 600-604, 1982.

[8] P. Farkás, M. Turcsány, and H. Bali. : Application of 2D complete complementary orthogonal codes in 2D-MC-SS-CDMA. *C. Proceedings*, 1–5, 2004.

[9] C.-Y. Pai, Y.-T. Ni, and C.-Y. Chen. : Two-Dimensional Binary Z-Complementary Array Pairs. *J. Transactions on Information Theory*, 67(6): 3892–3904, 2021.

[10] Z. Liu, U. Parampalli, and Y. L. Guan. : Optimal Odd-Length Binary Z-Complementary Pairs. *J. Transactions on Information Theory*, 60(9): 5768–5781, 2014.

[11] A. R. Adhikary, S. Majhi, Z. Liu, and Y. L. Guan. : New Sets of Optimal Odd-Length Binary Z-Complementary Pairs. *J. Transactions on Information Theory*, 66(1): 669–678, 2020.

[12] B. Shen, Y. Yang, Z. Zhou, P. Fan, and Y. Guan. : New Optimal Binary Z-Complementary Pairs of Odd Length $2^m + 3$. *J. Signal Processing Letters*, 26(12): 1931–1934, 2019.

[13] Z. Gu, Z. Zhou, Q. Wang, and P. Fan. : New Construction of Optimal Type-II Binary Z-Complementary Pairs. *J. Transactions on Information Theory*, 67(6): 3497–3508, 2021.

[14] S.Tian, M. Yang, and J.Wang. : Two constructions of binary Z-complementary pairs. *J. Transactions on Fundamentals of Electronics, Communications, and Computer Sciences*, 104(4): 768-772, 2021.

[15] Z. Liu, U. Parampalli, and Y. L. Guan. : On Even-Period Binary Z-Complementary Pairs with Large ZCZs. *J. Signal Processing Letters*, 21(3): 284–287, 2014.

[16] A. R. Adhikary, S. Majhi, Z. Liu, and Y. L. Guan. : New Sets of Even-Length Binary Z-Complementary Pairs With Asymptotic ZCZ Ratio of 3/4. *J. Signal Processing Letters*, 25(7): 970–973, 2018.

[17] C. Xie and Y. Sun. : Constructions of Even-Period Binary Z-Complementary Pairs With Large ZCZs. *J. Signal Processing Letters*, 25(8): 1141–1145, 2018.

[18] C.-Y. Pai, S.-W. Wu, and C.-Y. Chen. : Z-Complementary Pairs With Flexible Lengths From Generalized Boolean Functions. *J. Communications Letters*, 24(6): 1183–1187, 2020.

[19] Z. Gu, Y. Yang, and Z. Zhou. : New Sets of Even-Length Binary Z-Complementary Pairs. *C. 2019 Ninth International Workshop on Signal Design and its Applications in Communications (IWSDA)*, 1-5, 2019.

[20] T. Yu, X. Du, L. Li, and Y. Yang. : Constructions of Even-Length Z-Complementary Pairs With Large Zero Correlation Zones. *J. Signal Processing Letters*, 28: 828–831, 2021.

[21] R. Kumar, P. Sarkar, P. K. Srivastava, and S. Majhi. : A Direct Construction of Asymptotically Optimal Type-II ZCP for Every Possible Even Length. *J. IEEE Signal Processing Letters*, 28: 1799–1802, 2021.

[22] C.-Y. Pai and C.-Y. Chen. : A Novel Construction of Two-Dimensional Z-Complementary Array Pairs With Large Zero Correlation Zone. *J. Signal Processing Letters*, 28: 1245–1249, 2021.

[23] A. Roy, P. Sarkar, and S. Majhi. : A Direct Construction of q-Ary 2-D Z-Complementary Array Pair Based on Generalized Boolean Functions. *J. Communications Letters*, 25(3): 706-710, 2021.

[24] H. Zhang, C. Fan, S. Mesnager. : Constructions of two-dimensional Z complementary array pairs with a large ZCZ ratio. *J. Designs, Codes and Crytography*, 90: 1221–1239, 2022.

Keynote Talk: A survey of compositional inverses of permutation polynomials over finite fields

Steven (Qiang) Wang

Carleton University, Ottawa, Canada

Abstract. In this talk we survey on the recent results and methods in the study of compositional inverses of permutation polynomials over finite fields. In particular, we describe a framework in terms of a commutative diagram which unifies several recent methods in finding the inverses of permutation polynomials.

A proof of a conjecture on trivariate permutations

Daniele Bartoli[1], Mohit Pal[2], Pantelimon Stănică[3], Tommaso Toccotelli[1]

[1] Department of Mathematics and Computer Science,
University of Perugia, 06123 Perugia, Italy;
{daniele.bartoli@unipg.it,toccotelli.tommaso@gmail.com}

[2] Department of Informatics, University of Bergen, PB 7803, N-5020,
Bergen, Norway; Mohit.Pal@uib.no

[3] Applied Mathematics Department, Naval Postgraduate School,
Monterey, CA 93943, USA; pstanica@nps.edu

Keywords: Finite fields, Permutation polynomials, Differential uniformity, varieties, irreducible components
Mathematics Subject Classification 2020: 12E20, 11T06

Abstract

In this note we show (for a large enough dimension of the underlying field) a conjecture of [C. Beierle, C. Carlet, G. Leander, L. Perrin, *A further study of quadratic APN permutations in dimension nine*, Finite Fields Appl. 81 (2022), 102049] on a trivariate permutation. This function is a global representation of two new sporadic quadratic APN permutations in dimension 9 found by [C. Beierle, G. Leander, *New instances of quadratic APN functions*, IEEE Trans. Inf. Theory 68(1) (2022), 670—678].

1 Introduction and tools from algebraic geometry

Let $q = 2^m$, $m \in \mathbb{N}$, and denote by $\mathbb{F}_q$ the finite field with q elements. For any positive integer n, we denote by $\mathbb{F}_q[X_1, \ldots, X_n]$, the ring of polynomials in n indeterminates over finite field $\mathbb{F}_q$. An element $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ is called a permutation polynomial in n variables if the equation $f(X_1, \ldots X_n) = a$ has q^{n-1} solutions in $\mathbb{F}_q^n$ for each $a \in \mathbb{F}_q$. Let $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a map given by

$$F(X_1, \ldots, X_n) = (f_1(X_1, \ldots, X_n), \ldots, f_n(X_1, \ldots, X_n)),$$

where $f_i \in \mathbb{F}_q[X_1, \ldots, X_n]$ then F is called a vectorial permutation if it induces a permutation on $\mathbb{F}_q^n$.

Vectorial Boolean functions are fundamental building blocks in symmetric cryptography, since many block ciphers employ these as components in their S-boxes. Surely, as

it is known, to counter known cipher attacks, these vectorial Boolean functions have to satisfy many criteria such as nonlinearity, avalanche features, uniformity, etc. A known measure against the differential attack is the differential uniformity, which must be low. For a prime p and positive integer $n > 0$, the differential uniformity of an (n, n)-function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is defined as the maximum number of solutions x of the differential equation $F(x + a) - F(x) = b$, where $a \neq 0, b \in \mathbb{F}_{p^n}$. In odd characteristic, there are *perfect nonlinear* (PN) functions of differential uniformity 1, while in even characteristic, the best functions are *almost perfect nonlinear* (APN) of differential uniformity 2.

As a notation, $\mathbb{P}^r(\mathbb{F}_q)$ and $\mathbb{A}^r(\mathbb{F}_q)$ (or $\mathbb{F}_q^r$) denote the projective and the affine space of dimension $r \in \mathbb{N}$ over the finite field $\mathbb{F}_q$, respectively. A variety, and more specifically a curve or a surface (i.e. a variety of dimension 1 or 2, respectively), is described by a certain set of equations with coefficients in $\mathbb{F}_q$. We say that a variety $\mathcal{V}$ is *absolutely irreducible* if there are no varieties $\mathcal{V}'$ and $\mathcal{V}''$ defined over the algebraic closure of $\mathbb{F}_q$ (denoted by $\overline{\mathbb{F}_q}$) and different from $\mathcal{V}$ such that $\mathcal{V} = \mathcal{V}' \cup \mathcal{V}''$. If a variety $\mathcal{V} \subseteq \mathbb{A}^r(\mathbb{F}_q)$ is defined by $F_i(X_1, \ldots, X_r) = 0$, for $i = 1, \ldots s$, an $\mathbb{F}_q$-rational point of $\mathcal{V}$ is a point $(x_1, \ldots, x_r) \in \mathbb{A}^r(\mathbb{F}_q)$ such that $F_i(x_1, \ldots, x_r) = 0$, for $i = 1, \ldots, s$. The set of the $\mathbb{F}_q$-rational points of $\mathcal{V}$ is usually denoted by $\mathcal{V}(\mathbb{F}_q)$. If $s = 1$, $\mathcal{V}$ is called a hypersurface and it is absolutely irreducible if the corresponding polynomial $F(X_1, \ldots, X_r)$ is absolutely irreducible, i.e. it possesses no non-trivial factors over $\overline{\mathbb{F}_q}$. Moreover, we say that $\mathcal{V}$ is a variety of degree d (and write $\deg(\mathcal{V}) = d$) if $d = \#(\mathcal{V} \cap H)$, where $H \subseteq \mathbb{A}^r(\overline{\mathbb{F}_q})$ is a general projective subspace of dimension $r - s$. To determine the degree of a variety is generally not straighforward; however an upper bound to $\deg(\mathcal{V})$ is given by $\prod_{i=1}^{s} \deg(F_i)$. We also recall that the Frobenius map $\Phi_q : x \mapsto x^q$ is an automorphism of $\mathbb{F}_{q^k}$ and generates the group $Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)$ of automorphisms of $\mathbb{F}_{q^k}$ that fixes $\mathbb{F}_q$ pointwise. The Frobenius automorphism induces also a collineation of $\mathbb{A}^r(\overline{\mathbb{F}_q})$ and an automorphism of $\overline{\mathbb{F}_q}[X_1, \ldots, X_r]$. A crucial point in our investigation of permutation trinomials over $\mathbb{F}_{q^3}$ is to prove the existence of suitable $\mathbb{F}_q$-rational points in algebraic surfaces $\mathcal{V}$ attached to each permutation trinomial. This is reached by proving the existence of absolutely irreducible $\mathbb{F}_q$-rational components in $\mathcal{V}$ and lower bounding the number of their $\mathbb{F}_q$-rational points. To this end, generalizations of Lang-Weil type bounds for algebraic varieties are needed. To ensure the existence of a suitable $\mathbb{F}_q$-rational point of $\mathcal{V}$, we need the following result.

Theorem 1. [5, Theorem 7.1] *Let $\mathcal{V} \subseteq \mathbb{A}^n(\mathbb{F}_q)$ be an absolutely irreducible variety defined over $\mathbb{F}_q$ of dimension $r > 0$ and degree δ. If $q > 2(r + 1)\delta^2$, then the following estimate holds:*

$$\left|\#(\mathcal{V}(\mathbb{A}^n(\mathbb{F}_q))) - q^r\right| \leq (\delta - 1)(\delta - 2)q^{r-1/2} + 5\delta^{13/3}q^{r-1}. \tag{1}$$

In our approach we will make use of the following result

Lemma 2. [1, Lemma 2.1] *Let $\mathcal{H}$ be a projective hypersurface and $\mathcal{X}$ a projective variety of dimension $n-1$ in $\mathbb{P}^n(\mathbb{F}_q)$. If $\mathcal{X} \cap \mathcal{H}$ has a non-repeated absolutely irreducible component defined over $\mathbb{F}_q$ then $\mathcal{X}$ has a non-repeated absolutely irreducible component defined over $\mathbb{F}_q$.*

2 Main result

Beierle and Leander [3] found two new APN permutations in dimension 9, namely

$$x \mapsto x^3 + ux^{10} + u^2x^{17} + u^4x^{80} + u^5x^{192},$$
$$x \mapsto x^3 + u^2x^{10} + ux^{24} + u^4x^{80} + u^6x^{136}.$$

In this note, we shall consider the trivariate function $C_u : \mathbb{F}_q^3 \to \mathbb{F}_q^3$ given by

$$(X, Y, Z) \mapsto (X^3 + uY^2Z, Y^3 + uXZ^2, Z^3 + uX^2Y).$$

This trivariate function is the representation of the two APN permutations in dimension 9 found by [3] mentioned above, and has been considered in [2] where the authors have shown that it is a vectorial permutation for $m = 3$ and $u \in \mathbb{F}_{2^m}\backslash\{0, 1\}$. For $m > 3$, the authors have proposed the following conjecture.

Conjecture 3 ([2])**.** Let $m > 3$ and let $u \in \mathbb{F}_{2^m}^*$. Then the function $C_u : \mathbb{F}_{2^m}^3 \to \mathbb{F}_{2^m}^3$ given by

$$(X, Y, Z) \mapsto (X^3 + uY^2Z, Y^3 + uXZ^2, Z^3 + uX^2Y)$$

is not a permutation.

It is the intent of our note to show the conjecture for m large enough.

It is easy to observe that when m is even then C_u is not a permutation as in this case $C_u(X, 0, 0) = (X^3, 0, 0)$ and the function $X \mapsto X^3$ is 3-to-1. In what follows we assume that m is odd. Note that C_u is a permutation if and only if the equation

$$C_u(X + \alpha, Y + \beta, Z + \gamma) + C_u(X, Y, Z) = 0$$

has only the trivial solutions $\{(x, y, z, 0, 0, 0) \ : \ x, y, z \in \mathbb{F}_{2^m}\}$.

Such a condition reads

$$\begin{cases} \alpha X^2 + \alpha^2 X + u\gamma Y^2 + u\beta^2 Z & = \alpha^3 + u\beta^2\gamma \\ \beta Y^2 + \beta^2 Y + u\gamma^2 X + u\alpha Z^2 & = \beta^3 + u\gamma^2\alpha \\ \gamma Z^2 + \gamma^2 Z + u\beta X^2 + u\alpha^2 Y & = \gamma^3 + u\alpha^2\beta. \end{cases} \tag{2}$$

Before we take our algebraic geometry approach, we make some observations. First, assume that only one among α, β and γ is nonzero. Without loss of generality (here because of the symmetric property of C_u), we may assume that $\alpha \neq 0$ and $\beta = \gamma = 0$. Then System (2) becomes

$$\begin{cases} \alpha X^2 + \alpha^2 X + \alpha^3 & = 0 \\ u\alpha Z^2 & = 0 \\ u\alpha^2 Y & = 0. \end{cases}$$

It is straightforward to see that the first equation of the above system has no solution $X \in \mathbb{F}_{2^m}$ as m is odd.

Next, we assume that only one among α, β and γ is zero. Again, we may assume that $\alpha, \beta \neq 0$ and $\gamma = 0$. Then System (2) becomes

$$\begin{cases} \alpha X^2 + \alpha^2 X + u\beta^2 Z &= \alpha^3 \\ \beta Y^2 + \beta^2 Y + u\alpha Z^2 &= \beta^3 \\ u\beta X^2 + u\alpha^2 Y &= u\alpha^2\beta, \end{cases} \tag{3}$$

which can be further simplified by replacing $X \mapsto \alpha X$ and $Y \mapsto \beta Y$, i.e., System (3) is equivalent to the following system

$$\begin{cases} \alpha^3(X^2 + X + 1) + u\beta^2 Z &= 0 \\ \beta^3(Y^2 + Y + 1) + u\alpha Z^2 &= 0 \\ X^2 + Y + 1 &= 0. \end{cases} \tag{4}$$

Now, squaring the first equation and putting $X^2 = Y + 1$ into it, we have

$$\alpha^6(Y^2 + Y + 1) + u^2\beta^4 Z^2 = 0.$$

Multiplying above equation by α and putting $u\alpha Z^2 = \beta^3(Y^2 + Y + 1)$, we have

$$(\alpha^7 + u\beta^7)(Y^2 + Y + 1) = 0.$$

Thus, System (4) is equivalent to the following system

$$\begin{cases} (\alpha^7 + u\beta^7)(Y^2 + Y + 1) &= 0 \\ \beta^3(Y^2 + Y + 1) + u\alpha Z^2 &= 0 \\ X^2 + Y + 1 &= 0. \end{cases}$$

Notice that if $\alpha^7 + u\beta^7 = 0$, i.e., u is a 7^{th} power then the above system has nonzero solutions $(X, Y, Z) \in \mathbb{F}_q^3$ and consequently C_u is not a permutation. When u is not a 7^{th} power then the first equation of this system has no solution $X \in \mathbb{F}_{2^m}$ for m odd. Thus, in what follows, we assume that u is not a 7^{th} power and m is odd.

Let

$$f(\alpha, \beta, X, Y, Z) := \frac{\alpha^3 + \alpha^2 X + \alpha X^2 + \beta^2 Z u}{\beta^2 u + Y^2 u},$$

$$\begin{aligned} g(\beta, X, Y, Z) := {} & \beta^{12}u^9 + \beta^{12}u^6 + \beta^{12}u^3 + \beta^{12} + \beta^9 X Z^2 u^{10} + \beta^9 X Z^2 u^4 + \beta^9 Y^3 u^9 + \beta^9 Y^3 u^3 \\ & + \beta^8 XY Z^2 u^{10} + \beta^8 XY Z^2 u^4 + \beta^8 Y^4 u^6 + \beta^8 Y^4 + \beta^6 X^2 Z^4 u^8 + \beta^6 X^2 Z^4 u^5 \\ & + \beta^6 Y^6 u^6 + \beta^6 Y^6 u^3 + \beta^5 X^7 u^8 + \beta^5 X^7 u^5 + \beta^5 XY^4 Z^2 u^{10} + \beta^5 XY^4 Z^2 u^7 \\ & + \beta^4 X^7 Y u^8 + \beta^4 X^7 Y u^5 + \beta^4 X^2 Y^2 Z^4 u^8 + \beta^4 X^2 Y^2 Z^4 u^5 + \beta^4 XY^5 Z^2 u^{10} \\ & + \beta^4 XY^5 Z^2 u^7 + \beta^4 Y^8 u^9 + \beta^4 Y^8 + \beta^3 X^7 Y^2 u^5 + \beta^3 X^4 Y^4 Z u^6 + \beta^3 X^3 Z^6 u^6 \\ & + \beta^3 X^3 Z^6 u^3 + \beta^3 X^2 Y^3 Z^4 u^5 + \beta^3 XY^6 Z^2 u^4 + \beta^3 Y^9 u^3 + \beta^3 Y^2 Z^7 u^4 \\ & + \beta^2 X^8 Z^2 u^6 + \beta^2 X^7 Y^3 u^8 + \beta^2 X^5 Y^2 Z^3 u^7 + \beta^2 X^4 Y^5 Z u^6 + \beta^2 X^3 Y Z^6 u^3 \end{aligned}$$

$$
\begin{aligned}
&+ \beta^2XY^7Z^2u^7 + \beta^2XY^7Z^2u^4 + \beta^2XZ^9u^5 + \beta^2Y^{10}u^6 + \beta^2Y^3Z^7u^4\\
&+ \beta X^7Y^4u^8 + \beta X^4Y^6Zu^6 + \beta X^3Y^2Z^6u^6 + \beta X^3Y^2Z^6u^3 + \beta X^2Y^5Z^4u^5\\
&+ \beta XY^8Z^2u^7 + \beta Y^{11}u^9 + \beta Y^4Z^7u^4,\\
h(\beta,X,Y,Z) &:= u^5(\beta+Y)^2(\beta^3X^6u^3 + \beta^3X^6 + \beta^3Y^4Z^2u^5 + \beta^3Y^4Z^2u^2 + \beta^2X^6Yu^3 + \beta^2X^6Y\\
&+ \beta^2Y^5Z^2u^5 + \beta^2Y^5Z^2u^2 + \beta X^6Y^2u^3 + \beta X^6Y^2 + \beta Y^6Z^2u^5 + \beta Y^6Z^2u^2\\
&+ X^7Z^2u + X^4Y^2Z^3u^2 + X^2YZ^6u + XY^4Z^4u^3 + Y^7Z^2u^5 + Z^9),\\
a_0(\beta,Y,Z) &:= \beta^{24}u^{21} + \beta^{24}u^{18} + \beta^{24}u^{15} + \beta^{24}u^{12} + \beta^{24}u^9 + \beta^{24}u^6 + \beta^{24}u^3 + \beta^{24}\\
&+ \beta^{21}Y^3u^{21} + \beta^{21}Y^3u^{15} + \beta^{21}Y^3u^9 + \beta^{21}Y^3u^3 + \beta^{20}Y^4u^{21} + \beta^{20}Y^4u^{15}\\
&+ \beta^{20}Y^4u^9 + \beta^{20}Y^4u^3 + \beta^{18}Y^6u^{18} + \beta^{18}Y^6u^{15} + \beta^{18}Y^6u^6 + \beta^{18}Y^6u^3\\
&+ \beta^{17}Y^7u^{21} + \beta^{17}Y^7u^{15} + \beta^{17}Y^7u^9 + \beta^{17}Y^7u^3 + \beta^{16}Y^8u^{15} + \beta^{16}Y^8u^{12}\\
&+ \beta^{16}Y^8u^3 + \beta^{16}Y^8 + \beta^{15}Y^9u^{15} + \beta^{15}Y^9u^3 + \beta^{15}Y^2Z^7u^{16} + \beta^{15}Y^2Z^7u^4\\
&+ \beta^{14}Y^{10}u^{15} + \beta^{14}Y^{10}u^3 + \beta^{14}Y^3Z^7u^{16} + \beta^{14}Y^3Z^7u^4 + \beta^{13}Y^{11}u^{15}\\
&+ \beta^{13}Y^{11}u^3 + \beta^{13}Y^4Z^7u^{16} + \beta^{13}Y^4Z^7u^4 + \beta^{12}Y^{12}u^{15} + \beta^{12}Y^{12}u^{12}\\
&+ \beta^{12}Y^{12}u^9 + \beta^{12}Y^{12}u^6 + \beta^{11}Y^{13}u^{15} + \beta^{11}Y^{13}u^3 + \beta^{11}Y^6Z^7u^{16}\\
&+ \beta^{11}Y^6Z^7u^4 + \beta^{10}Y^{14}u^{15} + \beta^{10}Y^{14}u^3 + \beta^{10}Y^7Z^7u^{16} + \beta^{10}Y^7Z^7u^4\\
&+ \beta^9Y^{15}u^{15} + \beta^9Y^{15}u^9 + \beta^9Y^8Z^7u^{22} + \beta^9Y^8Z^7u^4 + \beta^8Y^{16}u^{21} + \beta^8Y^{16}u^{18}\\
&+ \beta^8Y^{16}u^9 + \beta^8Y^{16} + \beta^8Y^9Z^7u^{22} + \beta^8Y^9Z^7u^{16} + \beta^7Y^{17}u^{15} + \beta^7Y^{17}u^3\\
&+ \beta^7Y^{10}Z^7u^{16} + \beta^7Y^{10}Z^7u^4 + \beta^6Y^{18}u^{15} + \beta^6Y^{18}u^6 + \beta^6Y^{11}Z^7u^{22}\\
&+ \beta^6Y^{11}Z^7u^4 + \beta^6Y^4Z^{14}u^{11} + \beta^6Y^4Z^{14}u^8 + \beta^5Y^{19}u^{21} + \beta^5Y^{19}u^9\\
&+ \beta^5Y^{12}Z^7u^{16} + \beta^5Y^{12}Z^7u^4 + \beta^4Y^{20}u^{21} + \beta^4Y^{20}u^{12} + \beta^4Y^{13}Z^7u^{22}\\
&+ \beta^4Y^{13}Z^7u^{16} + \beta^4Y^6Z^{14}u^{11} + \beta^4Y^6Z^{14}u^8 + \beta^3Y^{21}u^{15} + \beta^3Y^{14}Z^7u^{16}\\
&+ \beta^3Y^7Z^{14}u^{11} + \beta^3Z^{21}u^{12} + \beta^2Y^{22}u^{18} + \beta^2Y^{15}Z^7u^{22} + \beta^2Y^8Z^{14}u^8\\
&+ \beta^2YZ^{21}u^{12} + \beta Y^{23}u^{21} + \beta Y^{16}Z^7u^{22} + \beta Y^9Z^{14}u^{11} + \beta Y^2Z^{21}u^{12},\\
a_1(\beta,Y,Z) &:= \beta^{21}Z^2u^{19} + \beta^{21}Z^2u^{13} + \beta^{21}Z^2u^7 + \beta^{21}Z^2u + \beta^{20}YZ^2u^{19} + \beta^{20}YZ^2u^{13}\\
&+ \beta^{20}YZ^2u^7 + \beta^{20}YZ^2u + \beta^{18}Y^3Z^2u^{19} + \beta^{18}Y^3Z^2u^{13} + \beta^{18}Y^3Z^2u^7\\
&+ \beta^{18}Y^3Z^2u + \beta^{17}Y^4Z^2u^{19} + \beta^{17}Y^4Z^2u^{13} + \beta^{17}Y^4Z^2u^7 + \beta^{17}Y^4Z^2u\\
&+ \beta^{15}Y^6Z^2u^{13} + \beta^{15}Y^6Z^2u + \beta^{14}Y^7Z^2u^{13} + \beta^{14}Y^7Z^2u + \beta^{13}Y^8Z^2u^{13}\\
&+ \beta^{13}Y^8Z^2u + \beta^{11}Y^{10}Z^2u^{13} + \beta^{11}Y^{10}Z^2u + \beta^{10}Y^{11}Z^2u^{13} + \beta^{10}Y^{11}Z^2u\\
&+ \beta^9Y^{12}Z^2u^{13} + \beta^9Y^{12}Z^2u^7 + \beta^8Y^{13}Z^2u^7 + \beta^8Y^{13}Z^2u + \beta^7Y^{14}Z^2u^{13}\\
&+ \beta^7Y^{14}Z^2u + \beta^6Y^{15}Z^2u^{13} + \beta^6Y^{15}Z^2u^7 + \beta^5Y^{16}Z^2u^{19} + \beta^5Y^{16}Z^2u^7\\
&+ \beta^4Y^{17}Z^2u^{19} + \beta^4Y^{17}Z^2u^{13} + \beta^3Y^{18}Z^2u^{13} + \beta^3Y^4Z^{16}u^9 + \beta^2Y^{19}Z^2u^{19}\\
&+ \beta^2Y^5Z^{16}u^9 + \beta Y^{20}Z^2u^{19} + \beta Y^6Z^{16}u^9,\\
a_2(\beta,Y,Z) &:= \beta^{18}Z^4u^{23} + \beta^{18}Z^4u^{20} + \beta^{18}Z^4u^{11} + \beta^{18}Z^4u^8 + \beta^{16}Y^2Z^4u^{23}\\
&+ \beta^{16}Y^2Z^4u^{20} + \beta^{16}Y^2Z^4u^{11} + \beta^{16}Y^2Z^4u^8 + \beta^{15}Y^3Z^4u^{23} + \beta^{15}Y^3Z^4u^{11}\\
&+ \beta^{14}Y^4Z^4u^{23} + \beta^{14}Y^4Z^4u^{11} + \beta^{13}Y^5Z^4u^{23} + \beta^{13}Y^5Z^4u^{11} + \beta^{11}Y^7Z^4u^{23}\\
&+ \beta^{11}Y^7Z^4u^{11} + \beta^{10}Y^8Z^4u^{23} + \beta^{10}Y^8Z^4u^{11} + \beta^9Y^9Z^4u^{23} + \beta^9Y^9Z^4u^{17}
\end{aligned}
$$

$$
\begin{aligned}
&+ \beta^9Y^2Z^{11}u^{18} + \beta^9Y^2Z^{11}u^6 + \beta^8Y^{10}Z^4u^{17} + \beta^8Y^{10}Z^4u^{11} + \beta^8Y^3Z^{11}u^{18}\\
&+ \beta^8Y^3Z^{11}u^6 + \beta^7Y^{11}Z^4u^{23} + \beta^7Y^{11}Z^4u^{11} + \beta^6Y^{12}Z^4u^{23} + \beta^6Y^{12}Z^4u^{17}\\
&+ \beta^6Y^{12}Z^4u^{11} + \beta^6Y^{12}Z^4u^8 + \beta^6Y^5Z^{11}u^{18} + \beta^6Y^5Z^{11}u^6 + \beta^5Y^{13}Z^4u^{23}\\
&+ \beta^5Y^{13}Z^4u^{11} + \beta^4Y^{14}Z^4u^{17} + \beta^4Y^{14}Z^4u^8 + \beta^4Y^7Z^{11}u^{18} + \beta^4Y^7Z^{11}u^6\\
&+ \beta^3Y^{15}Z^4u^{23} + \beta^3Y^{15}Z^4u^{11} + \beta^3Y^8Z^{11}u^6 + \beta^3YZ^{18}u^{13} + \beta^2Y^{16}Z^4u^{20}\\
&+ \beta^2Y^{16}Z^4u^{17} + \beta^2Y^9Z^{11}u^{18} + \beta^2Y^2Z^{18}u^{13} + \beta Y^{17}Z^4u^{23} + \beta Y^{17}Z^4u^{17}\\
&+ \beta Y^{10}Z^{11}u^{18} + \beta Y^3Z^{18}u^{13} + Y^{18}Z^4u^{23} + Y^{18}Z^4u^{20} + Y^4Z^{18}u^{13} + Y^4Z^{18}u^{10},\\
a_3(\beta,Y,Z) &:= \beta^{15}Z^6u^{21} + \beta^{15}Z^6u^{15} + \beta^{15}Z^6u^9 + \beta^{15}Z^6u^3 + \beta^{14}YZ^6u^{21} + \beta^{14}YZ^6u^{15}\\
&+ \beta^{14}YZ^6u^9 + \beta^{14}YZ^6u^3 + \beta^{13}Y^2Z^6u^{21} + \beta^{13}Y^2Z^6u^{15} + \beta^{13}Y^2Z^6u^9\\
&+ \beta^{13}Y^2Z^6u^3 + \beta^{11}Y^4Z^6u^{21} + \beta^{11}Y^4Z^6u^{15} + \beta^{11}Y^4Z^6u^9 + \beta^{11}Y^4Z^6u^3\\
&+ \beta^{10}Y^5Z^6u^{21} + \beta^{10}Y^5Z^6u^{15} + \beta^{10}Y^5Z^6u^9 + \beta^{10}Y^5Z^6u^3 + \beta^9Y^6Z^6u^{15}\\
&+ \beta^9Y^6Z^6u^3 + \beta^8Y^7Z^6u^{21} + \beta^8Y^7Z^6u^9 + \beta^7Y^8Z^6u^{21} + \beta^7Y^8Z^6u^{15} + \beta^7Y^8Z^6u^9\\
&+ \beta^7Y^8Z^6u^3 + \beta^6Y^9Z^6u^{15} + \beta^6Y^9Z^6u^3 + \beta^5Y^{10}Z^6u^{21} + \beta^5Y^{10}Z^6u^{15}\\
&+ \beta^5Y^{10}Z^6u^9 + \beta^5Y^{10}Z^6u^3 + \beta^4Y^{11}Z^6u^{21} + \beta^4Y^{11}Z^6u^9 + \beta^3Y^{12}Z^6u^{21}\\
&+ \beta^3Y^{12}Z^6u^{15} + \beta^3Y^{12}Z^6u^9 + \beta^2Y^{13}Z^6u^{15} + \beta Y^{14}Z^6u^{15},\\
a_4(\beta,Y,Z) &:= \beta^{15}Y^4Zu^{18} + \beta^{15}Y^4Zu^6 + \beta^{14}Y^5Zu^{18} + \beta^{14}Y^5Zu^6 + \beta^{13}Y^6Zu^{18}\\
&+ \beta^{13}Y^6Zu^6 + \beta^{12}Z^8u^{19} + \beta^{12}Z^8u^{16} + \beta^{12}Z^8u^{13} + \beta^{12}Z^8u^{10}\\
&+ \beta^{11}Y^8Zu^{18} + \beta^{11}Y^8Zu^6 + \beta^{10}Y^9Zu^{18} + \beta^{10}Y^9Zu^6 + \beta^9Y^{10}Zu^{18}\\
&+ \beta^9Y^{10}Zu^6 + \beta^9Y^3Z^8u^{19} + \beta^9Y^3Z^8u^{13} + \beta^8Y^4Z^8u^{16} + \beta^8Y^4Z^8u^{10}\\
&+ \beta^7Y^{12}Zu^{18} + \beta^7Y^{12}Zu^6 + \beta^6Y^{13}Zu^{18} + \beta^6Y^{13}Zu^6 + \beta^6Y^6Z^8u^{19}\\
&+ \beta^6Y^6Z^8u^{10} + \beta^5Y^{14}Zu^{18} + \beta^5Y^{14}Zu^6 + \beta^4Y^8Z^8u^{16} + \beta^4Y^8Z^8u^{13}\\
&+ \beta^3Y^{16}Zu^{18} + \beta^3Y^2Z^{15}u^{14} + \beta^3Y^2Z^{15}u^8 + \beta^2Y^{17}Zu^{18} + \beta^2Y^{10}Z^8u^{19}\\
&+ \beta^2Y^{10}Z^8u^{10} + \beta^2Y^3Z^{15}u^{14} + \beta^2Y^3Z^{15}u^8 + \beta Y^{18}Zu^{18} + \beta Y^{11}Z^8u^{19}\\
&+ \beta Y^{11}Z^8u^{13} + \beta Y^4Z^{15}u^{14} + \beta Y^4Z^{15}u^8 + Y^{12}Z^8u^{19} + Y^{12}Z^8u^{16},\\
a_5(\beta,Y,Z) &:= \beta^9Z^{10}u^{11} + \beta^9Z^{10}u^5 + \beta^8YZ^{10}u^{11} + \beta^8YZ^{10}u^5 + \beta^6Y^3Z^{10}u^{11}\\
&+ \beta^6Y^3Z^{10}u^5 + \beta^4Y^5Z^{10}u^{11} + \beta^4Y^5Z^{10}u^5 + \beta^3Y^6Z^{10}u^5 + \beta^2Y^7Z^{10}u^{11}\\
&+ \beta Y^8Z^{10}u^{11}\\
a_6(\beta,Y,Z) &:= \beta^9Y^4Z^5u^{20} + \beta^9Y^4Z^5u^8 + \beta^8Y^5Z^5u^{20} + \beta^8Y^5Z^5u^8 + \beta^6Y^7Z^5u^{20}\\
&+ \beta^6Y^7Z^5u^8 + \beta^6Z^{12}u^{15} + \beta^6Z^{12}u^{12} + \beta^6Z^{12}u^9 + \beta^6Z^{12}u^6 + \beta^4Y^9Z^5u^{20}\\
&+ \beta^4Y^9Z^5u^8 + \beta^4Y^2Z^{12}u^{15} + \beta^4Y^2Z^{12}u^{12} + \beta^4Y^2Z^{12}u^9 + \beta^4Y^2Z^{12}u^6\\
&+ \beta^3Y^{10}Z^5u^8 + \beta^3Y^3Z^{12}u^9 + \beta^2Y^{11}Z^5u^{20} + \beta^2Y^4Z^{12}u^{15} + \beta^2Y^4Z^{12}u^{12}\\
&+ \beta^2Y^4Z^{12}u^6 + \beta Y^{12}Z^5u^{20} + \beta Y^5Z^{12}u^9 + Y^6Z^{12}u^{15} + Y^6Z^{12}u^{12},\\
a_7(\beta,Y,Z) &:= \beta^{15}Y^2u^{17} + \beta^{15}Y^2u^5 + \beta^{14}Y^3u^{17} + \beta^{14}Y^3u^5 + \beta^{13}Y^4u^{17} + \beta^{13}Y^4u^5\\
&+ \beta^{11}Y^6u^{17} + \beta^{11}Y^6u^5 + \beta^{10}Y^7u^{17} + \beta^{10}Y^7u^5 + \beta^9Y^8u^{17} + \beta^9Y^8u^5\\
&+ \beta^7Y^{10}u^{17} + \beta^7Y^{10}u^5 + \beta^6Y^{11}u^{17} + \beta^6Y^{11}u^5 + \beta^5Y^{12}u^{17} + \beta^5Y^{12}u^5\\
&+ \beta^3Y^{14}u^{17} + \beta^3Z^{14}u^{13} + \beta^2Y^{15}u^{17} + \beta^2YZ^{14}u^{13} + \beta Y^{16}u^{17}
\end{aligned}
$$

$$
\begin{aligned}
&+ \beta Y^2 Z^{14} u^{13},\\
a_8(\beta, Y, Z) &:= \beta^6 Y^8 Z^2 u^{15} + \beta^6 Y^8 Z^2 u^{12} + \beta^4 Y^{10} Z^2 u^{15} + \beta^4 Y^{10} Z^2 u^{12} + \beta^3 Y^{11} Z^2 u^{15}\\
&+ \beta^3 Y^4 Z^9 u^{16} + \beta^3 Y^4 Z^9 u^{10} + \beta^2 Y^{12} Z^2 u^{12} + \beta^2 Y^5 Z^9 u^{16} + \beta^2 Y^5 Z^9 u^{10}\\
&+ \beta Y^{13} Z^2 u^{15} + \beta Y^6 Z^9 u^{16} + \beta Y^6 Z^9 u^{10},\\
a_9(\beta, Y, Z) &:= \beta^9 Y^2 Z^4 u^{19} + \beta^9 Y^2 Z^4 u^7 + \beta^8 Y^3 Z^4 u^{19} + \beta^8 Y^3 Z^4 u^7 + \beta^6 Y^5 Z^4 u^{19}\\
&+ \beta^6 Y^5 Z^4 u^7 + \beta^4 Y^7 Z^4 u^{19} + \beta^4 Y^7 Z^4 u^7 + \beta^3 Y^8 Z^4 u^{13} + \beta^3 Y^8 Z^4 u^7\\
&+ \beta^2 Y^9 Z^4 u^{19} + \beta^2 Y^9 Z^4 u^{13} + \beta Y^{10} Z^4 u^{19} + \beta Y^{10} Z^4 u^{13},\\
a_{10}(\beta, Y, Z) &:= \beta^3 Y^5 Z^6 u^{17} + \beta^2 Y^6 Z^6 u^{17} + \beta Y^7 Z^6 u^{17} + Y^8 Z^6 u^{17} + Y^8 Z^6 u^{14},\\
a_{11}(\beta, Y, Z) &:= \beta^3 Y^2 Z^8 u^9 + \beta^2 Y^3 Z^8 u^9 + \beta Y^4 Z^8 u^9,\\
a_{12}(\beta, Y, Z) &:= \beta^9 Z^3 u^{18} + \beta^9 Z^3 u^{12} + \beta^8 Y Z^3 u^{18} + \beta^8 Y Z^3 u^{12} + \beta^6 Y^3 Z^3 u^{18} + \beta^6 Y^3 Z^3 u^{12}\\
&+ \beta^4 Y^5 Z^3 u^{18} + \beta^4 Y^5 Z^3 u^{12} + \beta^3 Y^6 Z^3 u^{18} + \beta^2 Y^7 Z^3 u^{12} + \beta Y^8 Z^3 u^{12},\\
a_{13}(\beta, Y, Z) &:= 0,\\
a_{14}(\beta, Y, Z) &:= \beta^9 Y u^{19} + \beta^9 Y u^{13} + \beta^8 Y^2 u^{19} + \beta^8 Y^2 u^{13} + \beta^6 Y^4 u^{19} + \beta^6 Y^4 u^{10}\\
&+ \beta^4 Y^6 u^{19} + \beta^4 Y^6 u^{10} + \beta^3 Y^7 u^{13} + \beta^3 Z^7 u^{14} + \beta^2 Y^8 u^{19} + \beta^2 Y^8 u^{13}\\
&+ \beta^2 Y^8 u^{10} + \beta^2 Y Z^7 u^{14} + \beta Y^9 u^{19} + \beta Y^2 Z^7 u^{14},\\
a_{15}(\beta, Y, Z) &:= \beta^3 Y^4 Z^2 u^{17} + \beta^3 Y^4 Z^2 u^{11} + \beta^2 Y^5 Z^2 u^{17} + \beta^2 Y^5 Z^2 u^{11} + \beta Y^6 Z^2 u^{17} + \beta Y^6 Z^2 u^{11},\\
a_{16}(\beta, Y, Z) &:= \beta^3 Y Z^4 u^{15} + \beta^2 Y^2 Z^4 u^{15} + \beta Y^3 Z^4 u^{15} + Y^4 Z^4 u^{15} + Y^4 Z^4 u^{12},\\
a_{17}(\beta, Y, Z) &:= 0,\\
a_{18}(\beta, Y, Z) &:= \beta^3 Y^2 Z u^{16} + \beta^2 Y^3 Z u^{16} + \beta Y^4 Z u^{16},\\
a_{19}(\beta, Y, Z) &:= 0,\\
a_{20}(\beta, Y, Z) &:= 0,\\
a_{21}(\beta, Y, Z) &:= \beta^3 u^{15} + \beta^2 Y u^{15} + \beta Y^2 u^{15}.
\end{aligned}
$$

Proposition 4. *Each element of*

$$
\begin{aligned}
\Theta := \quad \{(x, y, z, a, b, c) \in \mathbb{F}_q^6 : (b + y)h(b, x, y, z) \neq 0,\ & c = f(a, b, x, y, z),\\
& a = g(b, x, y, z)/h(b, x, y, z), \textstyle\sum_{i=0}^{21} a_i(b, y, z)x^i = 0\}
\end{aligned}
$$

is a solution of System (2)*.*

Proof. This is easily checked via direct computations in MAGMA [4]. □

Proposition 5. *Let* $\mathcal{V} \subset \mathbb{A}^6(\mathbb{F}_q)$ *be the variety defined by*

$$
\begin{cases}
X_3 = f(X_1, X_2, X_4, X_5, X_6)\\
X_1 = g(X_2, X_4, X_5, X_6)/h(X_2, X_4, X_5, X_6)\\
\sum_{i=0}^{21} a_i(X_2, X_5, X_6)X_4^i = 0.
\end{cases}
$$

Then $\mathcal{V}$ *contains an absolutely irreducible component defined over* $\mathbb{F}_q$*, distinct from* $X_1 = X_2 = X_3 = 0$*, of degree at most* 27*, and not contained in* $(X_2 + X_5)h(X_2, X_4, X_5, X_6) = 0$*.*

Proof. Since $\sum_{i=0}^{21} a_i(X_2, X_5, X_6)X_4^i$ is a homogeneous polynomial of degree 24 it defines a surface $\mathcal{S}$ in $\mathbb{P}^3(\mathbb{F}_q)$. First note that X_2 is not a factor of $\sum_{i=0}^{21} a_i(X_2, X_5, X_6)X_4^i$, otherwise $u \in \mathbb{F}_4$, a contradiction. Also, $\mathcal{S}$ contains an absolutely irreducible component defined over $\mathbb{F}_q$, since its intersection with the plane $X_4 = 0$ is

$$a_{21}(X_2, X_5, X_6) = u^{15}X_2(X_2^2 + X_2X_5 + X_5^2) = 0$$

and by Lemma 2 there exists an absolutely irreducible component $\mathcal{S}'$ defined over $\mathbb{F}_q$ whose intersection with $X_4 = 0$ is $X_2 = 0$. Since the intersection between $(X_2 + X_5)h(X_2, X_4, X_5, X_6) = 0$ and $X_2 = 0$ is

$$u^5X_6^2(X_2 + X_5)^2((u^2 + u^5)X_2^3X_5^4 + (u^2 + u^5)X_2^2X_5^5 + (u^2 + u^5)X_2X_5^6 + u^5X_5^7 + X_6^7) = 0,$$

$\mathcal{S}'$ cannot be contained in $(X_2 + X_5)h(X_2, X_4, X_5, X_6) = 0$.

Clearly, $\mathcal{S}'$ extends to a variety $\mathcal{V}'$ contained in $\mathcal{V}$, absolutely irreducible and $\mathbb{F}_q$-rational (by considering the two extra equations $X_3 = f(X_1, X_2, X_4, X_5, X_6)$ and $X_1 = g(X_2, X_4, X_5, X_6)/h(X_2, X_4, X_5, X_6)$). Since $\mathcal{S}'$ is different from $X_2 = 0$, $\mathcal{V}'$ is different from $X_1 = X_2 = X_3 = 0$. The degree of $\mathcal{V}'$ is upper bounded by the degree of $\mathcal{V}$, that is at most $3^3 = 27$. □

The following is the main achievement of our paper.

Theorem 6. *If m is large enough, Conjecture 3 is true.*

Proof. By Proposition 5 and Theorem 1, if m is large enough, the absolutely irreducible $\mathbb{F}_q$-rational component $\mathcal{V}'$ (and thus $\mathcal{V}$) possesses roughly q^3 of $\mathbb{F}_q$-rational points. Since $\mathcal{V}'$ is not $X_1 = X_2 = X_3 = 0$ and it not contained in $(X_2 + X_5)h(X_2, X_4, X_5, X_6) = 0$, the set Θ is not empty and the claim follows. □

Remark 7. Using Theorem 1 it is possible to give a more accurate estimate for the minimum integer m that confirms the conjecture. First, notice that points of $\mathcal{V}'$ not belonging to $(X_2 + X_5)h(X_2, X_4, X_5, X_6) = 0$ correspond to quadruples $(x_2, x_4, x_5, x_6) \in \mathbb{F}_q^4$ such that $\sum_{i=0}^{21} a_i(x_2, x_4, x_5)x_4^i = 0$ and $(x_2 + x_5)h(x_2, x_4, x_5, x_6) \neq 0$. It can be easily verified that the intersections of $\mathcal{S}$ and $(X_2 + X_5)h(X_2, X_4, X_5, X_6) = 0$ with $X_4 = 0$ are coprime: this shows that they do not share any component. Also, since the degree of these surfaces is 24 and 12 respectively, their intersection is a projective space curve of degree 288 and it contains at most $288q$ projective $\mathbb{F}_q$-rational points; see [6]. This shows the existence of at most $288q(q-1)$ nonzero quadruples $(x_1, x_2, x_3, x_4) \in \mathbb{F}_q^4$ such that $\sum_{i=0}^{21} a_i(x_2, x_4, x_5)x_4^i = 0$ and $(x_2+x_5)h(x_2, x_4, x_5, x_6) = 0$. Arguing similarly, there are at most $24q(q-1)$ nonzero quadruples $(x_1, x_2, x_3, x_4) \in \mathbb{F}_q^4$ satisfying $\sum_{i=0}^{21} a_i(x_2, x_4, x_5)x_4^i = 0$ and $x_2 = 0$ (and thus lying on $X_1 = X_2 = X_3 = 0$). By Theorem 1 the number of $\mathbb{F}_q$-rational points in Θ is at least

$$q^3 - 25 \cdot 26 \cdot q^{5/2} - 5 \cdot (27)^{13/3}q^2 - 312q(q-1),$$

that is larger than 0 when $m \geq 25$ and thus Conjecture 3 holds true.

References

[1] Y. Aubry, G. McGuire, F. Rodier, *A few more functions that are not APN infinitely often*, In Finite fields: theory and applications, vol. 518 of Contemp. Math. Amer. Math. Soc., Providence, RI, 2010, pp. 23–31.

[2] C. Beierle, C. Carlet, G. Leander, L. Perrin, *A further study of quadratic APN permutations in dimension nine*, Finite Fields Appl. 81 (2022), 102049.

[3] C. Beierle, G. Leander, *New instances of quadratic APN functions*, IEEE Trans. Inf. Theory 68(1) (2022), 670—678.

[4] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24(3-4) (1993), 235–265.

[5] A. Cafure, G. Matera, *Improved explicit estimates on the number of solutions of equations over a finite field*, Finite Fields Appl. 12, 2 (2006), 155–185.

[6] M. Homma, *A bound on the number of points of a curve in projective space over a finite field*, Theory and Applications of Finite Fields in: Contemp. Mat. 579, 103–110 (2012).

On the bijectivity of the map χ

Anna-Maurin Graner Björn Kriepke
Lucas Krompholz Gohar M. Kyureghyan
Institute of Mathematics
University of Rostock
Germany
{anna-maurin.graner,bjoern.kriepke,lucas.krompholz,gohar.kyureghyan}@uni-rostock.de

Abstract

We prove that for $n > 1$ the map $\chi : \mathbb{F}_q^n \to \mathbb{F}_q^n$, defined by $y = \chi(x)$ with $y_i = x_i + x_{i+2} \cdot (1 + x_{i+1})$ for $1 \leq i \leq n$, is bijective if and only if $q = 2$ and n is odd, as it was conjectured in [8].

1 Introduction

Let q be any prime power and n a positive integer. Several cryptographic primitives, including ASCON [4] and SHA-3 [6], use the map $\chi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ given by $y = \chi(x)$ with

$$y_i = x_i + x_{i+2} \cdot (1 + x_{i+1})$$

for $1 \leq i \leq n$, where the indices are computed modulo n. Let the symbol $\odot$ denote the element wise multiplication of two vectors (also known as the Hadamard product), i.e., $z = x \odot y$ with $z_i = x_i \cdot y_i$ for all $i = 1, \ldots, n$. Further, denote by S the cyclic left shift operator on $\mathbb{F}_q^n$, that is $\mathrm{S}(x_1, \ldots, x_n) = (x_2, \ldots, x_n, x_1)$. Let S^j denote the j-th iterate of S for $j \geq 0$. Note that S^0 is the identity map. Then χ can also be written as

$$\chi(x) = x + \mathrm{S}(x) \odot \mathrm{S}^2(x) + \mathrm{S}^2(x).$$

It is known that $\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is bijective if and only if n is odd [2]. Some partial results are proved about bijectivity of χ for $q \neq 2$. In [8] it was shown that for $k \geq 1$ the map χ is not a permutation, when

- q is odd,
- $q = 2^k$ and n is even,
- $q = 2^{2k}$ and $n > 1$ is odd,
- $q = 2^{3k}$ and $n > 1$ is odd.

In [7] the following additional parameters were ruled out using an approach based on Gröbner basis:

- $q = 2^{5k}$ or $q = 2^{7k}$ and n is a multiple of 3 or 5.

It was conjectured in [8] that χ is not a permutation in all other cases except when $q = 2$ and n odd. We confirm this conjecture using linear algebra methods. More precisely, we prove in Lemmas 3 to 5 that the following result holds:

Theorem 1. *For $q = 2$ the map χ is a permutation if and only if n is odd. For any prime power $q > 2$, the map $\chi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is a permutation if and only if q is even and $n = 1$.*

We conclude our note with a short proof for the rank of the linear part of $\chi(x+a)+\chi(x)$, which appears in the study of the differential properties of the map $\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n$.

2 Deriving the linear system

The map χ is not a permutation if and only if there exist vectors $a, x \in \mathbb{F}_q^n$ with $a \neq 0$ such that

$$\chi(x + a) - \chi(x) = 0. \tag{1}$$

Note that for any j the map S^j is linear over $\mathbb{F}_q$. Furthermore, the Hadamard product is commutative and distributive with respect to addition, i.e. $x \odot y = y \odot x$ and $x \odot (y+z) = x \odot y + x \odot z$ for all $x, y, z \in \mathbb{F}_q^n$. Moreover, we have $\mathrm{S}^j(x \odot y) = \mathrm{S}^j(x) \odot \mathrm{S}^j(y)$. Using these properties, we obtain

$$\begin{aligned}
\chi(x + a) &= x + a + \mathrm{S}(x + a) \odot \mathrm{S}^2(x + a) + \mathrm{S}^2(x + a) \\
&= x + a + [\mathrm{S}(x) + \mathrm{S}(a)] \odot [\mathrm{S}^2(x) + \mathrm{S}^2(a)] + \mathrm{S}^2(x) + \mathrm{S}^2(a) \\
&= x + a + \mathrm{S}(x) \odot \mathrm{S}^2(x) + \mathrm{S}(x) \odot \mathrm{S}^2(a) + \mathrm{S}(a) \odot \mathrm{S}^2(x) + \mathrm{S}(a) \odot \mathrm{S}^2(a) + \mathrm{S}^2(x) + \mathrm{S}^2(a) \\
&= \chi(x) + a + \mathrm{S}(x) \odot \mathrm{S}^2(a) + \mathrm{S}(a) \odot \mathrm{S}^2(x) + \mathrm{S}(a) \odot \mathrm{S}^2(a) + \mathrm{S}^2(a)
\end{aligned}$$

and therefore

$$\chi(x + a) - \chi(x) = a + \mathrm{S}^2(a) + \mathrm{S}(a \odot \mathrm{S}(x) + x \odot \mathrm{S}(a) + a \odot \mathrm{S}(a)).$$

For a fixed $a \in \mathbb{F}_q^n \setminus \{0\}$, the equation $\chi(x + a) - \chi(x) = 0$ has a solution x if and only if

$$-a - \mathrm{S}^2(a) = \mathrm{S}(a \odot \mathrm{S}(x) + x \odot \mathrm{S}(a) + a \odot \mathrm{S}(a))$$

has a solution, which, by applying S^{-1} on both sides, is equivalent to

$$-\mathrm{S}^{-1}(a) - \mathrm{S}(a) - a \odot \mathrm{S}(a) = a \odot \mathrm{S}(x) + x \odot \mathrm{S}(a). \tag{2}$$

The right-hand side of (2) is a linear map in x and hence it reduces to a system of linear equations over $\mathbb{F}_q$. We represent this system of equations using matrices:

$$\begin{pmatrix} a_2 & a_1 & & & & & \\ & a_3 & a_2 & & & & \\ & & a_4 & a_3 & & & \\ & & & \ddots & \ddots & & \\ & & & & a_{n-1} & a_{n-2} & \\ & & & & & a_n & a_{n-1} \\ a_n & & & & & & a_1 \end{pmatrix} \cdot x = - \begin{pmatrix} a_1a_2 + a_2 + a_n \\ a_2a_3 + a_3 + a_1 \\ a_3a_4 + a_4 + a_2 \\ \vdots \\ a_{n-2}a_{n-1} + a_{n-1} + a_{n-3} \\ a_{n-1}a_n + a_n + a_{n-2} \\ a_na_1 + a_1 + a_{n-1} \end{pmatrix}, \tag{3}$$

where $a = (a_1, \ldots, a_n)$. We denote the coefficient matrix in (3) by $A(a)$ and the vector in its right-hand side by $b(a)$. We abbreviate $A(a) \cdot x = b(a)$ often by $(A(a)|b(a))$.

Observe that the map $\chi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is bijective if and only if for any non-zero $a \in \mathbb{F}_q^n$ equation (3) has no solution. Our goal is now to check whether (3) has a solution x for some fixed non-zero a.

3 The case $q > 2$

In this section we show that for $q > 2$ the map χ is a permutation on $\mathbb{F}_q^n$ if and only if q is even and $n = 1$. We consider separately the cases $n = 1, 2, 3$ and $n > 3$.

First let us assume that $n = 1$. In that case $\mathrm{S}(x) = x$ is the identity map and therefore $\chi(x) = x + \mathrm{S}(x) \odot \mathrm{S}^2(x) + \mathrm{S}^2(x) = x + x^2 + x = x^2 + 2x = x(x+2)$, which is a permutation if and only if q is even, as for q odd we have $\chi(0) = \chi(-2)$ and χ is not injective.

Remark 2. In general for any n it holds that $\chi(0, \ldots, 0) = \chi(-2, \ldots, -2)$ and therefore χ is never a permutation in odd characteristic, as noted in [8]. Therefore, from now on we could restrict ourselves to even characteristic. However, the rest of the proof presented here is valid independently of the characteristic of $\mathbb{F}_q$, with the minor exception in the case $n = 3$.

We continue with $n = 2$. In this case (3) has the form

$$\left(\begin{array}{cc|c} a_2 & a_1 & -a_1a_2 - 2a_2 \\ a_2 & a_1 & -a_1a_2 - 2a_1 \end{array}\right).$$

This has a solution for example in the case $a = (1, 1)$ which shows that χ is not a permutation.

Next, let $n = 3$. Now the system (3) looks like

$$\left(\begin{array}{ccc|c} a_2 & a_1 & & -a_1a_2 - a_2 - a_3 \\ & a_3 & a_2 & -a_2a_3 - a_3 - a_1 \\ a_3 & & a_1 & -a_3a_1 - a_1 - a_2 \end{array}\right). \tag{4}$$

Note that the determinant of the coefficient matrix is $2a_1a_2a_3$. Therefore, if q is odd, we can choose a_1, a_2, a_3 all nonzero and the corresponding system always has a solution. In

the case q even, assume that $a_2 \neq 0$. Let r_1, r_2, r_3 be the rows of the system (4). By replacing r_3 with $a_3 r_1 + a_1 r_2 + a_2 r_3$ we obtain

$$\left(\begin{array}{ccc|c} a_2 & a_1 & & a_1a_2 + a_2 + a_3 \\ & a_3 & a_2 & a_2a_3 + a_3 + a_1 \\ & & 0 & a_1^2 + a_2^2 + a_3^2 + a_1a_2 + a_1a_3 + a_2a_3 + a_1a_2a_3 \end{array}\right). \tag{5}$$

This system has a solution if there exist choices of $a_1, a_2, a_3 \in \mathbb{F}_q$ such that $a_2, a_3 \neq 0$ and

$$a_1^2 + (a_2 + a_3 + a_2a_3)a_1 + (a_2a_3 + a_2^2 + a_3^2) = 0, \tag{6}$$

which is a quadratic equation in a_1. Having in mind, that in binary fields a quadratic equation $X^2 + uX + v = 0$ has always a solution if $u = 0$, we put $a_2 + a_3 + a_2a_3 = 0$ in (6). Equivalently, by adding 1 on both sides, $(a_2 + 1)(a_3 + 1) = 1$. As $q > 2$, we can choose an element $a_3 \in \mathbb{F}_q \setminus \{0, 1\}$ and then $a_2 = \frac{1}{a_3+1} + 1 = \frac{a_3}{a_3+1} \neq 0$. For these $a_2, a_3 \neq 0$ the quadratic equation (6) has a solution $a_1 \in \mathbb{F}_q$, implying the existence of $(a_1, a_2, a_3) \neq 0$ for which the linear system (5) has a solution x.

We have thus proved the following lemma.

Lemma 3. *Let $q > 2$. If $n = 1$ then χ is a permutation if and only if q is even. If $n = 2, 3$ then χ is not a permutation.*

Let now $n > 3$. Again, we show that for certain choices of the vector $a \in \mathbb{F}_q^n \setminus \{0\}$ the equation (3) admits a solution x. Let $a_n = 0$. Then the linear system (3) reduces to

$$\left(\begin{array}{ccccccc|c} a_2 & a_1 & & & & & & -a_1a_2 - a_2 \\ & a_3 & a_2 & & & & & -a_2a_3 - a_3 - a_1 \\ & & a_4 & a_3 & & & & -a_3a_4 - a_4 - a_2 \\ & & & \ddots & \ddots & & & \vdots \\ & & & & a_{n-1} & a_{n-2} & 0 & -a_{n-2}a_{n-1} - a_{n-1} - a_{n-3} \\ & & & & 0 & 0 & a_{n-1} & -a_{n-2} \\ & & & & 0 & 0 & a_1 & -a_1 - a_{n-1} \end{array}\right).$$

Further, let all $a_1, \ldots, a_{n-1}$ be non-zero and assume

$$\det \begin{pmatrix} a_{n-1} & a_{n-2} \\ a_1 & a_1 + a_{n-1} \end{pmatrix} = 0,$$

or equivalently, $a_{n-1}(a_1 + a_{n-1}) = a_1a_{n-2}$. Under this assumption there is a solution $x \in \mathbb{F}_q^n$. Indeed we can choose x_{n-1} arbitrarily, for example $x_{n-1} = 1$, and then $x_n = -\frac{a_{n-2}}{a_{n-1}}$. The remaining components are obtained by simple back substitution, as the other diagonal entries are all nonzero.

Now it remains to see that there are non-zero $a_1, a_{n-1}, a_{n-2} \in \mathbb{F}_q$ such that the assumption $a_{n-1}(a_1 + a_{n-1}) = a_1a_{n-2}$ is satisfied. Note that because $n > 3$ the components a_1, a_{n-1}, a_{n-2} do not coincide. Let $a_{n-1} = 1$ and choose $a_1 \in \mathbb{F}_q \setminus \{0, -1\}$ arbitrarily. Then $a_1 + 1 \neq 0$ and $a_{n-2} = \frac{a_1+1}{a_1} \neq 0$, fulfilling the requirements.

We have thus proved the following result.

Lemma 4. *Let $q > 2$ and $n > 3$. Then $\chi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is not a permutation.*

4 The special case $q = 2$

It is known that for $q = 2$ the map $\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is bijective if and only if n is odd. If n is even it is easy to see that χ is not a permutation. Indeed,

$$\chi(1, 0, 1, 0, \ldots, 1, 0) = (0, \ldots, 0) = \chi(0, \ldots, 0),$$

as it has been noted in [2]. The fact that χ is a permutation for n odd was proved in [2] by using a seed-and-leap method to compute the preimage of a given element $y \in \mathbb{F}_2^n$. A more detailed proof of this approach can be found in [3]. Another method to compute the inverse of χ for n odd is given in Appendix D of [1], however without a proof. In [5] an explicit inverse formula of χ is given and proved.

To have a unified proof for Theorem 1, we present here a short proof for the statement that $\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is bijective if n is odd, applying the method developed in the previous sections.

Let now n be odd. If $n = 1$ then $\chi(x) = x^2 = x$ which is a permutation. So now assume $n \geq 3$. Let $a \in \mathbb{F}_2^n \setminus \{0\}$ be arbitrary. We aim to show that there is no solution x to $\chi(x) + \chi(x + a) = 0$. It can be easily seen that χ is shift-invariant, i.e. $\mathrm{S}(\chi(x)) = \chi(\mathrm{S}(x))$ for all $x \in \mathbb{F}_2^n$. Therefore, if $\chi(x) + \chi(x + a) = 0$ has a solution, then it follows that also

$$0 = \mathrm{S}(0) = \mathrm{S}(\chi(x) + \chi(x + a)) = \chi(\mathrm{S}(x)) + \chi(\mathrm{S}(x) + \mathrm{S}(a))$$

and there also exists a solution $\mathrm{S}(x)$ for $\mathrm{S}(a)$.

In the following we show that (3) has no solution by considering three cases. First we assume that a has two consecutive entries which are zero. Next we will assume that a has a zero entry such that the entries before and after are both nonzero. And finally we will assume that a only has nonzero entries.

Suppose now (3) has a solution x for a non-zero a with $a_i = a_{i+1} = 0$ for some $1 \leq i \leq n$. Since χ is shift-invariant, by considering an appropriate shift of a, we may assume without loss of generality that $a_n = a_1 = 0$. The last row of (3) then looks as follows:

$$\left(\begin{array}{cc|c} 0 & 0 & a_{n-1} \end{array} \right).$$

As the system has a solution x, it then follows that $a_{n-1} = 0$. However, then by considering the $(n-1)$-th row, it follows that also $a_{n-2} = 0$. By repeating this argument we obtain $a = 0$, a contradiction.

Next we assume that there exists an index $i \in \{1, \ldots, n\}$ such that $a_i = 0$ and $a_{i-1} = a_{i+1} = 1$. Again, by considering shifts of a, we may assume that $i = n$. From the last two rows of (3) it then immediately follows that $a_{n-2} = x_n = 0$. If $a_{n-3} = 0$, then we are in the previous case. Otherwise, we can repeat this argument and obtain that $a_{n-2k} = 0$ for all integers k. However, using that $n = 2m + 1$ is odd, we then also obtain $a_{n-2m} = a_1 = 0$, a contradiction to the assumption that $a_1 \neq 0$.

Finally, we need to consider $a = (1, \dots, 1)$. In this case (3) reduces to

$$\left(\begin{array}{ccccccc|c} 1 & 1 & & & & & & 1 \\ & 1 & 1 & & & & & 1 \\ & & 1 & 1 & & & & 1 \\ & & & \ddots & \ddots & & & \vdots \\ & & & & 1 & 1 & & 1 \\ & & & & & 1 & 1 & 1 \\ 1 & & & & & & 1 & 1 \end{array}\right)$$

By adding every of the first $n-1$ rows to the last one, we obtain (using that $n-1$ is even) the row

$$\left(\begin{array}{ccc|c} 0 & & 0 & 1 \end{array}\right)$$

which means that the equation has no solution.

The above considerations imply the following result:

Lemma 5. *The map $\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a permutation if and only if n is odd.*

Open Problem 6. Can our approach be used to find more information on the image set of $\chi : \mathbb{F}_q^n \to \mathbb{F}_q^n$, like its size or the preimage distribution?

5 Rank of the coefficient matrix $A(a)$ over $\mathbb{F}_2$

The equation (3) appears in the study of differential and linear properties of χ. In particular, the ranks of matrices $A(a)$ allow to determine the Walsh spectrum of χ. In [8] the following proposition is proved:

Proposition 7. *For any $a \in \mathbb{F}_2^n$ the rank of the matrix $A(a)$ over $\mathbb{F}_2$ is given by*

$$\operatorname{rank} A(a) = \omega(a) := \begin{cases} n-1, & a = (1, \dots, 1) \\ \mathrm{wt}(a) + \mathrm{r}(a), & \text{otherwise} \end{cases}$$

where $\mathrm{wt}(a)$ is the Hamming weight and $\mathrm{r}(a)$ is the number of 001-patterns in a. More precisely, $\mathrm{r}(a)$ is the number of indices $i = 1, \dots, n$ such that $(a_i, a_{i+1}, a_{i+2}) = (0, 0, 1)$ where the indices are computed modulo n.

We present a shorter proof of this fact using induction on n.

Claim 8. *Proposition 7 is true for $n = 1, 2, 3$.*

Proof. For $n = 1$, observe that $A(a_1) = (2a_1) = (0)$, and $\operatorname{rank} A(0) = \operatorname{rank} A(1) = 0 = \omega(1) = \omega(0)$. For $n = 2$ we have

$$A(a_1, a_2) = \begin{pmatrix} a_2 & a_1 \\ a_2 & a_1 \end{pmatrix}.$$

It is easily seen that, $\operatorname{rank} A(0,0) = 0 = \omega(0,0)$ and $\operatorname{rank} A(1,1) = \operatorname{rank} A(1,0) = \operatorname{rank} A(0,1) = 1 = \omega(1,1) = \omega(1,0) = \omega(0,1)$. Let $n = 3$, in which case

$$A(a_1, a_2, a_3) = \begin{pmatrix} a_2 & a_1 & \\ & a_3 & a_2 \\ a_3 & & a_1 \end{pmatrix}. \tag{7}$$

Using the shift-invariance of the rank of $A(a)$, we only need to consider the cases when a equals $(0,0,0)$, $(1,0,0)$, $(1,1,0)$, or $(1,1,1)$. It is easily seen that $\operatorname{rank} A(0,0,0) = 0 = \omega(0,0,0)$ and $\omega(1,0,0) = 2 = \operatorname{rank} A(1,0,0)$ and $\omega(1,1,0) = 2 = \operatorname{rank} A(1,1,0)$ and $\omega(1,1,1) = 2 = \operatorname{rank} A(1,1,1)$. □

Claim 9. *Proposition 7 is true for $a = (0,\dots,0)$ and $a = (1,\dots,1)$ with $n \geq 3$.*

Proof. If $a = (0,\dots,0)$ then $A(a)$ is the zero matrix and $\operatorname{rank} A(a) = 0 = \omega(a)$ is clear.

If $a = (1,\dots,1)$, then the first $n-1$ rows of $A(a)$ are linearly independent, so $\operatorname{rank} A(a) \geq n-1$. On the other hand, $(1,\dots,1)$ is in the kernel of $A(a)$, so $\operatorname{rank} A(a) \leq n-1$ and therefore $\operatorname{rank} A(a) = n-1 = \omega(a)$. □

We now proceed by induction on n. Let $n > 3$ be fixed and assume that the claim is true for all vectors $u \in \mathbb{F}_2^k$ with $k < n$. Let $a \in \mathbb{F}_2^n$. If $a = (0,\dots,0)$ or $a = (1,\dots,1)$ then the claim is true by Claim 9. Therefore, we may assume that $a \neq (0,\dots,0), (1,\dots,1)$. Note that from the shift-invariance of χ it follows that the rank of $A(a)$ is invariant under shifts of a. Equivalently, this can also be seen by switching rows and columns. Therefore, we can assume that $a_1 = 1, a_n = 0$. We write the vector a in the following form:

$$a = (\underbrace{1, *, \dots, *, 0}_{=u}, \underbrace{1, \dots, 1}_{=v}, \underbrace{0, \dots, 0}_{=w})$$

More precisely, let k be the last index such that $a_k = 1$ and a_j be the first index such that $a_i = 1$ for all $i = j,\dots,k$. Then $u = (a_1,\dots,a_{j-1}) = (1,*,\dots,*,0), v = (a_j,\dots,a_k) = (1,\dots,1)$ and $w = (a_{k+1},\dots,a_n) = (0,\dots,0)$. Note that we allow the vector u to be empty. This happens if and only if $a = (1,\dots,1,0,\dots,0)$, equivalently, $j = 1$. If a contains at least one occurrence of a 001-pattern, then by shift-invariance we can assume that w contains at least two zeros. Otherwise, $w = (0)$.

Note that $\operatorname{wt}(a) = \operatorname{wt}(u) + \operatorname{wt}(v) = \operatorname{wt}(u) + (k-j+1)$. Now consider the 001-patterns. Any 001-pattern in a either is completely contained inside u, ends exactly at a_j or ends at a_1. In the first case the 001-pattern is also contained in u. In the second case we know that $u = (1,*,\dots,*,0,0)$ ends in at least two zeros, and it also has a 001-pattern which ends at a_1. The last case occurs if and only if w has at least two zeros. It follows that

$$\mathrm{r}(a) = \begin{cases} \mathrm{r}(u) + 1 & w \text{ contains at least two zeros} \\ \mathrm{r}(u) & \text{otherwise.} \end{cases}$$

Then the matrix $A(a)$ has the following form:

$$\left(\begin{array}{cccc|cccc|cccc}
a_2 & a_1 & & & & & & & & & & \\
 & \ddots & \ddots & & & & & & & & & \\
 & & a_{j-1} & a_{j-2} & & & & & & & & \\
0 & & & a_j & a_{j-1} & & & & & & & \\
\hline
 & & & & a_{j+1} & a_j & & & & & & \\
 & & & & & \ddots & \ddots & & & & & \\
 & & & & & & a_{k-1} & a_{k-2} & & & & \\
 & & & & & & & a_k & a_{k-1} & & & \\
\hline
 & & & & & & & & a_{k+1} & a_k & & \\
 & & & & & & & & & a_{k+2} & a_{k+1} & \\
 & & & & & & & & & & \ddots & \ddots \\
 & & & & & & & & & & & a_n \\
a_n & & & & & & & & & & & a_1
\end{array}\right)$$

$$= \left(\begin{array}{cccc|cccc|cccc}
a_2 & a_1 & & & & & & & & & & \\
 & \ddots & \ddots & & & & & & & & & \\
 & & 0 & a_{j-2} & & & & & & & & \\
0 & & & 1 & 0 & & & & & & & \\
\hline
 & & & & 1 & 1 & & & & & & \\
 & & & & & \ddots & \ddots & & & & & \\
 & & & & & & 1 & 1 & & & & \\
 & & & & & & & 1 & 1 & & & \\
\hline
 & & & & & & & & 0 & 1 & & \\
 & & & & & & & & & 0 & 0 & \\
 & & & & & & & & & & \ddots & \ddots \\
 & & & & & & & & & & & 0 \\
0 & & & & & & & & & & & 1
\end{array}\right) \tag{8}$$

Note that $A(a)$ is a block diagonal matrix. The first block is the matrix $A(u)$ with $\operatorname{rank} A(u) = \omega(u)$ by the induction hypothesis. This also holds in the degenerate case that u is empty if we then define $\omega(u) = 0$. The second block has rank $k - j$. Note that if $k = j$ then the second block is empty. The third block has rank 2 if w includes at least two zeros, otherwise it has the form $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and has rank 1. Remember that the rank of a block diagonal matrix is the sum of the ranks of the blocks on the diagonal. It follows

that

$$\begin{aligned}\operatorname{rank} A(a) &= \omega(u) + (k-j) + \begin{cases} 2 & w \text{ contains at least two zeros} \\ 1 & \text{otherwise} \end{cases} \\ &= \operatorname{wt}(u) + (k-j+1) + \mathrm{r}(u) + \begin{cases} 1 & w \text{ contains at least two zeros} \\ 0 & \text{otherwise} \end{cases} \\ &= \operatorname{wt}(a) + \mathrm{r}(a) = \omega(a).\end{aligned}$$

For clarity, we also write down how (8) looks in the degenerate cases, namely that u empty, $j = k$ or both. We keep the horizontal and vertical lines to show which blocks vanish. If u is empty and $j < k$, then $a = (1, \ldots, 1, 0, \ldots, 0)$ and

$$A(a) = \left(\begin{array}{cccccc|cccc} 1 & 1 & & & & & & & & \\ & \ddots & \ddots & & & & & & & \\ & & 1 & 1 & & & & & & \\ & & & 1 & 1 & & & & & \\ \hline & & & & & 0 & 1 & & & \\ & & & & & & 0 & 0 & & \\ & & & & & & & \ddots & \ddots & \\ & & & & & & & & 0 & 0 \\ 0 & & & & & & & & & 1 \end{array}\right).$$

If u is not empty and $j = k$, then $a = (1, *, \ldots, *, 0, 1, 0, \ldots, 0)$ and

$$A(a) = \left(\begin{array}{cccccc|c|ccc} a_2 & a_1 & & & & & & & & \\ & \ddots & \ddots & & & & & & & \\ & & 0 & a_{j-2} & & & & & & \\ 0 & & & 1 & 0 & & & & & \\ \hline\hline & & & & & & 0 & 1 & & \\ & & & & & & & 0 & 0 & \\ & & & & & & & & \ddots & \ddots \\ & & & & & & & & & 0 \quad 0 \\ 0 & & & & & & & & & 1 \end{array}\right).$$

If u is empty and $j = k$, then $a = (1, 0, \ldots, 0)$ and

$$A(a) = \left(\begin{array}{c|ccccc} \hline\hline 0 & 1 & & & & \\ & 0 & 0 & & & \\ & & \ddots & \ddots & & \\ & & & 0 & 0 & \\ 0 & & & & 1 \end{array}\right).$$

References

[1] Alex Biryukov, Charles Bouillaguet, and Dmitry Khovratovich. *Cryptographic Schemes Based on the ASASA Structure: Black-box, White-box, and Public-key*. Cryptology ePrint Archive, Paper 2014/474. 2014. URL: https://eprint.iacr.org/2014/474 (visited on 01/18/2024).

[2] Joan Daemen. "Cipher and hash function design strategies based on linear and differential cryptanalysis". PhD thesis. KU Leuven, 1995.

[3] Joan Daemen, René Govaerts, and Joos Vandewalle. "An efficient nonlinear shift-invariant transformation". In: *Proceedings of the 15th Symposium on Information Theory in the Benelux*. Werkgemeenschap voor Informatie- en Communicatietheorie, 1994.

[4] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. "Ascon v1.2: Lightweight Authenticated Encryption and Hashing". In: *Journal of Cryptology* 34.3 (June 2021), p. 33. ISSN: 1432-1378. DOI: 10/gtfgst.

[5] Fukang Liu, Santanu Sarkar, Willi Meier, and Takanori Isobe. "The Inverse of χ and Its Applications to Rasta-Like Ciphers". In: *Journal of Cryptology* 35.4 (Oct. 2022), p. 28. ISSN: 1432-1378. DOI: 10/gtfgn7.

[6] NIST. *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. Tech. rep. Federal Information Processing Standard (FIPS) 202. U.S. Department of Commerce, Aug. 2015. DOI: 10.6028/NIST.FIPS.202.

[7] Kamil Otal. *A Solution to a Conjecture on the Maps $\chi_n^{(k)}$*. Cryptology ePrint Archive, Paper 2023/1782. 2023. URL: https://eprint.iacr.org/2023/1782 (visited on 01/18/2024).

[8] Jan Schoone and Joan Daemen. "Algebraic properties of the maps χ_n". In: *Designs, Codes and Cryptography* (2024). DOI: 10.1007/s10623-024-01395-w.

An effective approach to enumerate universal cycles for k-permutations

Zuling Chang
School of Mathematics and Statistics
Zhengzhou University
zuling_chang@zzu.edu.cn

Qiang Wang
School of Mathematics and Statistics
Carleton University
wang@math.carleton.ca

Jie Xue
School of Mathematics and Statistics
Zhengzhou University
xuejie@zzu.edu.cn

Abstract

A universal cycle for k-permutations is a cyclic arrangement in which each k-permutation appears exactly once as k consecutive elements. In this paper, we study the enumeration problem of universal cycles for k-permutations (Problem 477[**?**]) and obtain exact formulae for $k = 3, 4$.

1 Introduction

Universal cycles were introduced by Chung, Diaconis, and Graham [**?**] as generalizations of de Bruijn cycles [**?**], which are cyclic binary sequence of length 2^n that contain every binary n-tuple. Universal cycles are connected with Gray codes deeply [**?**, **?**]. In this paper we consider the universal cycles for k-permutations. Given a positive integer n, let $[n] = \{1, 2, \ldots, n\}$. A *$k$-permutation* is an ordered arrangement of k distinct elements in $[n]$, $1 \leq k \leq n$. Let $P_{n,k}$ be the set of all k-permutations of the n-set $[n]$. Obviously, $|P_{n,k}| = n!/(n-k)!$. Let $C = (c_1, c_2, \ldots, c_{|P_{n,k}|})$ be a cyclic arrangement (or periodic sequence), where each $c_i \in [n]$ for $1 \leq i \leq |P_{n,k}|$. If in C each k-permutation appears exactly once as k consecutive elements, then we say that C is a *universal cycle* for $P_{n,k}$. For example, if $n = 4$ and $k = 2$, then (123413242143) is a universal cycle for $P_{4,2}$

It is obvious that there is no universal cycle for k-permutations when $k = n$. Jackson [**?**] showed that the universal cycle for k-permutations always exists when $k < n$. There are lots of results about the construction of universal cycles for k-permutations, mainly for the case that $k = n - 1$ named *shorthand permutations* [**?**, **?**, **?**, **?**]. Wong [**?**] introduced the relaxed shorthand notation to encode permutations. Recently, Sawada and Williams [**?**] consider the universal cycle for strings with fixed-content. An interesting problem is to enumerate distinct universal cycles for k-permutations. This problem was formally presented in [**?**].

Problem 1. (Problem 477 [?]) How many different universal cycles for $P_{n,k}$ exist?

As far as we know, this enumeration problem is still open. When $k = 1$, the number of universal cycles for $P_{n,1}$ is obviously equal to $(n-1)!$. However, for $k \geq 2$, it is not easy to enumerate universal cycles. The number of universal cycles for $P_{n,2}$ and $P_{n,3}$ were obtained in [?], using Eulerian tours on certain digraphs and their adjacency matrices, their powers, and corresponding eigenvalues. The key is to find an algebraic relation between the adjacency matrix and the all one matrix, and thus to determine these eigenvalues. However, for $k \geq 4$, it is complicated to determine the enumeration formula by using the method in [?]. In this paper, we propose a new method to find eigenvalues of the adjacency matrix and thus count the number of universal cycles. Based on this method, we obtain the exact formula for $k = 4$, and this also gives a new proof of the exact formula for $k = 3$.

Let us recall some definitions and concepts for digraphs. For a vertex v in a digraph, its out-degree is the number of arcs with initial vertex v, and its in-degree is the number of arcs with final vertex v. A digraph is balanced if each vertex has the same in-degree and out-degree. Obviously, a digraph contains an Eulerian tour if and only if the digraph is connected and balanced (see, for example, [?, Theorem 1.7.2]).

Given a digraph D, its *adjacency matrix* is the (0,1)-matrix $A = (a_{i,j})$ where $a_{i,j} = 1$ if $v_i v_j$ is an arc of D, and $a_{i,j} = 0$ otherwise. Let Γ be the diagonal matrix of the vertex out-degrees. The *Laplacian matrix* of D is defined as $L = \Gamma - A$. The eigenvalues of L are called the Laplacian eigenvalues of D.

Now we introduce the definition of the transition digraph. Let D be a digraph with vertex set $P_{n,k-1}$. The arcs of D satisfy the following rule: for any two vertices $i_1 i_2 \cdots i_{k-1}$ and $j_1 j_2 \cdots j_{k-1}$, there is an arc from $i_1 i_2 \cdots i_{k-1}$ to $j_1 j_2 \cdots j_{k-1}$ if and only if $i_s = j_{s-1}$ for $2 \leq s \leq k-1$, and $i_1 \neq j_{k-1}$. Such a digraph is called the transition digraph of $P_{n,k}$. Let uv be an arc in D with initial vertex u and final vertex v. If $u = i_1 i_2 \cdots i_{k-1}$, then $v = i_2 i_3 \cdots i_{k-1} i_k$, where $i_k \in [n] \backslash \{i_1, i_2, \ldots, i_{k-1}\}$, and so the arc uv may be regarded as the k-permutation $i_1 i_2 \cdots i_{k-1} i_k$. On the other hand, any k-permutation $i_1 i_2 \cdots i_{k-1} i_k$ in $P_{n,k}$ is represented by an arc with initial vertex $i_1 i_2 \cdots i_{k-1}$ and final vertex $i_2 i_3 \cdots i_{k-1} i_k$. Jackson [?] showed that such transition digraph is balanced and connected. One can see that any Eulerian tour in this transition digraph corresponds to a universal cycle for $P_{n,k}$, which leads to the following proposition directly.

Proposition 2. *The number of distinct universal cycles for $P_{n,k}$ is equal to the number of Eulerian tours of its transition digraph.*

This proposition implies that it is sufficient to consider the number of Eulerian tours in the transition digraph of $P_{n,k}$. Let D be a connected balanced digraph, and let $\epsilon(D)$ denote the number of Eulerian tours of D. We use $d^+(v)$ to denote the out-degree of a vertex v. There is a surprising connection between the number of Eulerian tours and Laplacian eigenvalues, given by the next lemma.

Lemma 3. ([?]) *Let D be a connected balanced digraph with vertex set V. If the Laplacian*

eigenvalues of D are $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_{|V|-1} > \mu_{|V|} = 0$, then

$$\epsilon(D) = \frac{1}{|V|}\mu_1\mu_2\cdots\mu_{|V|-1}\prod_{v\in V}(d^+(v)-1)!. \tag{1}$$

According to Lemma **??**, to count the number of universal cycles for $P_{n,k}$, it is enough to compute the corresponding Laplacian eigenvalues. Let D be the transition digraph of $P_{n,k}$ with adjacency matrix A and Laplacian matrix L. Since D is regular, the eigenvalues of L can be determined by the eigenvalues of A. Hence the eigenvalues of A are the key to count the number of universal cycles. However, the eigenvalues of A are usually more difficult to compute directly, since the order of A is $n!/(n-k+1)!$. In order to determine the eigenvalues of A, we introduce the representation matrix T of the transition digraph D (see Definition **??** for details). The first main result of the paper establishes an algebraic relation of the representation matrix T and adjacency matrix A.

Lemma 4. *The minimal polynomial of A divides the characteristic polynomial of T.*

From [**?**, Corollary 3.3.4] and Lemma **??**, the eigenvalues of A are contained in the set of eigenvalues of T, without counting multiplicities. Note that the order of T is $\sum_{i=0}^{k-1}\frac{(k-1!)^2}{(i!)^2(k-1-i)!}$. Clearly, if n is sufficiently large for k, then the order of T is generally much smaller than the order of A. Therefore, Lemma **??** provides an efficient approach to find all possible vaules of eigenvalues of A. Once the values of eigenvalues are determined, we use the standard techniques from spectral graph theory to determine their multiplicities and thus the number of universal cycles can be obtained from Lemma **??**. In particular, we obtain the exact formulae for $P_{n,3}$ and $P_{n,4}$ in the following results.

Theorem 5. ([**?**]) *The number of universal cycles for $P_{n,3}$ is equal to $n^{n-2}(n-1)^{\frac{n(n-3)}{2}-1}(n-2)^{n-1}(n-3)^{\frac{(n-1)(n-2)}{2}}((n-3)!)^{n(n-1)}$.*

Theorem 6. *The number of universal cycles for $P_{n,4}$ is equal to $n^{n-2}(n-1)^{\frac{n(n-3)}{2}-1}(n-2)^{\frac{n(n-2)(n-4)}{3}-2}(n-3)^{\frac{(n-1)(3n-2)}{2}-1}(n-4)^{(n-1)(n-2)-1}(n^2-7n+13)^{\frac{n(n-2)(n-4)}{3}}((n-4)!)^{n(n-1)(n-2)}$.*

The rest of this paper is organized as follows. In Section **??** we introduce some definitions and properties of the adjacency matrix and the so-called representation matrix of transition digraph with vertex set $P_{n,k}$. The detailed proofs of Theorems **??** and **??** are provided in Section 3 and Section 4, respectively.

2 Adjacency matrix and representation matrix

For the sake of convenience, in this section, we consider the transition digraph D with vertex set $P_{n,m}$, $1 \leq m \leq n-2$. At this time the Eulerian tours in D correspond to universal cycles for $P_{n,m+1}$. Let A be the adjacency matrix of D. We use $\tau_l(u,v)$ to denote the number of walks from u to v in D with length $l \geq 0$. Thus the (u,v)-entry of A^l is equal to $\tau_l(u,v)$.

For a square matrix M, let $\mathrm{tr}(M)$ denote the trace of M. We note that the diagonal entry of A^l is the number of closed walks of length l. Therefore, the transition digraph D has $\mathrm{tr}(A^l)$ closed walks of length l.

Lemma 7. *Let D be the transition digraph with vertex set $P_{n,m}$. Then its adjacency matrix A satisfies the following properties:*
(1) $\mathrm{tr}(A^0) = n!/(n-m)!$*;*
(2) if $1 \le l \le m$*, then* $\mathrm{tr}(A^l) = 0$*;*
(3) if $n \ge m+1$*, then* $\mathrm{tr}(A^{m+1}) = n!/(n-m-1)!$.

Proof. Since A^0 is an identity matrix, $\mathrm{tr}(A^0) = |P_{n,m}| = n!/(n-m)!$. Note that a closed l-walk in D is equivalent to a periodic sequence $(c_1, c_2, \ldots, c_l)$ which satisfies the following conditions: any m consecutive elements form an m-permutation in $P_{n,m}$, and any $m+1$ consecutive elements form an $(m+1)$-permutation in $P_{n,m+1}$. This means that, in D, there are no closed walks of length less than $m+1$. Hence $\mathrm{tr}(A^l) = 0$ for any $1 \le l \le m$, and $\mathrm{tr}(A^{m+1}) = |P_{n,m+1}| = n!/(n-m-1)!$. □

About $\tau_l(u, v)$, since D is vertex-transitive, there is an automorphism θ such that $\theta(u) = 12\cdots m$ and $\theta(v) = \beta$ where $\beta \in P_{n,m}$. Then $\tau_l(u, v) = \tau_l(12\cdots m, \beta)$. Thus, in order to discuss the number of l-walks in D, it suffices to consider the number of l-walks from the vertex $12\cdots m$ to any other vertex in D.

A *multiset* is a collection in which elements may occur more than once. The number of times an element occurs in a multiset is called its multiplicity. The cardinality of a multiset is the sum of the multiplicities of its elements. Let $S = \{1, 2, \ldots, m, n^{[n-m]}\}$ be a multiset, where the multiplicity of the element n is $n-m$. Let $P^*_{n,m}$ be the set of all arrangements of m elements in the n-multiset S. Obviously,

$$|P^*_{n,m}| = \sum_{i=0}^{m} \frac{m!}{i!}\binom{m}{i} = \sum_{i=0}^{m} \frac{(m!)^2}{(i!)^2(m-i)!}.$$

Let δ be an integer-valued function on $[n]$ with

$$\delta(i) = \begin{cases} i, & \text{if } i \le m, \\ n, & \text{if } i > m, \end{cases}$$

for any $1 \le i \le n$. We shall define a map $\phi : P_{n,m} \mapsto P^*_{n,m}$ such that for any permutation $b_1 b_2 \cdots b_m \in P_{n,m}$,

$$\phi(b_1 b_2 \cdots b_m) = \delta(b_1)\delta(b_2)\cdots\delta(b_m).$$

Clearly, ϕ is a surjection. Moreover, for any $\alpha \in P^*_{n,m}$, the preimage $\phi^{-1}(\alpha)$ is the set of all permutations of $P_{n,m}$ that map to α under ϕ. For convenience, we may assume that all the arrangements in $P^*_{n,m} = \{\alpha^{(1)}, \ldots, \alpha^{(|P^*_{n,m}|)}\}$ are listed by lexicographical order, that is,

$$\alpha^{(1)} \preccurlyeq \alpha^{(2)} \preccurlyeq \cdots \preccurlyeq \alpha^{(|P^*_{n,m}|)},$$

where $\alpha^{(i)} = a_1^{(i)} a_2^{(i)} \cdots a_m^{(i)}$. In particular, $\alpha^{(1)} = 12\cdots m$ and $\alpha^{(|P^*_{n,m}|)} = nn\cdots n$.

Based on the fact that D is vertex-transitive, we have the following result.

Lemma 8. *Suppose $\alpha^{(i)} \in P^*_{n,m}$. Then $\tau_l(\alpha^{(1)}, b) = \tau_l(\alpha^{(1)}, b')$ for any $b, b' \in \phi^{-1}(\alpha^{(i)})$.*

We use $\tau_l^*(\alpha^{(1)}, \alpha^{(i)})$ to denote the number of l-walks from $12\cdots m$ to any permutation in $\phi^{-1}(\alpha^{(i)})$, that is, $\tau_l^*(\alpha^{(1)}, \alpha^{(i)}) = \tau_l(\alpha^{(1)}, b)$ where $b \in \phi^{-1}(\alpha^{(i)})$.

For $l \geq 0$, we let $X^l = (\tau_l^*(\alpha^{(1)}, \alpha^{(1)}), \tau_l^*(\alpha^{(1)}, \alpha^{(2)}), \ldots, \tau_l^*(\alpha^{(1)}, \alpha^{(|P_{n,m}^*|)}))$. Clearly, $X^0 = (1, 0, \ldots, 0)$. To study the property of X^l, we need some auxiliary tools.

Let $\varrho : P_{n,m}^* \times P_{n,m}^* \mapsto \{0, 1\}$ and $\sigma : P_{n,m}^* \mapsto \{0, 1, \ldots, m\}$ be two functions defined as follows:

$$\varrho(\alpha^{(i)}, \alpha^{(j)}) = \begin{cases} 1, & \text{if } a_2^{(i)} \cdots a_m^{(i)} = a_1^{(j)} \cdots a_{m-1}^{(j)} \text{ and } a_1^{(i)} \neq a_m^{(j)}, \\ 1, & \text{if } a_2^{(i)} \cdots a_m^{(i)} = a_1^{(j)} \cdots a_{m-1}^{(j)} \text{ and } a_1^{(i)} = a_m^{(j)} = n, \\ 0, & \text{otherwise,} \end{cases}$$

and

$$\sigma(\alpha^{(i)}) = \#\{a_t^{(i)} : 1 \leq t \leq m, a_t^{(i)} = n\}.$$

Now we introduce the definition of the representation matrix for a transition digraph.

Definition 9. Let D be a transition digraph with vertex set $P_{n,m}$. The representation matrix, denoted by T, of D is defined as follows:

- T is a matrix of order $|P_{n,m}^*|$;
- for any two arrangements $\alpha^{(i)}$ and $\alpha^{(j)}$ in $P_{n,m}^*$, the (i, j)-entry of T is

$$T(i, j) = \begin{cases} n - m - \sigma(\alpha^{(j)}), & \text{if } \varrho(\alpha^{(i)}, \alpha^{(j)}) = 1 \text{ and } a_1^{(i)} = n, \\ 1, & \text{if } \varrho(\alpha^{(i)}, \alpha^{(j)}) = 1 \text{ and } a_1^{(i)} \neq n, \\ 0, & \text{otherwise.} \end{cases}$$

We remark that the matrix T can also be viewed as a quotient-like matrix for the transition digraph D (see, e.g., [**?**]).

The following lemma describes a relation between the representation matrix T and the vector X^l.

Lemma 10. *Let $X^l = (\tau_l^*(\alpha^{(1)}, \alpha^{(1)}), \tau_l^*(\alpha^{(1)}, \alpha^{(2)}), \ldots, \tau_l^*(\alpha^{(1)}, \alpha^{(|P_{n,m}^*|)}))$ and T defined as above. Then $X^l T = X^{l+1}$.*

Proof. Set $q = |P_{n,m}^*|$. Let $X^l = (\tau_l^*(\alpha^{(1)}, \alpha^{(1)}), \tau_l^*(\alpha^{(1)}, \alpha^{(2)}), \ldots, \tau_l^*(\alpha^{(1)}, \alpha^{(q)}))$. It suffices to prove that, for $1 \leq s \leq q$,

$$\tau_{l+1}^*(\alpha^{(1)}, \alpha^{(s)}) = \sum_{i=1}^{q} \tau_l^*(\alpha^{(1)}, \alpha^{(i)}) T(i, s).$$

Suppose that $\alpha^{(s)} = a_1 a_2 \cdots a_m$. Let $b = b_1 b_2 \cdots b_m$ be a permutation in $P_{n,m}$ such that $b_1 b_2 \cdots b_m \in \phi^{-1}(\alpha^{(s)})$. Then $\delta(b_i) = a_i$ for $1 \leq i \leq m$. We define three subsets of $[n]$:

$$R = \{z : z \neq b_m, z b_1 b_2 \cdots b_{m-1} \in P_{n,m}\}, R_1 = \{z \in R : z \leq m\} \text{ and } R_2 = \{z \in R : z > m\}.$$

Obviously, $R = R_1 \cup R_2$ and $R_1 \cap R_2 = \emptyset$. For any $z \in R$, there is an arc from $zb_1 \cdots b_{m-1}$ to $b_1 b_2 \cdots b_m$ in the transition graph. If $z \in R_1$, then $\phi(zb_1 \cdots b_{m-1}) = za_1 a_2 \cdots a_{m-1}$. If $z \in R_2$, then $\phi(zb_1 \cdots b_{m-1}) = na_1 a_2 \cdots a_{m-1}$. It follows that

$$\begin{aligned}
\tau^*_{l+1}(\alpha^{(1)}, \alpha^{(s)}) &= \tau_{l+1}(\alpha^{(1)}, b) \\
&= \sum_{z \in R} \tau_l(\alpha^{(1)}, zb_1 b_2 \cdots b_{m-1}) \\
&= \sum_{z \in R_1} \tau_l(\alpha^{(1)}, zb_1 b_2 \cdots b_{m-1}) + \sum_{z \in R_2} \tau_l(\alpha^{(1)}, zb_1 b_2 \cdots b_{m-1}) \\
&= \sum_{z \in R_1} \tau^*_l(\alpha^{(1)}, za_1 a_2 \cdots a_{m-1}) + \sum_{z \in R_2} \tau^*_l(\alpha^{(1)}, na_1 a_2 \cdots a_{m-1}).
\end{aligned}$$

Since $\phi(b_1 b_2 \cdots b_m) = \alpha^{(s)}$, the permutation $b_1 b_2 \cdots b_m$ contains $\sigma(\alpha^{(s)})$ integers greater than m. It is easy to see that $|R_2| = n - m - \sigma(\alpha^{(s)})$. Set $\beta = a_1 a_2 \cdots a_{m-1}$. Then we have

$$\tau^*_{l+1}(\alpha^{(1)}, \alpha^{(s)}) = \sum_{z \in R_1} \tau^*_l(\alpha^{(1)}, z\beta) + (n - m - \sigma(\alpha^{(s)}))\tau^*_l(\alpha^{(1)}, n\beta). \tag{2}$$

On the other hand, by the definition of T, one can see that

$$\sum_{i=1}^{m} \tau^*_l(\alpha^{(1)}, \alpha^{(i)}) T(i, s) = \sum_{z \in R_3} \tau^*_l(\alpha^{(1)}, z\beta) + (n - k - \sigma(\alpha^{(s)}))\tau^*_l(\alpha^{(1)}, n\beta), \tag{3}$$

where $R_3 = \{z \leq m : z \neq a_m, z\beta \in P^*_{n,m}\}$. Clearly, $R_3 = R_1$. Combining (**??**) and (**??**), the required equality follows. □

Lemma 11. *Let T and A be the representation matrix and adjacency matrix of a transition digraph D respectively. If $f(\lambda)$ is a polynomial such that $f(T) = \mathbf{0}$, then $f(A) = \mathbf{0}$.*

Proof. Let $f(\lambda) = \sum_{i=0}^{s} c_i \lambda^i$ such that $f(T) = \sum_{i=0}^{s} c_i T^i = \mathbf{0}$. It suffices to show that

$$f(A) = \sum_{i=0}^{s} c_i A^i = \mathbf{0}. \tag{4}$$

Let u and v be vertices in D ($u = v$ is allowed). Thus, to show (**??**), it suffices to prove that

$$\sum_{i=0}^{s} c_i \tau_i(u, v) = 0. \tag{5}$$

According to Lemma **??**, it is enough to prove that for any $\alpha^{(j)} \in P^*_{n,m}$,

$$\sum_{i=0}^{s} c_i \tau^*_i(\alpha^{(1)}, \alpha^{(j)}) = 0. \tag{6}$$

By the definition of X^l and Lemma **??**, Equation (**??**) is equivalent to

$$\sum_{i=0}^{s} c_i X^i = \sum_{i=0}^{s} c_i X^0 T^i = X^0 (\sum_{i=0}^{s} c_i T^i) = X^0 f(T) = \mathbf{0}.$$

Hence the proof is complete. □

Proof of Lemma **??**. Suppose that $p(\lambda)$ is the characteristic polynomial of T. The Cayley-Hamilton Theorem implies that $p(T) = \mathbf{0}$. By Lemma **??**, one can see that $p(\lambda)$ is a monic polynomial that annihilates A. This leads to that the minimal polynomial of A divides $p(\lambda)$, which completes the proof. □

3 Enumeration formula for $k = 3$

In this section we re-derive the exact formula for $P_{n,3}$, which was first obtained in [**?**] using a different method. In this case, we recall that the transition graph D is defined on the vertex set $P_{n,2}$ and $P^*_{n,2}$ is the set of all arrangements of 2 elements of $\{1, 2, n^{[n-2]}\}$. We may list the arrangements in $P^*_{n,2}$ by lexicographical order, as follows:

$$12 \preccurlyeq 1n \preccurlyeq 21 \preccurlyeq 2n \preccurlyeq n1 \preccurlyeq n2 \preccurlyeq nn.$$

Thus, the representation matrix T can be written as

$$T = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ n-2 & n-3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & n-2 & n-3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & n-3 & n-3 & n-4 \end{bmatrix}.$$

A simple calculation shows that the characteristic polynomial of T is

$$p_T(\lambda) = (\lambda - n + 2)(\lambda - 1)(\lambda + 1)(\lambda^2 + \lambda + n - 2)^2.$$

According to Lemma **??**, we obtain that the characteristic polynomial of A is

$$p_A(\lambda) = (\lambda - n + 2)(\lambda - 1)^{t_1}(\lambda + 1)^{t_2}(\lambda^2 + \lambda + n - 2)^{t_3},$$

where t_1, t_2, t_3 are nonnegative integers. Let p and q be two roots of $\lambda^2 + \lambda + n - 2 = 0$. It follows that the eigenvalues of A are listed as $n - 2, 1^{[t_1]}, (-1)^{[t_2]}, p^{[t_3]}, q^{[t_3]}$ with their multiplicites. Using the relationship between eigenvalues and trace of a matrix, it follows from Lemma **??** that

$$\begin{cases} \mathrm{tr}(A^0) = t_1 + t_2 + 2t_3 + 1 = n(n-1), \\ \mathrm{tr}(A) = n - 2 + t_1 - t_2 + t_3(p+q) = 0, \\ \mathrm{tr}(A^2) = (n-2)^2 + t_1 + t_2 + t_3(p^2+q^2) = 0. \end{cases} \tag{7}$$

Since p and q are roots of $\lambda^2+\lambda+n-2=0$, one can see that

$$\begin{cases} p+q=-1, \\ p^2+q^2=-2n+5. \end{cases} \tag{8}$$

Combining (**??**) and (**??**), we obtain that $t_1=(n-1)(n-2)/2$, $t_2=n(n-3)/2$ and $t_3=n-1$. Then the next result follows directly.

Lemma 12. *Let A be the adjacency matrix of the transition digraph defined on $P_{n,2}$. Then the eigenvalues of A are $n-2, 1^{[(n-1)(n-2)/2]}, (-1)^{[n(n-3)/2]}, p^{[n-1]}, q^{[n-1]}$, where p and q are roots of $\lambda^2+\lambda+n-2=0$.*

Since the out-degree of any vertex in the transition digraph is $(n-2)$, the Laplacian matrix L and the adjacency matrix A satisfy the equation $L=(n-2)I-A$. Hence the eigenvalues of L can be obtained by the above lemma.

Corollary 13. *Let L be the Laplacian matrix of the transition digraph defined on $P_{n,2}$. Then the eigenvalues of L are $0, (n-3)^{[(n-1)(n-2)/2]}, (n-1)^{[n(n-3)/2]}, (n-2-p)^{[n-1]}, (n-2-q)^{[n-1]}$, where p and q are roots of $\lambda^2+\lambda+n-2=0$.*

We are now in a position to prove Theorem **??**.

Proof of Theorem **??**. Proposition **??** shows that the number of distinct universal cycles for $P_{n,3}$ is equal to the number of Eulerian tours in D. Combining Lemma **??** and Corollary **??**, one can see that the number of Eulerian tours in D is

$$\epsilon(D)=\frac{1}{n(n-1)}(n-3)^{\frac{(n-1)(n-2)}{2}}(n-1)^{\frac{n(n-3)}{2}}(n-2-p)^{n-1}(n-2-q)^{n-1}\prod_{v\in V(D)}(n-3)!. \tag{9}$$

Since p and q are roots of $\lambda^2+\lambda+n-2=0$, it follows that

$$(n-2-p)(n-2-q)=n(n-2).$$

Therefore, we obtain that

$$\epsilon(D)=n^{n-2}(n-1)^{\frac{n(n-3)}{2}-1}(n-2)^{n-1}(n-3)^{\frac{(n-1)(n-2)}{2}}((n-3)!)^{n(n-1)},$$

and the result follows. □

4 Enumerating formula for $k=4$

We now derive the enumeration formula for $P_{n,4}$ using this method. Let D be the corresponding transition digraph. Clearly, D is defined on $P_{n,3}$. All arrangements in $P^*_{n,3}$ can be listed by lexicographical order, as follows:

$$\begin{aligned} 123 \preccurlyeq 12n \preccurlyeq 132 \preccurlyeq 13n \preccurlyeq 1n2 \preccurlyeq 1n3 \preccurlyeq 1nn \preccurlyeq 213 \preccurlyeq 21n \preccurlyeq 231 \preccurlyeq 23n \preccurlyeq 2n1 \\ \preccurlyeq 2n3 \preccurlyeq 2nn \preccurlyeq 312 \preccurlyeq 31n \preccurlyeq 321 \preccurlyeq 32n \preccurlyeq 3n1 \preccurlyeq 3n2 \preccurlyeq 3nn \preccurlyeq n12 \preccurlyeq n13 \\ \preccurlyeq n1n \preccurlyeq n21 \preccurlyeq n23 \preccurlyeq n2n \preccurlyeq n31 \preccurlyeq n32 \preccurlyeq n3n \preccurlyeq nn1 \preccurlyeq nn2 \preccurlyeq nn3 \preccurlyeq nnn \end{aligned}$$

Table 1: Power sums of the roots

sum	value	sum	value	sum	value	sum	value
a_1+a_2	1	$\sum_{i=1}^{3} b_i$	1	$\sum_{i=1}^{3} c_i$	-1	$\sum_{i=1}^{3} d_i$	-1
$a_1^2+a_2^2$	-1	$\sum_{i=1}^{3} b_i^2$	-1	$\sum_{i=1}^{3} c_i^2$	3	$\sum_{i=1}^{3} d_i^2$	$-2n+7$
$a_1^3+a_2^3$	-2	$\sum_{i=1}^{3} b_i^3$	$3n-11$	$\sum_{i=1}^{3} c_i^3$	$3n-13$	$\sum_{i=1}^{3} d_i^3$	$3(n-3)(4-n)-1$
$a_1^4+a_2^4$	-1	$\sum_{i=1}^{3} b_i^4$	$4n-13$	$\sum_{i=1}^{3} c_i^4$	$-4n+19$	$\sum_{i=1}^{3} d_i^4$	$2(n-3)(3n-11)+1$

According to Definition **??**, one can determine the representation matrix T of D, which is exhibited in the Appendix. Using MAPLE, we obtain that the characteristic polynomial of T is

$$p_T(\lambda) = (\lambda-n+3)(\lambda+1)^2(\lambda^2-\lambda+1)^2(\lambda^3-\lambda^2+\lambda-n+3)^3(\lambda^3+\lambda^2-\lambda-n+3)^3 \\ (\lambda^3+\lambda^2+(n-3)\lambda+(n-3)^2)^3.$$

Then by Lemma **??**, it follows that the characteristic polynomial of A is

$$p_A(\lambda) = (\lambda-n+3)(\lambda+1)^{t_1}(\lambda^2-\lambda+1)^{t_2}(\lambda^3-\lambda^2+\lambda-n+3)^{t_3}(\lambda^3+\lambda^2-\lambda-n+3)^{t_4} \\ (\lambda^3+\lambda^2+(n-3)\lambda+(n-3)^2)^{t_5},$$

where t_1, t_2, t_3, t_4, t_5 are indetermined nonnegative integers. We may assume that the roots of the irreducible factors of $p_A(\lambda)$ are as follows:

- the roots of $\lambda^2-\lambda+1$ are denoted by a_1 and a_2;
- the roots of $\lambda^3-\lambda^2+\lambda-n+3$ are denoted by b_1, b_2 and b_3;
- the roots of $\lambda^3+\lambda^2-\lambda-n+3$ are denoted by c_1, c_2 and c_3;
- the roots of $\lambda^3+\lambda^2+(n-3)\lambda+(n-3)^2$ are denoted by d_1, d_2 and d_3.

The power sums of the above roots are presented in Table **??**. Note that the eigenvalues of A are

$$n-3, (-1)^{[t_1]}, a_1^{[t_2]}, a_2^{[t_2]}, b_1^{[t_3]}, b_2^{[t_3]}, b_3^{[t_3]}, c_1^{[t_4]}, c_2^{[t_4]}, c_3^{[t_5]}, d_1^{[t_5]}, d_2^{[t_5]}, d_3^{[t_5]}.$$

According to Lemma **??**, it follows that

$$\begin{cases} \mathrm{tr}(A^0) = 1+t_1+2t_2+3t_3+3t_4+3t_5 = n(n-1)(n-2) \\ \mathrm{tr}(A) = n-3-t_1+t_2(a_1+a_2)+t_3\sum_{i=1}^{3} b_i+t_4\sum_{i=1}^{3} c_i+t_5\sum_{i=1}^{3} d_i = 0 \\ \mathrm{tr}(A^2) = (n-3)^2+t_1+t_2(a_1^2+a_2^2)+t_3\sum_{i=1}^{3} b_i^2+t_4\sum_{i=1}^{3} c_i^2+t_5\sum_{i=1}^{3} d_i^2 = 0 \\ \mathrm{tr}(A^3) = (n-3)^3-t_1+t_2(a_1^3+a_2^3)+t_3\sum_{i=1}^{3} b_i^3+t_4\sum_{i=1}^{3} c_i^3+t_5\sum_{i=1}^{3} d_i^3 = 0 \\ \mathrm{tr}(A^4) = (n-3)^4+t_1+t_2(a_1^4+a_2^4)+t_3\sum_{i=1}^{3} b_i^4+t_4\sum_{i=1}^{3} c_i^4+t_5\sum_{i=1}^{3} d_i^4 = n!/(n-4)! \end{cases}$$

Combining with the power sums in Table **??**, it follows from the calculation that

$$\begin{cases} t_1 = n(n-2)(n-4)/3-1, \\ t_2 = n(n-2)(n-4)/3, \\ t_3 = (n-1)(n-2)/2, \\ t_4 = (n-1)(n-2)/2-1, \\ t_5 = n-1. \end{cases} \tag{10}$$

Let L be the Laplacian matrix of D. Since the out-degree of any vertex in D is $n-3$, we have $L=(n-3)I-A$. Thus, the eigenvalues of L are

$$0,(n-2)^{[t_1]},(n-3-a_1)^{[t_2]},(n-3-a_2)^{[t_2]},(n-3-b_1)^{[t_3]},(n-3-b_2)^{[t_3]},(n-3-b_3)^{[t_3]},$$
$$(n-3-c_1)^{[t_4]},(n-3-c_2)^{[t_4]},(n-3-c_3)^{[t_5]},(n-3-d_1)^{[t_5]},(n-3-d_2)^{[t_5]},(n-3-d_3)^{[t_5]}.$$

Since a_1 and a_2 are roots of $\lambda^2-\lambda+1=0$, we obtain that $a_1+a_2=1$ and $a_1a_2=1$. It follows that $(n-3-a_1)(n-3-a_2)=n^2-7n+13$. Similarly, one can see that

$$\begin{cases}(n-3-b_1)(n-3-b_2)(n-3-b_3)=(n-3)^2(n-4),\\(n-3-c_1)(n-3-c_2)(n-3-c_3)=(n-1)(n-3)(n-4),\\(n-3-d_1)(n-3-d_2)(n-3-d_3)=n(n-3)^2.\end{cases}$$

Thus the product of the nonzero eigenvalues of L, denoted by z, is

$$z=(n-2)^{t_1}(n^2-7n+13)^{t_2}((n-3)^2(n-4))^{t_3}((n-1)(n-3)(n-4))^{t_4}(n(n-3)^2)^{t_5},$$

where the values of t_i, $i=1,2,\ldots,5$, are from (**??**). By Lemma **??**, the number of Eulerian tours of D is

$$\begin{aligned}\epsilon(D) &= z\frac{(n-3)!}{n!}\prod_{v\in V(D)}(d^+(v)-1)!\\ &= \frac{z}{n(n-1)(n-2)}((n-4)!)^{n(n-1)(n-2)}\\ &= n^{n-2}(n-1)^{\frac{n(n-3)}{2}-1}(n-2)^{\frac{n(n-2)(n-4)}{3}-2}(n-3)^{\frac{(n-1)(3n-2)}{2}-1}(n-4)^{(n-1)(n-2)-1}\\ &\quad (n^2-7n+13)^{\frac{n(n-2)(n-4)}{3}}((n-4)!)^{n(n-1)(n-2)},\end{aligned}$$

which yields the exact formula in Theorem **??**.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Nos. 62272420 and 12001498).

References

[1] J. Bang-Jensen, G. Gutin, *Digraphs: Theory, Algorithms and Applications*, Springer Monographs in Mathematics, 2nd ed., Springer-Verlag, London, 2009.

[2] N.G. de Bruijn, A combinatorial problem,*Proceedings of the Section of Sciences of the Koninklijke Nederlandse Akademie van Wetenschappen te Amsterdam*, 49 (1946) 758-764.

[3] Z. Chang, J. Xue, Enumerations of universal cycles for k-permutations, *Discrete Mathematics*, 345 (2022) 112975.

[4] F. Chung, P. Diaconis, R. Graham, Universal cycles for combinatorial structures, *Discrete Mathematics*, 110 (1992) 43-59.

[5] C. Dalfó, M.A. Fiol, M. Miller, J. Ryan, J. Širáň, An algebraic approach to lifts of digraphs, *Discrete Applied Mathematics*, 269 (2019) 68-76.

[6] D. Gabric, J. Sawada, A. Williams, D. Wong, A successor rule framework for constructing k-ary de Bruijn sequences and universal cycles, *IEEE Transactions on Information Theory*, 66 (2020) 679-687.

[7] A.E. Holroyd, F. Ruskey, A. Williams, Shorthand universal cycles for permutations, *Algorithmica*, 64 (2012) 215-245.

[8] R. Horn, C. Johnson, *Matrix analysis*, Cambridge University Press, Cambridge, 2013.

[9] B. Jackson, Universal cycles of k-subsets and k-permutations, *Discrete Mathematics*, 117 (1993) 141-150.

[10] B. Jackson, B. Stevens, G. Hurlbert, Research problems on Gray codes and universal cycles, *Discrete Mathematics*, 309 (2009) 5341-5348.

[11] R. Johnson, Universal cycles for permutations, *Discrete Mathematics*, 309 (2009) 5264-5270.

[12] D.E. Knuth, *The Art of Computer Programming, Volume 4, Generating All Tuples and Permutations*, Fascicle 2, Addison-Wesley, 2005.

[13] F. Ruskey, A. Williams, An explicit universal cycle for the $(n-1)$-permutations of an n-set, *ACM Transactions on Algorithms*, 6-3 (2010) article 45: 1-12.

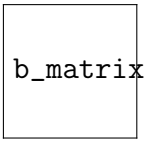
[14] J. Sawada, A. Williams, A Universal Cycle for Strings with Fixed-Content, In: Lubiw A., Salavatipour M., He M. (eds) Algorithms and Data Structures. WADS 2021. Lecture Notes in Computer Science, vol 12808. Springer, Cham.

[15] R. Sedgewick, Permutation Generation Methods, *Computing Surveys*, 9 (1977) 137-164.

[16] R.P. Stanley, *Algebraic Combinatorics*, Springer-Verlag, New York, 2013.

[17] D. Wong, A new universal cycle for permutations, *Graphs and Combinatorics*, 33 (2017) 1393-1399.

Appendix: transpose of the representation matrix T



Invited Talk: Sustainable and Multifunctional Wireless Networks

Christos Masouros

Dept. Electrical and Electronic Engineering, University College London

Abstract. The future global cellular infrastructure will underpin a variety of applications, such as smart city solutions, urban security, infrastructure monitoring, and smart mobility, among others. These emerging applications require new network functionalities that go beyond traditional communication. Key network KPIs for 6G include Gb/s data rates, cm-level localization, μs-level latency, and Tb/Joule energy efficiency. Additionally, future networks must support the UN's Sustainable Development Goals to ensure sustainability, net-zero emissions, resilience, and inclusivity. The multifunctionality and net-zero emissions agenda call for a redesign of multi-access technologies for 6G and beyond. In this talk, I focus on enabling multifunctionality in signals and wireless transmissions as a means of reducing hardware redundancy and minimizing carbon footprint. We will explore the emerging field of integrated sensing and communications (ISAC), which represents a paradigm shift towards combining sensing and communication functionalities within a single transmission, utilizing a single spectrum and ultimately sharing a common infrastructure.

Featured Talk: Bus Coding for Low-Power On-chip Interconnects

Wai Ho Mow

HongKong University of Science and Technology, Hong Kong, China

Abstract. Due to the recent drastic demand on AI accelerator hardware, novel very-large-scale (and even wafer-scale) circuit integration architectures, which may involve 3D stacking mutliple chiplets onto silicon interposers with sophisticated layer interconnections, have been introduced. The capacitive crosstalk of the on-chip bus interconnects induces high power consumption and limits data transmission speed. The classical solution of adding ground shielding is area-inefficient. One of the more area-efficient approaches, called bus coding, is to add one or a few redundant wires which send encoded signals in such a way that the overall latency and/or power consumption is reduced. The most famous single-redundancy-wire bus code is the bus invert code, which has been standardized and adopted in numerous inter-chip bus interconnects applications. In this talk, various known families of low-power bus codes will be surveyed. It will be pointed out that many known bus codes may actually increase, rather than decrease, overall power consumption, after the codec power consumption is taken into consideration. Lastly, our latest works on low-power bus codes, which can achieve the state-of-the-art overall power saving, will be presented.

Observations on NIST SP 800-90B Entropy Estimators

Melis Aslan
Middle East Technical University
Ankara, TURKEY
melisa@metu.edu.tr

Ali Doğanaksoy
Middle East Technical University
Ankara, TURKEY
aldoks@metu.edu.tr

Zülfükar Saygı
TOBB ETU
Ankara, TURKEY
zsaygi@etu.edu.tr

Meltem Sönmez Turan
National Institute of Standards and Technology
Gaithersburg, MD
meltem.turan@nist.gov

Fatih Sulak
Atilim University
Ankara, TURKEY
fatih.sulak@atilim.edu.tr

Abstract

Random numbers play a crucial role in cryptography, since security of cryptographic protocols relies on the assumption of availability of uniformly distributed and unpredictable random numbers to generate secret keys, nonces, salt, etc. However, real-world random number generators sometimes fail and produce outputs with low entropy, leading to security vulnerabilities. The NIST Special Publication (SP) 800-90 series provide guidelines and recommendations for generating random numbers for cryptographic applications and describes 10 black-box entropy estimation methods. This paper evaluates the effectiveness and limitations of the SP 800-90 methods by exploring the accuracy of these estimators using simulated random numbers with known entropy, investigating the correlation between entropy estimates, and studying the impacts of deterministic transformations on the estimators.

Keywords: cryptography, entropy estimation, min-entropy, randomness

1 Introduction

Random numbers are widely used in cryptographic protocols to generate secret keys, initialization vectors, nonces, salts, etc. The security of these protocols relies on the assumption that these numbers are generated uniformly at random and are unpredictable.

However, real-world random number generators sometimes fail and produce outputs with low entropy, leading to security vulnerabilities [1, 2].

A variety of organizations have developed standards and guidelines on generating random numbers that are suitable for cryptographic applications, such as the National Institute of Standards of Technology (NIST) [3, 4, 5, 6], the International Organization for Standardization (ISO) [7, 8, 9, 10], and Bundesamt für Sicherheit in der Informationstechnik (BSI) [11, 12, 13].

Cryptographic random number generators are typically composed of multiple components, including (i) a *noise source* that extracts randomness from physical phenomena (e.g., thermal noise, mouse movements, radioactive decay, free-running oscillator) to generate a *seed* and (ii) a *pseudorandom number generator* (PRNG) (also known as a *deterministic random bit generator*) that extends the seed to generate a long random-looking sequence. Since PRNGs are deterministic, the entropy is solely provided by the noise source, and it is important to measure the unpredictability of the noise source outputs.

Various statistical randomness tests can be applied to measure the quality of the random numbers. The most commonly used statistical randomness suites are TestU01 [14], DIEHARD [15], DIEHARDER [16], and NIST Special Publication (SP) 800-22 Rev.1 [17]. These tests may not be suitable for assessing noise source outputs, as they typically have strong biases and would fail these tests.

The unpredictability of noise source outputs is measured using *entropy*, and two commonly used measures of entropy are *Shannon entropy* and *min-entropy*. *Min-entropy* is a more conservative measure, which is based on the probability of guessing the most-likely output of a randomness source.

Estimating the entropy of noise source outputs is challenging, because the distribution of the output values is generally unknown. The BSI standards require stochastic modeling of the noise source to specify a family of probability distributions to estimate entropy. Since stochastic modeling may not be possible or practical due to the diversity and complexity of the random number generators, NIST standards allow using black-box statistical methods for entropy estimation.

SP 800-90B [4] describes ten entropy estimators: most common value, collision, Markov, compression, t-tuple, longest repeated substring (LRS), multi most common in window prediction, lag prediction, multiple Markov Model with Counting (multiMMC) prediction, and LZ78Y. The minimum of these ten estimates is used to estimate the min-entropy of the noise source outputs.

Related work. Zhu et al. [18] showed that the collision and compression estimates provide significant underestimates and proposed a new estimator that achieves better accuracy for min-entropy. Kim et al. [19] also showed that the compression estimate underestimates min-entropy and proposed two kinds of min-entropy estimators to improve computational complexity and estimation accuracy by leveraging two variations of Maurer's test. Hill [20] demonstrated that the collision and compression estimators incorrectly use the central limit theorem. Hill [20] also claimed that the Markov estimator should not be directly compared to other estimators since it does not use confidence intervals during estimation. Additionally, Turan et al. [21] provided a correlation and sensitivity analysis of statistical randomness tests.

Contributions. This paper evaluates the accuracy, effectiveness, and limitations of the SP 800-90B estimators using simulated random numbers with known entropy, investigates the correlation between entropy estimates, and studies the impacts of deterministic transformations on the estimators.

Organization. Section 2 provides preliminaries on SP 800-90B entropy estimation and overviews of two correlation metrics. Section 3 describes the paper's methodology. Section 4 presents experimental results and discussion.

2 Preliminaries

2.1 Min-Entropy

In information theory, entropy is a measure of uncertainty associated with the outcomes of a random variable. There are different measures of entropy, and NIST SP 800-90B [4] uses *min-entropy*, which is a conservative entropy measurement based on the probability of guessing the most likely output of a randomness source.

Definition 1. Let $\mathcal{X}$ be a random variable that takes values from the set $A = \{x_1, x_2, \ldots, x_n\}$ with probabilities $Pr(\mathcal{X} = x_i) = p_i$ for $i = 1, 2, \ldots, n$. The *min-entropy* of the random variable $\mathcal{X}$ is defined as

$$\begin{aligned} H_\infty &= \min_{1 \le i \le n} (-\log_2 p_i) \\ &= -\log_2 (\max_{1 \le i \le n} p_i). \end{aligned}$$

The random variable $\mathcal{X}$ is said to have min-entropy h if the probability of observing any particular value for $\mathcal{X}$ is at most 2^{-h}. When the random variable has a uniform probability distribution (i.e., $p_1 = p_2 = \cdots = p_n = 1/n$), the variable has the maximum possible value for the min-entropy, which is $\log_2 n$.

In the following chapters of this paper, *entropy* refers to *min-entropy*.

2.2 Entropy Estimation Based on SP 800-90B

SP 800-90B [4] describes an *entropy source* model, that is composed of a noise source, health tests, and an optional conditioning function. The standard also provides guidelines for the generation of random numbers using entropy sources and specifies entropy estimation techniques to ensure the randomness and unpredictability of the outputs. These black-box techniques are applied to noise source outputs and are independent of the internals of the noise source.

SP 800-90B [4] defines two tracks to estimate the min-entropy of an entropy source: independent and identically distributed (IID) and non-IID. To determine which track to use, a number of statistical tests are applied to an output sequence generated by the entropy source to check the IID assumption. If the output sequence passes these tests, the source is assumed to generate IID outputs, and only the most common value method is used to estimate the entropy. Otherwise, the source is assumed to generate non-IID

outputs, and the minimum of the 10 SP 800-90B estimators is used to estimate the entropy of the source. Table 1 lists the estimators and corresponding metrics provided in the standard. Except for collision, Markov, and compression, the estimators provide support for non-binary noise source outputs.

The estimators take noise source outputs $S = (s_1, s_2, \ldots, s_L)$, where $s_i \in A = \{x_1, x_2, \ldots, x_n\}$, and return a min-entropy estimate between 0 and $\log_2 n$. The collision, Markov, and compression estimators are only defined for binary inputs (i.e., $n = 2$). To establish the final entropy estimate, the standard considers the entropy estimate from the designers and the impact of the conditioning components. This study focuses on the black-box estimators, and the additional considerations — including IID testing — are outside of the scope of this study.

Table 1: Entropy estimators of NIST SP 800-90B

Estimator	*Metric*	Support for $n > 2$?
Most Common Value	Proportion of the most common value in the input data set	✓
Collision	Probability of the most-likely output, depending on the number of collisions	×
Markov	Dependencies between consecutive values	×
Compression	Compression amount of the input dataset	×
t-Tuple	Frequency of t-tuples	✓
Longest Repeated Substring (LRS)	Number of repeated substrings	✓
Multi Most Common in Window Prediction	Number of correct predictions based on the most common value	✓
Lag Prediction	Number of correct predictions based on periodicity	✓
MultiMMC Prediction	Number of correct predictions based on multiple Markov models	✓
LZ78Y Prediction	Number of correct predictions based on a dictionary constructed using observed tuples	✓

2.3 Correlation Analysis

The Pearson [22] and Spearman [23] correlation coefficients are commonly used metrics to measure the correlation between two random variables. The correlation coefficients take values between -1 and 1. A value close to 1 or -1 shows a strong positive or negative association between variables, whereas a value close to 0 shows a weak association. The Pearson correlation [22] measures the strength of a linear relationship between two random variables, assuming that the variables are distributed normally, whereas the Spearman correlation [23] describes the monotonic relationship between variables without the assumption that the variables have normal distribution.

Definition 2. Let $\mathcal{X}$ and $\mathcal{Y}$ be random variables. The Pearson correlation coefficient r

between a given paired dataset $\{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\}$ is defined as

$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}},$$

where n is the sample size, x_i and y_i are sample points, $\bar{x}$ is the sample mean of $\mathcal{X}$, and $\bar{y}$ is the sample mean of $\mathcal{Y}$.

Definition 3. Let $\mathcal{X}$ and $\mathcal{Y}$ be random variables. The Spearman correlation coefficient ρ between a given paired dataset $\{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\}$ is defined as

$$\rho = 1 - \frac{6\sum_{i=1}^{n} d_i^2}{n(n^2 - 1)},$$

where n is the sample size, and d_i is the difference between the rank of the paired samples.

3 Methodology

The goal of this study is to answer the following questions regarding the entropy estimators introduced in SP 800-90B [4]:

1. *How closely do the entropy estimators match the true entropy of the source?*
2. *How correlated are the entropy estimators?*
3. *How do different deterministic transformations impact the entropy estimate?*

3.1 Entropy Estimation using Known Distributions

One approach to understanding the accuracy of the entropy estimators is to simulate various sequences with known probability distributions (hence, known entropy), and check the difference between the estimated entropy and the true entropy. In cases where certain entropy estimators consistently yield outlier results compared to others, it is important to investigate the underlying reasons for such discrepancies. This could involve examining the specific characteristics of the input data, inherent biases in the estimation techniques, or the impacts of using different input lengths and sample sizes.

3.2 Correlation of the Entropy Estimators

Understanding the correlation between different entropy estimators can provide insights into the reliability, robustness, and limitations of the estimators for cryptographic applications. One aspect to consider is the agreement between different entropy estimation methods by assessing whether they tend to produce similar entropy estimates for the same set of input sequences. This study employed correlation analysis to quantify the relationship between pairs of entropy estimates and used the Pearson and Spearman correlation coefficients.

3.3 Impact of Deterministic Transformations

The noise source outputs are typically processed using deterministic conditioning functions to reduce their statistical bias and improve their entropy rate (i.e., entropy per bit). The impacts of a number of deterministic transformations that are applied to the output sequence are of interest here.

Let $S = (s_1, s_2, \ldots, s_L)$ be a noise source output with length L, and let $S' = (s'_1, s'_2, \ldots, s'_L)$ be generated from S via a deterministic transformation. This study uses the following transformations:

- **Reverse:** This transformation generates a new sequence by changing the order of the sequence. The generated sequence $S' = (s_L, s_{L-1}, \ldots, s_2, s_1)$ is constructed with $s'_i = s_{L-i+1}$ for each $i = 1, 2, \ldots, L$. For example, the reversed sequence of $S = (\texttt{10110001110010})$ is $S' = (\texttt{01001110001101})$.

- **Binary Derivative:** This transformation generates a new sequence by XORing (i.e., modulo 2 addition) the consecutive bits of the sequence. The generated sequence $S' = (s'_1, s'_2, \ldots, s'_L)$ is constructed with

$$s'_i = \begin{cases} s_i \oplus s_{i+1}, & i = 1, 2, \ldots, L-1, \\ s_1, & i = L. \end{cases}$$

  For example, the binary derivative of $S = (\texttt{10110001110010})$ is $S' = (\texttt{11010010010111})$.

- ***t*-Rotation:** This transformation applies a t-bit rotation to the input sequence, i.e., t-bit rotation of $S = (s_1, s_2, \ldots, s_L)$ is $S' = (s_{t+1}, s_{t+2}, \ldots, s_L, s_1, s_2, \ldots, s_t)$, where $t = 16, 64, 128$, or 1024. For example, 2-bit rotation of $S = (\texttt{101100011100 10})$ is $S' = (\texttt{11000111001010})$.

4 Experimental Results

4.1 Simulated Datasets

The following datasets with known entropy were simulated for the experiments:

1. **Uniform distribution with full entropy.** The datasets are generated using the Cipher Block Chaining (CBC) mode of the block cipher Advanced Encryption Standard (AES) [24]. Sequences are generated for three different sample sizes (i.e., the size of the noise source output): binary, 4-bit, and 8-bit. For each sample size, 1000 sequences of length 1 000 000 were generated. In these sequences, all outputs are assumed to have an equal probability of occurring, and are independent. Hence, the outputs have full entropy.

2. **Biased binary distribution with entropy=0.5.** The dataset follows a biased binary distribution, where the probability of observing a 0 is 0.7, and the probability of observing a 1 is 0.3. For each sample size, 1000 sequences of length 1 000 000 were

generated. In these sequences, the expected entropy of a sequence is 0.5 per bit. This data is generated using the random number generator Mersenne Twister (MT19937) in `C++`.

3. **4-bit near-uniform with entropy=0.5.** This dataset follows a 4-bit near-uniform distribution, where the probability of observing the template `0000` is 0.25, and the probability of observing other 4-bit templates is 0.05. For each sample size, 1000 sequences of length 1 000 000 were generated. In these sequences, the expected entropy of a sequence is 0.5 per bit. This data is generated using the random number generator in `C++`.

4. **8-bit near-uniform with entropy=0.5.** This dataset follows an 8-bit near-uniform distribution, where the probability of observing the template `00000000` is 0.06, and the probability of observing other 8-bit templates is 0.003686. For each sample size, 1000 sequences of length 1 000 000 were generated. In these sequences, the expected entropy of a sequence is 0.5 per bit. This data is generated using the random number generator in `C++`.

4.2 Accuracy of Entropy Estimators

Table 2 compares the actual and estimated entropy values for binary, 4-bit, and 8-bit uniformly distributed data with full entropy. It shows that compression and collision estimates produce the smallest estimates for binary data, which is consistent with the findings of Zhu et al. [18] and Kim et al. [19]. Figure 1 in Appendix shows the distribution of the entropy estimation, and compression, and LRS estimators seem to show high variation compared to other estimators.

Table 2: Mean and standard deviation of entropy estimators for binary, 4-bit, and 8-bit sources with full entropy

	1-bit		**4-bit**			**8-bit**		
	Mean	**Std. Dev.**	**Mean**	**Mean/bit**	**Std. Dev.**	**Mean**	**Mean/bit**	**Std. Dev.**
MCV	0.9951	0.0009	3.9514	0.9879	0.0056	7.6736	0.9592	0.0222
Collision	0.9141	0.0194	*	*	*	*	*	*
Markov	0.9982	0.0011	*	*	*	*	*	*
Compression	0.8535	0.0287	*	*	*	*	*	*
t-Tuple	0.9294	0.0104	3.7799	0.9450	0.0149	7.6736	0.9592	0.0222
LRS	0.9785	0.0262	3.8928	0.9732	0.1131	7.7468	0.9683	0.1878
Multi MCW	0.9954	0.0114	3.9635	0.9909	0.0662	7.8169	0.9771	0.1315
Lag Prediction	0.9957	0.0072	3.9677	0.9919	0.0416	7.8116	0.9764	0.1679
MultiMMC	0.9951	0.0129	3.9616	0.9904	0.0778	7.8197	0.9775	0.1302
LZ78Y	0.9956	0.0096	3.9616	0.9904	0.0778	7.8198	0.9775	0.1302

The same experiments were repeated for biased binary distribution, 4-bit near-uniform distribution, and 8-bit near-uniform distribution, and the results are summarized in Table 3. Similar to uniform distribution, the compression estimate underestimates entropy for biased distributions. However, LRS and lag prediction overestimate the entropy by approximately 50%. Similar results were obtained for 4-bit and 8-bit samples.

Table 3: Mean and standard deviation of entropy estimators of datasets for biased binary, 4-bit near-uniform, and 8-bit near-uniform distributions

	Biased Binary Dist.		**4-bit Near-uniform**			**8-bit Near-uniform**		
	Mean	**Std. Dev.**	**Mean**	**Mean/bit**	**Std. Dev.**	**Mean**	**Mean/bit**	**Std. Dev.**
MCV	0.5122	0.0009	1.9872	0.4968	0.0050	4.0169	0.5021	0.0160
Collision	0.5095	0.0020	*	*	*	*	*	*
Markov	0.5146	0.0011	*	*	*	*	*	*
Compression	0.3224	0.0009	*	*	*	*	*	*
t-Tuple	0.5031	0.0116	1.9710	0.4928	0.0197	3.9993	0.4999	0.0380
LRS	0.7692	0.0205	3.2364	0.8091	0.0954	6.9466	0.8683	0.1884
Multi MCW	0.5121	0.0055	1.9860	0.4965	0.0200	4.0063	0.5008	0.0738
Lag Prediction	0.7756	0.0263	3.2812	0.8203	0.0923	6.9558	0.8695	0.2984
MultiMMC	0.5118	0.0055	1.9861	0.4965	0.0200	4.1557	0.5195	0.1028
LZ78Y	0.5118	0.0055	1.9860	0.4965	0.0200	4.1556	0.5194	0.1027

4.3 Correlations of Estimators

The Pearson and Spearman coefficients were used to measure the correlation between entropy estimators. Using 200 binary sequences of length 1 000 000, Table 4 and Table 5 show the Pearson and Spearman correlations among different estimators, respectively. According to Table 4, a strong or moderate correlation was observed for the (MCV, Markov), (MultiMCW, MultiMMC) (MultiMMC, LZ78Y), and (MultiMCW, LZ78Y) estimators using Pearson's metric. When the same experiments were conducted using Spearman's metric, a correlation was still observed between (MCV, Markov). However, (MultiMMC, LZ78Y) and (MultiMCW, LZ78Y) correlations were no longer as strong. Additionally, the correlation between (Markov, LZ78Y) was observed to be strong for Spearman's metric.

Table 4: Pearson correlation among different estimators for uniform distribution with full entropy

	MCV	**Collision**	**Markov**	**Compression**	**t-Tuple**	**LRS**	**MultiMCW**	**Lag Prediction**	**MultiMMC**	**LZ78Y**
MCV	1.0000	-0.0531	**0.5338**	-0.1170	0.0564	-0.0506	0.0535	-0.0745	0.2174	0.2610
Collision		1.0000	0.1315	-0.0092	0.0163	0.0563	0.0071	-0.0281	-0.0286	-0.0856
Markov			1.0000	0.0347	0.0821	-0.0158	0.0261	-0.0581	0.1767	0.2278
Compression				1.0000	-0.0422	0.0284	0.0281	-0.0011	0.1094	0.0756
t-Tuple					1.0000	0.0388	0.0444	0.0583	0.0760	0.0765
LRS						1.0000	-0.0449	0.0059	-0.0557	-0.0505
MultiMCW							1.0000	-0.0063	**0.4702**	**0.8063**
Lag Prediction								1.0000	-0.0363	-0.0281
MultiMMC									1.0000	**0.4693**
LZ78Y										1.0000

Table 5: Spearman correlation among different estimators for uniform distribution with full entropy

	MCV	**Collision**	**Markov**	**Compression**	**t-Tuple**	**LRS**	**MultiMCW**	**Lag Prediction**	**MultiMMC**	**LZ78Y**
MCV	1.0000	-0.0426	**0.5410**	-0.1012	0.0636	-0.0317	-0.0601	0.0314	0.1825	0.4991
Collision		1.0000	0.1224	0.0282	0.0254	0.0035	0.0140	0.0009	0.0017	-0.1207
Markov			1.0000	0.0491	0.0954	-0.0215	-0.0454	0.0510	0.1784	**0.6420**
Compression				1.0000	0.0138	0.1014	0.0202	0.0200	0.1711	0.1143
t-Tuple					1.0000	0.0714	-0.0104	-0.0789	0.0316	0.0575
LRS						1.0000	0.0396	-0.0641	0.0187	0.0008
MultiMCW							1.0000	-0.0593	0.0784	-0.1028
Lag Prediction								1.0000	0.0178	0.1391
MultiMMC									1.0000	0.1982
LZ78Y										1.0000

4.4 Impact of the Transformations

For this experiment, 200 uniformly distributed sequences of length 1 000 000 with full entropy were used. These sequences were transformed using a reversing, binary derivative and t-rotation for $t = 16, 64, 128, 1024$. Entropy estimates for the original and transformed sequences were compared, and their Pearson and Spearman correlation coefficients are listed in the Table 6 and Table 7, respectively. Reversing and rotating the input sequences did not have any impact on its entropy estimation for the MCV, collision, Markov, t-tuple, and LRS estimators (hence, the same estimate is obtained) for either of the correlation metrics. Among different transformations, binary derivative seems to have the highest impact on the prediction based estimates, namely multiMCW, Lag, multiMMC and LZ78Y.

Table 6: Pearson Correlation according to the estimation results of transformed sequences

	Original	**Reversed**	**Bin. Drv.**	**16-rot.**	**64-rot.**	**128-rot.**	**1024-rot.**
MCV	1.0000	1.0000	-0.0289	1.0000	1.0000	1.0000	1.0000
Collision	1.0000	1.0000	-0.0160	1.0000	1.0000	1.0000	1.0000
Markov	1.0000	1.0000	0.4586	1.0000	1.0000	1.0000	1.0000
Compression	1.0000	0.3334	0.4887	0.3379	0.3374	0.3927	0.3368
t-Tuple	1.0000	1.0000	0.1144	1.0000	1.0000	1.0000	1.0000
LRS	1.0000	1.0000	0.7013	1.0000	1.0000	1.0000	1.0000
Multi MCW	1.0000	0.1301	0.8455	0.9999	0.9998	0.9997	0.9994
Lag Prediction	1.0000	0.1492	0.0037	0.9983	0.9971	0.9962	0.9915
MultiMMC	1.0000	0.0564	-0.0189	0.9977	0.9962	0.9962	0.8329
LZ78Y	1.0000	0.0598	0.1510	0.9961	0.9927	0.9918	0.9738

Table 7: Spearman Correlation according to the estimation results of transformed sequences

	Original	**Reversed**	**Bin. Drv.**	**16-rot.**	**64-rot.**	**128-rot.**	**1024-rot.**
MCV	1.0000	1.0000	-0.0432	1.0000	1.0000	1.0000	1.0000
Collision	1.0000	1.0000	0.0565	1.0000	1.0000	1.0000	1.0000
Markov	1.0000	1.0000	0.4030	1.0000	1.0000	1.0000	1.0000
Compression	1.0000	0.3090	0.5283	0.3053	0.3053	0.3685	0.3094
t-Tuple	1.0000	1.0000	0.0964	1.0000	1.0000	1.0000	1.0000
LRS	1.0000	1.0000	0.5425	1.0000	1.0000	1.0000	1.0000
Multi MCW	1.0000	0.8795	0.0170	0.9975	0.9954	0.9947	0.9869
Lag Prediction	1.0000	0.3607	-0.0282	0.9822	0.9717	0.9603	0.9219
MultiMMC	1.0000	0.3762	0.2872	0.9162	0.8772	0.8770	0.6943
LZ78Y	1.0000	0.6069	0.3580	0.9941	0.9884	0.9867	0.9530

5 Discussion

In this paper, we studied the black-box entropy estimators described in NIST SP 800-90B. We observed that compression and collision estimates both underestimate the entropy both for uniform and biased distributions, which is consistent with the findings of Zhu

et al. [18] and Kim et al. [19]. The remaining estimates are close to the true entropy for the uniform distribution. However, LRS and lag prediction overestimate entropy for binary, 4-bit, and 8-bit sequences for biased distributions. Understanding the reasons for this gap based on the details of the estimators is planned for future work.

These experiments show a strong correlation between the Markov and MCV tests for uniform distribution. Additionally, we observed that taking binary derivation significantly changes the entropy estimates, especially for prediction-based estimators.

We expect the provided results to help improve the accuracy of NIST's entropy estimation strategy and promote similar studies to consider the impacts of commonly used conditioning or post-processing functions.

Acknowledgements

The authors thank Sevim Seda Odacıoğlu for her contributions on implementations of the estimators.

References

[1] Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. Mining your ps and qs: detection of widespread weak keys in network devices. In *Proceedings of the 21st USENIX Conference on Security Symposium*, Security'12, page 35, USA, 2012. USENIX Association.

[2] Daniel J. Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou, Nadia Heninger, Tanja Lange, and Nicko van Someren. Factoring rsa keys from certified smart cards: Coppersmith in the wild. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013*, pages 341–360, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[3] Elaine B. Barker and John M. Kelsey. SP 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators. Technical report, National Institute of Standards and Technology, June 2015.

[4] Meltem Sönmez Turan, Elaine B. Barker, John M. Kelsey, Kerry A. McKay, Mary L. Baish, and Michael Boyle. SP 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation. Technical report, National Institute of Standards and Technology, January 2018.

[5] Elaine B. Barker, John M. Kelsey, Kerry A. McKay, Allen Roginsky, and Meltem Sönmez Turan. SP 800 90C Recommendation for Random Bit Generator (RBG) Constructions (3rd Draft). Technical report, National Institute of Standards and Technology, September 2022.

[6] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, N. Heckert, James Dray, San

Vo, and Lawrence Bassham. SP 800-22 Rev. 1a A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Technical report, National Institute of Standards and Technology, 2010.

[7] ISO Central Secretary. ISO/IEC 19790:2012 Information technology — Security techniques — Security requirements for cryptographic modules. Standard ISO/IEC 19790:2012, International Organization for Standardization, Geneva, CH, 2012.

[8] ISO Central Secretary. ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model. Standard ISO/IEC 15408-1:2009, International Organization for Standardization, Geneva, CH, 2015.

[9] ISO Central Secretary. ISO/IEC 18031:2011 Information technology — Security techniques — Random bit generation. Standard ISO/IEC 18031:2011, International Organization for Standardization, Geneva, CH, 2011.

[10] ISO Central Secretary. Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408. Standard ISO/IEC 20543:2019, International Organization for Standardization, Geneva, CH, 2019.

[11] AIS 20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren (Version 3). Report, Bundesamt für Sicherheit in der Informationstechnik (BSI), May 2013.

[12] AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren (Version 3). Report, Bundesamt für Sicherheit in der Informationstechnik (BSI), May 2013.

[13] Matthias Peter and Werner Schindler. A Proposal for Functionality Classes for Random Number Generators (Version 2.35, DRAFT) . Report, Bundesamt für Sicherheit in der Informationstechnik (BSI), September 2022.

[14] P. L'Ecuyer and R. Simard. Testu01: A c library for empirical testing of random number generators, 2007.

[15] G. Marsaglia. The marsaglia random number cdrom including the diehard battery of tests of randomness, 1996.

[16] R. G. Brown. Dieharder: A random number test suite, 2013.

[17] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, M. L. Stefan Leigh, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo. A statistical test suite for random and pseudo random number generators for cryptographic applications, 2001.

[18] Shuangyi Zhu, Yuan Ma, Tianyu Chen, Jingqiang Lin, and JiwuJing. Analysis and improvement of entropy estimatorsin nist sp 800-90b for non-iid entropysources. *IACR Transactions on Symmetric Cryptology*, 2017(3):151–168, 2017.

[19] Yongjune Kim, Cyril Guyot, and Young-Sik Kim. On the efficient estimation of min-entropy. *IEEE Transactions on Information Forensics and Security*, 16:3013–3025, 2021.

[20] Joshua E. Hill. SP 800-90B Refinements: Validation Process, Estimator Confidence Intervals, and Assessment Stability. ICMC, 2020.

[21] M. Sönmez Turan, A. Doganaksoy, and S. Boztas. On independence and sensitivity of statistical randomness tests. *In International Conference on Sequences and Their Applications (SETA)*, 2008.

[22] K. Pearson and Galton Laboratory for National Eugenics. *"Note on Regression and Inheritance in the Case of Two Parents".* Proceedings of the Royal Society. Royal Society, 1895.

[23] C. Spearman. The proof and measurement of association between two things. *American Journal of Psychology*, 15:88–103, 1904.

[24] Morris Dworkin, Nicky Mouha, and Meltem Sönmez Turan. Advanced Encryption Standard (AES). *Federal Inf. Process. Stds. (NIST FIPS) 197, National Institute of Standards and Technology, Gaithersburg, MD*, 2001 (updated 2023).

Appendix

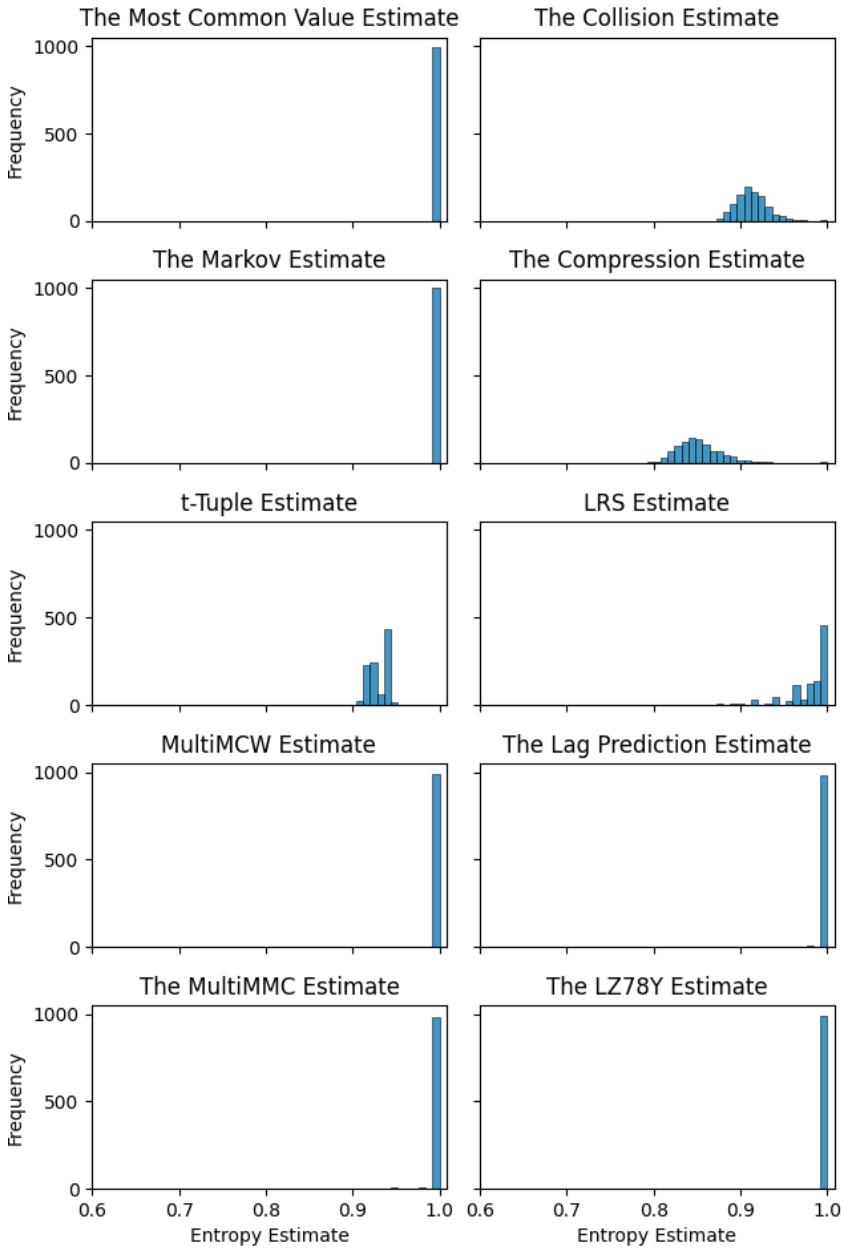


Figure 1: Distribution of entropy estimates for full-entropy binary inputs

Two Pattern Properties of Binary Sequences Invariant under the Continued Fraction Operator K (the Berlekamp-Massey Algorithm)

Mónica del P. Canales Chacón
MATEMATICVM, @matematicvm, Valdivia, Chile
monicadelpilar@gmail.com

Sergio Jara Ceballos
Universidad Austral de Chile, Facultad de Ingeniería, Valdivia, Chile
serjara.ing.mat@gmail.com

Michael Vielhaber
HS Bremerhaven, FB 2, Bremerhaven, Germany
vielhaber@gmail.com

Abstract

We show that a binary sequence $s = (s_1, s_2, \dots) \in \{0,1\}^\omega$ which is zero outside some arithmetic progression (residue class) $[r]_n$, *i.e.* $\mathrm{supp}(s) \subset [r]_n$, maintains this property under forward and backward iteration of the continued fraction operator $\mathbf{K}$: We still have $\mathrm{supp}(\mathbf{K}^u(s)) \subset [r]_n$ for all $u \in \mathbb{Z}$.

The isometry $\mathbf{K}$ implements the Berlekamp-Massey Algorithm in such a way that $\mathbf{K}(s)$ is the discrepancy sequence of s and at the same time is the sequence of encodings of the partial denominators of the continued fraction expansion of $G(s) = \sum_{k\in\mathbb{N}} s_k x^{-k} \in \mathbb{F}_2[[x^{-1}]]$.

Furthermore, the property $s_{2n-1} = s_{2n}, \forall n \in \mathbb{N}$ is maintained under $\mathbf{K}^u, u \in \mathbb{Z}$.

Keywords: Berlekamp-Massey Algorithm, Invariance under the BMA, linear complexity, sequences with restricted support.

Notation:
$\mathbb{N} = \{1, 2, 3, \dots\}$, $A = \{0, 1\}$ is the binary alphabet
0/1-inversion: $\overline{0} = 1,\ \overline{1} = 0,\ \overline{10011} = 01100$
$A^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \dots\}$ and A^ω are the finite, resp. infinite words over A

1 Introduction

The continued fraction operator **K** is a modification of the well-known Berlekamp-Massey Algorithm (BMA). **K** delivers the linear complexity profile and computes the discrepancy sequence in such a way that it *is* immediately an encoding of the partial denominators (PD) of the binary sequence interpreted as formal power series.

We show that this operator **K**, an isometry on A^ω, with $A = \{0, 1\}$, has the property that sequences s whose support (indices $i \in \mathbb{N}$ with $s_i \neq 0$) lies within some residue class $i \equiv r \mod n$, $\mathrm{supp}(s) \subset [r]_n$, are mapped to sequences $\mathbf{K}^u(s)$, which again satisfy $\mathrm{supp}(\mathbf{K}^u(s)) \subset [r]_n$, and this is valid for any number $u \in \mathbb{Z}$ of iterations.

We shall also see that the property $s_{2n-1} = s_{2n}, \forall n \in \mathbb{N}$, *i.e.* all 0s and 1s appear in pairs or runs of even length, is preserved by $\mathbf{K}^u(s), u \in \mathbb{Z}$ as well.

2 Continued Fractions, Partial Denominators, the Berlekamp-Massey-Algorithm, and the Isometry K

The usual way to compute the continued fraction expansion (CFE) of a formal power series $s := \sum_{k\in\mathbb{N}} s_k x^{-k} \in \mathbb{F}_2[[x^{-1}]]$ starts with $s^{(0)} := s, b_0 := 0$ and then iteratively sets

$$\forall i \in \mathbb{N}\colon\ s^{(i)} := \frac{1}{\{s^{(i-1)}\}} = \frac{1}{s^{(i-1)} - b_{i-1}}, b_i := \lfloor s^{(i)} \rfloor, \text{ yielding } s = 0 + \frac{1\,|}{|b_1} + \frac{1\,|}{|b_2} + \cdots,$$

where $s^{(i)} \in \mathbb{F}_2((x^{-1}))$ has positive degree for $i \in \mathbb{N}$, the floor function $\lfloor s^{(i)} \rfloor$ gives the polynomial part $b_i \in \mathbb{F}_2[x]$ as partial denominator (PD), and we have $\{s^{(i)}\} \in \mathbb{F}_2[[x^{-1}]]$. We also denote the CFE by $s = [b_1, b_2, b_3, \dots]$.

The convergents $A_i/B_i \in \mathbb{F}_2(x)$ to s are obtained via Perron's [13] schema, see Table 1. We use the Thue-Morse sequence $s = 01101001\dots$ (see [1]) with $G(s) = \frac{1\ \ |}{|x^2+x+1} + \frac{1\ \ |}{|x^2+1} + \frac{1\,|}{|x^2} + \cdots$ as example ($b_0 = 0$ is omitted).

i	-1	0	1	2	3	4	$\dots$
b_i			x^2+x+1	x^2+1	x^2	x^2+1	$\dots$
A_i	1	0	1	x^2+1	x^4+x^2+1	x^6+x^2	$\dots$
B_i	0	1	x^2+x+1	x^4+x^3+x	$x^6+x^5+x^3+x^2+x+1$	$x^8+x^7+x^6+x^3+1$	$\dots$

Table 1: Schema for PDs $b_i \in \mathbb{F}_2[x]$ and convergents $A_i/B_i \in \mathbb{F}_2(x)$.

The initial values are $A_{-1} = B_0 = 1$, $B_{-1} = A_0 = 0$ as in the real case, and then $A_i := b_i \cdot A_{i-1} + A_{i-2}$, $B_i := b_i \cdot B_{i-1} + B_{i-2}$. Setting $r := A_i/B_i$ (a rational, *i.e.* ultimately periodic sequence), we have $r_k = s_k$ at least for $1 \le k \le \deg(B_i) + \deg(B_{i-1})$.

The continued fraction expansion and thereby the linear complexity profile is readily computed by the well-known Berlekamp-Massey-Algorithm (BMA).

In order to read off the PDs directly from the discrepancy sequence (d_k) – any sequence with $d_k = 0$, whenever the previous approximation also generates the current sequence

bit s_k, and $d_k = 1$ otherwise –, we have to make 3 simple, but crucial adjustments to the Berlekamp-Massey algorithm, as given by Dornstetter [4]:
1. Start with the convergents $A_{-1}/B_{-1} = 1/0$ and $A_0/B_0 = 0/1$.
2. Use the feedback polynomial, not its reciprocal, the connection polynomial.
3. Do not normalize the polynomials (this has an effect only for char $\mathbb{F}_p \geq 3$).

Only then, the resulting isometry $\mathbf{K}$ satisfies the observations on the support described in this paper. $\mathbf{K}$ is obtained as composition of three functions (see [15]),

$$\mathbf{K}\colon \text{sequence} \overset{G}{\longmapsto} \text{formal power series} \overset{\mathcal{K}}{\longmapsto} \text{continued fraction expansion} \overset{\pi^\infty}{\longmapsto} \text{discrepancy seq.}$$

We first treat the case of irrational that is aperiodic sequences:

$$\mathbb{F}_2^\omega \ni s \overset{G}{\longmapsto} G(s,x) = \sum_{k=1}^{\infty} s_k x^{-k} \in \mathbb{F}_2[[x^{-1}]]$$

$$G(s,x) = \frac{1}{|b_1(x)} + \frac{1}{|b_2(x)} + \frac{1}{|b_3(x)} + \cdots \overset{\mathcal{K}}{\longmapsto} (b_1, b_2, b_3, \dots) \in (\mathbb{F}_2[x]\backslash\mathbb{F}_2)^\omega$$

$$(b_i)_{i=1}^{\infty} \overset{\pi^\infty}{\longmapsto} \pi(b_1)\pi(b_2)\pi(b_3)\ldots = \mathbf{K}(s) \in \mathbb{F}_2^\omega,$$

where

$$\pi\colon \mathbb{F}_2[x]\backslash\mathbb{F}_2 \ni p(x) = \sum_{k=0}^{g} a_k x^k \mapsto \pi(p) = 0^{g-1} a_g \ldots a_1 a_0 \in \Pi_2$$

and

$$\Pi_2 := \{(a_1, \dots, a_n) \in \mathbb{F}_2^* \mid \exists g \in \mathbb{N} : n = 2g, a_1 = \cdots = a_{g-1} = 0, a_g \neq 0\}$$

is the set of polynomial encodings. $\Pi_2 \cup 0^\omega$ is a complete prefix code.

In the rational case, the CFE of $G(s)$ has only finitely many PDs and thus
$s \overset{G}{\longmapsto} G(s) = 0 + \frac{1}{|b_1(x)} + \cdots + \frac{1}{|b_n(x)} \overset{\mathcal{K}}{\longmapsto} (b_1, \dots, b_n) \in (\mathbb{F}_2[x]\backslash\mathbb{F}_2)^* \overset{\pi^\infty}{\longmapsto} \pi(b_1)\ldots\pi(b_n)0^\omega$
$= \mathbf{K}(s) \in \mathbb{F}_2^\omega$, including $\mathbf{K}(0^\omega) = 0^\omega$ with the empty tuple from $(\mathbb{F}_2[x]\backslash\mathbb{F}_2)^*$.

$\mathbf{K}$ is an isometry on $\mathbb{F}_2^\omega$, see [15, Thm. 5], and we have the following connection to the linear complexity: Let n_0 be the position (in s and $\mathbf{K}(s)$) at the end of an encoding $\pi(b_{i-1})$, $n_1 = n_0 + g$ the position of the leading coefficient a_g in $\pi(b_i)$, where $g = \deg(b_i)$ and $n_2 = n_1 + g = n_0 + 2g$ is the position of the constant term a_0 of b_i. At position n_1 the linear complexity jumps from $n_0/2$ to $n_2/2$ that is by $g = \deg(b_i)$ and remains otherwise constant within the positions of the encoding $\pi(b_i)$. The linear complexity deviation $L(n) - n/2$ is negative from position $n_0 + 1$ to $n_1 - 1$, it is positive afterwards until $n_2 - 1$ and zero in n_2 as well as in n_0 and in general at the end of every encoding π.

Lemma 1. *The linear complexity is*

$$L(n) = \begin{cases} n_0/2 \\ n_0/2 \\ n_0/2 + g \\ n_2/2 \\ n_2/2 \end{cases} = n/2 + \begin{cases} 0, & n = n_0, \\ -(n - n_0)/2, & n_0 < n < n_1, \\ g/2, & n = n_1, \\ +(n_2 - n)/2, & n_1 < n < n_2, \\ 0, & n = n_2. \end{cases}$$

Proof. See Theorem 6 and Proposition 8 in [15]. □

K is a discrepancy sequence for s since from n_0 to $n_1 - 1$ it is zero, no adjustment of the LFSR length is necessary, at n_1 it is nonzero, and the linear complexity / LFSR length increases by g. From n_1 to n_2, with $L \geq n/2$, no change in the LFSR length will take place.

The implementations of the BMA by Massey [9], by Lidl/Niederreiter [8], and the BMA* by Dornstetter [4] / Vielhaber [15] are pairwise different in the part $a_{g-1} \ldots a_1 a_0$ between n_1 and n_2, but all coincide (of course) in the discrepancy sequence being zero from $n_0 + 1$ to $n_1 - 1$, 0^{g-1}, followed by some nonzero symbol at n_1.

However, *only* the Dornstetter / **K** implementation described here yields immediately useful information on the PDs and *only* for this BMA* implementation, the implications about supports and residue classes in this paper are valid. Fast implementations are given in [2] [11] [12].

Example 2. for **K**

(i) Rational sequence: Let $s = (s_k)_{k=1}^{\infty} = 1(110)^{\omega} \in \mathbb{F}_2^{\omega}$, then

$$G(s) \;=\; \frac{1}{x} + \frac{x+1}{x^3+1} = \frac{x^3+1+x^2+x}{x^4+x} = \frac{1}{\frac{x^4+1+x+1}{(x+1)^3}} = \frac{1 \;\;|}{|x+1} + \frac{1 \;\;|}{|x^2+1}.$$

Thus $\mathcal{K}(G(s)) = (x+1, x^2+1) \in \mathbb{F}_2[x]^*$ and $\mathbf{K}(s) = 1101010^{\omega} \in \mathbb{F}_2^{\omega}$, where $11 = \pi(x+1)$, $0101 = \pi(x^2+1)$.

(ii) Irrational sequence: The (Prouhet-) Thue-Morse (-Hedlund) sequence $s = 0110.1001.1001.0110.1001\ldots$ is quadratic-algebraic with ultimately periodic CFE $G(s) = [x^2+x+1, (x^2+1, x^2, x^2+1)^{\omega}]$ (the analogue of Lagrange's result [7] for formal power series). We infer $\mathbf{K}(s) = 0111(0101\ 0100\ 0101)^{\omega}$. Note that $\mathrm{supp}(\mathbf{K}(s)) \subset [0]_2 \,\dot\cup\, \{3\}$, but $\mathrm{supp}(s) \not\subset [r]_n$ for no r, n: A single bit outside the residue class completely destroys the pattern.

3 The Main Result: Arithmetic Progressions as Supersets of the Support of a Binary Sequence are Invariant under K

Definition 3. (i) For $n \in \mathbb{N}, r \in \mathbb{Z}$ (usually we take $0 \leq r < n$), let $[r]_n = \{k \in \mathbb{N} \mid k \equiv r \pmod n\} \subset \mathbb{N}$ be an arithmetic progression (residue class from $\mathbb{Z}/n\mathbb{Z}$ restricted to $\mathbb{N}$). We will use the $[r]_n$ as supersets for index sets of formal power series.

(ii) Let $\mathrm{supp}(s) := \{k \mid s_k \neq 0\} \subset \mathbb{N}$ be the support of $s \in A^{\omega}$ or $s \in \mathbb{F}_2[[x^{-1}]]$.

We first mention a technical lemma from [11],which we shall need in parts II and III of the proof of Theorem 6 and in the proof of Theorem 9:

Lemma 4. Equivalence Lemma [11, Lemma 11]

Let A, B be two consecutive PDs of a CFE. Replacing A, B by the three PDs $A+1, 1, 1+B$ does not change the overall value of the CFE.

Proof. See Lemma 11 in [11], also ...

Using Perron's schema with A, B and with $A+1, 1, 1+B$ both yield the same result:

$$x \mid y \overset{A}{\mid} Ay + x \overset{B}{\mid} ABy + Bx + y \text{ and}$$
$$x \mid y \overset{A+1}{\mid} Ay + y + x \overset{1}{\mid} Ay\underline{+y} + x\underline{+y} \overset{B+1}{\mid} ABy + Bx\underline{+Ay + x + Ay} + y\underline{+x}$$

(underlined parts cancel for $\mathbb{F}_2$, the lemma does not carry over to char ≥ 3). □

We have the following lemma concerning the position of nonzero coefficients in PDs, given a formal power series s with $\mathrm{supp}(s) \subset [r]_n$:

Lemma 5. *Let* $\mathrm{supp}(s) \subset [r]_n$ *for some* $n \in \mathbb{N}, 0 \leq r \leq n$.

(i) The first PD, b_1*, has degree* $g_1 \in [r]_n$ *and the nonzero coefficients* a_k*, if any, are also at indices* $k \in [r]_n$.

(ii) The second PD, b_2*, has degree* g_2 *and nonzero coefficients' indices in* $[-r]_n$.

(iii) All PDs with odd index, $b_3, b_5, \ldots$ *behave as* b_1 *does, with support in* $[r]_n$*. The PDs with even indices have support in* $[-r]_n$.

Proof. *(i)* From $\pi(b_1) = 0^{g_1-1}a_{g_1} \ldots a_0$ and $\mathrm{supp}(s) \subset [r]_n$, we have $g_1 = \deg(b_1) \in [r]_n$. The distance from a_{g_1} of all nonzero coefficients in π is a multiple of n and thus their index is in the same residue class, $k \in [g_1]_n = [r]_n$.

(ii) With $|\pi(b_1)| = 2 \cdot g_1$, the position of a_{g_2} in $\pi(b_2)$ is at $2g_1 + g_2 \equiv 2r + g_2 \in [r]_n$ and hence $g_2 \in [-r]_n$. As in *(i)* the same applies for the further nonzero coefficients: $a_k \neq 0$ implies $k \in [-r]_n$.

(iii) From $|\pi(b_1)\pi(b_2)| = 2(g_1+g_2) \equiv 2(r+(-r)) \equiv 0 \mod n$, we see that the situation for the degree g_3 of b_3 is the same as for b_1 in *(i)*, then b_4 behaves as in *(ii)* and the general case follows by induction. □

We now come to the Main Theorem of the paper:

Theorem 6. Invariance of Arithmetic Progressions under **K**

For any given $n \in \mathbb{N}$, $0 \leq r \leq n-1$*, for all binary sequences* $s \in A^\omega$ *such that the support of* s *is contained in* $[r]_n$ *i.e.*

$$G(s,x) = \sum_{k \in \mathbb{N}} s_k x^{-k} = \sum_{k \in [r]_n} s_k x^{-k}$$

the resulting sequences $\mathbf{K}^u(s)$ *again have support* $\mathrm{supp}(\mathbf{K}^{(u)}(s)) \subset [r]_n$*, for all* $u \in \mathbb{Z}$*. In other words* $\forall u \in \mathbb{Z}, \forall n \in \mathbb{N}, \forall 0 \leq r < n$:

$$\mathrm{supp}(s) \subset [r]_n \iff \mathrm{supp}(\mathbf{K}^u(s)) \subset [r]_n \iff (\mathbf{K}^u(s))_k = 0, \forall k \notin [r]_n.$$

Proof. For $n = 1$, $[0]_1 = \mathbb{N}$, nothing has to be shown. Otherwise, we proceed in 5 steps.

I. *"Blow-Up" / "Telescoping-out"* (from s to $\mathbf{K}(s)$ at $[0]_n$)

We start with $r = 0, u = 1$, any $n \geq 2 \in \mathbb{N}$. Let $s \in A^\omega$ have $\mathrm{supp}(s) \subset [0]_n$.

Set $\alpha_k := s_{nk}, k \in \mathbb{N}$, the subsequence with indices from $[0]_n$. By construction,

$$G(s,x) = \sum_{k \in \mathbb{N}} s_k x^{-k} = \sum_{k \in [0]_n} s_k x^{-k} = \sum_{k \in \mathbb{N}} s_{k \cdot n} \left(x^n\right)^{-k} = \sum_{k \in \mathbb{N}} \alpha_k \left(x^n\right)^{-k} = G(\alpha, x^n).$$

Let now $\beta := \mathbf{K}(\alpha)$ be the CFE of $G(\alpha, y)$ (where no restrictions on the support apply). Then $\beta = \pi(b_1)\pi(b_2)\dots$ is the concatenation of the encodings of the PDs of $G(\alpha, y) = \frac{1}{|b_1(y)} + \frac{1}{|b_2(y)} + \cdots$. We now do a "Blow-Up" or "Telescoping-out" and set $y := x^n$, effectively introducing $n-1$ zeroes between any two symbols from β.

From $\pi(p(y)) = \pi(\sum_{j=0}^{g} p_j y^j) = 0^{g-1}1p_{g-1}p_{g-2}\dots p_1 p_0$, we then get

$$\pi(p(x^n)) = \pi(\sum_{j=0}^{g} p_j x^{n\cdot j}) = 0^{n\cdot g-1}10^{n-1}p_{g-1}0^{n-1}p_{g-2}\dots 0^{n-1}p_1 0^{n-1}p_0,$$

where only the powers of x which are multiples of n are used for the p_j. This gives

$$G(\alpha, x^n) = \frac{1}{|b_1(x^n)} + \frac{1}{|b_2(x^n)} + \frac{1}{|b_3(x^n)} + \cdots = G(s, x).$$

Now, $0^{n\cdot g-1}10^{n-1}p_{g-1}0^{n-1}p_{g-2}\dots 0^{n-1}p_1 0^{n-1}p_0$ has the property that the indices of its coefficients p_j lie in the set $[0]_n$. Since this is valid for all $\pi(b_i(x^n))$, and each of these $\pi(\cdot)$ have a length which is a multiple of n, namely $n \cdot 2 \cdot \deg(b_i(y))$, the whole result $\mathbf{K}(s)$ is covered by $[0]_n$.

II. *"Last Shift"* (from $s, \mathbf{K}(s) \subset [0]_n$ to $s, \mathbf{K}(s) \subset [n-1]_n$)

Let $\mathrm{supp}(s) \subset [n-1]_n, n \geq 2$. Let $\hat{s} := (0, s_1, s_2, \dots)$, hence $\mathrm{supp}(\hat{s}) \subset [0]_n$ and with part I also $\mathrm{supp}(\mathbf{K}(\hat{s})) \subset [0]_n$. Furthermore, we have $G(\hat{s}) = x^{-1} \cdot G(s)$.

The CFE of $G(\hat{s}) = [b_1, b_2, b_3, \dots]$ consists only of PDs with $\deg(b_i)$ a multiple of n, in particular $\deg(b_i) > 1$. Applying the Equivalence Lemma, we generate a new, but equivalent CFE $G(\hat{s}) = [b'_1, b'_2, b'_3, \dots]$, where b'_{2i-1} has constant term zero by, if necessary, inverting this term, introducing a pseudo-PD '1' as b'_{2i}, inverting the constant term of the next PD b'_{2i+1}, and so on.

We then multiply the whole CFE by x, which amounts to alternately divide and multiply the PDs by x:

$$G(s) = x \cdot G(\hat{s}) = [b'_1/x, b'_2 \cdot x, b'_3/x, \dots],$$

where the division at odd indices is well-defined, since $\deg(b'_{2i-1}) > 1$ and the constant term is zero. Also, the pseudo-PDs '1' occur only at even indices and are replaced by x.

Now, in $\mathbf{K}(s) = \pi^{\infty}(b'_1/x, b'_2 \cdot x, b'_3/x, \dots)$, the odd-indexed b'_{2i-1}/x have support and degree in $[-1]_n$, the even-indexed $b'_{2i} \cdot x$ have support and degree in $[1]_n$, including the special case x from '1' with degree 1. Each pair (b'_{2i-1}, b'_{2i}) has an overall degree sum from $[-1]_n + [1]_n = [0]_n$, allowing the induction as in Lemma 5, and giving $\mathrm{supp}(\mathbf{K}(s)) \subset [-1]_n$.

III. *"First Shift"* (from $s, \mathbf{K}(s) \subset [0]_n$ to $s, \mathbf{K}(s) \subset [1]_n$)

This is essentially a repetition of part II, shift direction and parity inverted.

Let $\mathrm{supp}(s) \subset [1]_n, n \geq 2$. Let first $s_1 = 0$. Let $\hat{s} := \sigma(s) := (s_2, s_3, \dots)$, hence $\mathrm{supp}(\hat{s}), \mathrm{supp}(\mathbf{K}(\hat{s})) \subset [0]_n$. Also, $G(\hat{s}) = x \cdot G(s)$.

The CFE of $G(\hat{s}) = [b_1, b_2, b_3, \dots]$ consists only of PDs with $n \mid \deg(b_i)$.

As before, by Lemma 5, we generate an equivalent CFE $G(\hat{s}) = [b'_1, b'_2, b'_3, \dots]$, where now the *even* b'_{2i} have constant term zero, applying Lemma 5, introducing pseudo-PDs '1' as b'_{2i+1} at odd index.

We then divide by x, giving $G(s) = G(\hat{s})/x = [b'_1 \cdot x, b'_2/x, b'_3 \cdot x, \dots]$, where the division at even indices is well-defined, as before and the pseudo-PDs '1', now at odd indices, are again replaced by x.

Now, in $\mathbf{K}(s) = \pi^\infty(b'_1 \cdot x, b'_2/x, b'_3 \cdot x, \dots)$, the odd-indexed $b'_{2i-1} \cdot x$ have support and degree in $[1]_n$, including the special case x from '1' with degree 1. The even-indexed b'_{2i}/x have support and degree in $[-1]_n$. Thus, again each pair (b'_{2i-1}, b'_{2i}) has an overall degree sum from $[1]_n + [-1]_n = [0]_n$, allowing the induction as in Lemma 5.

For $s_1 = 1$, $x \cdot G(s) = 1 + G(\hat{s})$. Observe that $1 + [b_1, b_2, \dots] = 0 + [1, b_1 + 1, b_2, \dots]$ by Lemma 5 with $(1, b_1) \equiv (0, 1, b_1 + 1)$, see [11, Cor. 12], which fits neatly into the overall process, the pseudo-PD being at an odd index. All in all, $\mathrm{supp}(\mathbf{K}(s)) \subset [1]_n$.

IV. *"General Shift"* (from $[r]_n$ to $[r \pm 1]_n$)

Let $r \notin \{-1, 0, +1\}$ and $\mathrm{supp}(s) \subset [r]_n$. By the condition on r, all PDs have degree at least 2 and all constant terms are zero, also the first bit $s_1 = 0$. The sequence $\overleftarrow{s} := (s_2, s_3, s_4, \dots)$ has $\mathrm{supp}(\overleftarrow{s}) \subset [r-1]_n$, the sequence $\overrightarrow{s} := (0, s_1, s_2, \dots)$ has $\mathrm{supp}\,(\overrightarrow{s}) \subset [r+1]_n$, by construction.

Hence, from $G(s) =: [b_1, b_2, b_3, \dots]$, we immediately obtain $G(\overleftarrow{s}) = [b_1/x, b_2 \cdot x, b_3/x, \dots]$ and $G(\overrightarrow{s}) = [b_1 \cdot x, b_2/x, b_3 \cdot x, \dots]$, all terms well-defined and no pseudo-PD '1' involved.

Therefore, the 3 sequences $00\pi^\infty(b_1/x, b_2 \cdot x, b_3/x, \dots) = 0\pi^\infty(b_1, b_2, b_3, \dots) = \pi^\infty(b_1 \cdot x, b_2/x, b_3 \cdot x, \dots)$ are one and the same, in other words $\mathrm{supp}(\overleftarrow{s}) \subset [r-1]_n \Leftrightarrow \mathrm{supp}(\mathbf{K}(s)) \subset [r]_n \Leftrightarrow \mathrm{supp}(\overrightarrow{s}) \subset [r+1]_n$.

In parts I, II, III, we have seen that $\mathrm{supp}(s) \subset [a]_n \Leftrightarrow \mathrm{supp}(\mathbf{K}(s)) \subset [a]_n$ for $a \in \{-1, 0, +1\}$. By the previous equality, we can now extend this to $a = 2$ and $a = -2$, and by induction to all $0 \le a, r \le n - 1$.

V. *Isometry & Induction* (from $\mathbf{K}(s)$ to $\mathbf{K}^u(s)$)

We now show for arbitrary $n \in \mathbb{N}$, $0 \le r < n$ and any $u \in \mathbb{Z}$ that $\mathbf{K}^u$ maintains the invariant, $\mathrm{supp}(\mathbf{K}^u(s)) \subset [r]_n$. We have seen that this is true for $u = 1$. By induction, this is also valid for $u \in \mathbb{N}$ (forward application of $\mathbf{K}$).

$\mathbf{K}$ is an isometry. Therefore, restricting $\mathbf{K}$ to the first k coordinates, we have $\mathbf{K}^{2!^k}(s)_{1\dots k} = (s_1, \dots, s_k)$ and thus $\mathbf{K}^{2^k-1}(s)_{1\dots k} = \mathbf{K}^{-1}(s)_{1\dots k}$, since $\mathbf{K}$ is invertible as isometry. Hence, the (positive) case $u = 2^k - 1$ already has shown $\mathrm{supp}(\mathbf{K}^{-1}) \subset [r]_n$ for the first k coordinates. Letting $k \to \infty$ shows the claim for $u = -1$. Applying induction to the (negative) exponent shows it for all $u \in \mathbb{Z}$. □

As a consequence of Main Theorem 6 and Lemma 5, we obtain the following corollary:

Corollary 7. (*i*) *Let* $\mathrm{supp}(s) \subset [0]_n$ *for some* $n \in \mathbb{N}$. *Then all PDs of all* $\mathbf{K}^u(s)$ *have degrees and indices of nonzero coefficients a multiple of* n.

(*ii*) *Let* $\mathrm{supp}(s) \subset [r]_n$ *for some* $n \in \mathbb{N}$ *and* $1 \le r \le n - 1$. *Then all* $\mathbf{K}^u(s)$ *have alternately degrees* $d \equiv r \pmod n$, *for* $b_1, b_3, b_5, \dots$, *and degrees* $d \equiv n - r \pmod n$, *for* $b_2, b_4, b_6, \dots$. *The same applies for the indices of nonzero coefficients.*

In particular, for $n = 2$, *we obtain*:
(*iii*) *Let* $s \in A^\omega$ *be such that* $s_{2i-1} = 0, i \in \mathbb{N}$, *i.e.* $\mathrm{supp}(s) \subset [0]_2$. *Then all odd coefficients of* $\mathbf{K}^u(s), u \in \mathbb{Z}$ *are zero as well and thus the PDs are all of even degree.*

(*iv*) *Similarly, for* $\mathrm{supp}(s) \subset [1]_2$*, only coefficients with odd indices may be non-zero and thus all* $\mathbf{K}^u(s), u \in \mathbb{Z}$ *have only PDs with odd degree.*

Proof. The corollary follows immediately from Lemma 5 and Main Theorem 6. □

Conjecture 8. Theorem 6 is valid for sequences over any finite field $\mathbb{F}_q$.

Proof. Idea: Parts I, IV, and V of the proof carry over without change to any $\mathbb{F}_q$. For parts II and III, we must replace Lemma 4 by the more involved cases treated in [12]. □

4 A Further Sequence Pattern Property Maintained by K

Theorem 9. *Let* $s = (s_1, s_2, \dots) \in A^\omega$ *be a binary sequence with* $s_{2n-1} = s_{2n}, \forall n \in \mathbb{N}$.
Then for any $u \in \mathbb{Z}$, $t = (t_1, t_2, \dots) := \mathbf{K}^u(s)$ *also satisfies* $t_{2n-1} = t_{2n}, \forall n \in \mathbb{N}$.

Proof. Firstly, we have $G(s, x) = (x + 1) \cdot G(\hat{s}, x^2)$ with $\hat{s}_n := s_{2n}$, since two consecutive 1s can be extracted into the factor $(x + 1)$, leaving a single 1 at an even index.

Now, $\mathbf{K}(\hat{s})$ is just some binary sequence, which we call $\hat{t}$. By blow-up with a factor of 2, $G(\hat{s}, x^2)$ has a CFE $[\hat{b}_1, \hat{b}_2, \dots]$ such that $\pi(\hat{b}_1)\pi(\hat{b}_2)\dots = 0\hat{t}_1 0\hat{t}_2 0\hat{t}_3 0\hat{t}_4 \dots$, where the $\hat{b}_i$ are polynomials in x^2, *e.g.* $\pi(x^2) = 0100, \pi(x^2 + 1) = 0101$.

From $G(s, x) = (x + 1) \cdot G(\hat{s}, x^2)$, the desired CFE $\mathbf{K}(s)$ then corresponds to the CFE of $G(s, x) = [\hat{b}_1/(x + 1), \hat{b}_2 \cdot (x + 1), \hat{b}_3/(x + 1), \hat{b}_4 \cdot (x + 1), \dots]$ — if well-defined.

The PDs with odd index therefore have to be multiples of $(x + 1)$, which is equivalent to having an even number of coefficients 1. Again, we apply the Equivalence Lemma.

This time, we include or exclude a constant term $a_0 = 1$ in such a way that $\hat{b}'_{2i-1}$ has an even number of nonzero (*i.e.* 1) coefficients. As before, we introduce a pseudo-PD 1 (=: $\hat{b}'_{2i}$) after $\hat{b}'_{2i-1}$ in this case, toggle the constant coefficient of the next PD, and so on.

We now have PDs with odd index, having an even number of (still isolated) 1s, and PDs with even index, having any number of (isolated) 1s, or being the pseudo-PD 1.

We multiply the PDs with even index by $x+1$, giving a pattern '11' for every (isolated) 1 present previously, and a pseudo-PD 1 is changed to $x + 1$ with $\pi(x + 1) = 11$.

The PDs with odd index have to be divided by $(x + 1)$. Such a PD now has an even number of 1s. Hence we can split the coefficient sequence $0^{l_1}10^{k_1}10^{l_2}10^{k_2}10^{l_3}10^{k_3}1\dots$ into parts $0^{l_i}10^{k_i}1$, corresponding to polynomials $x^{k_i+1} + 1 = (x + 1) \cdot \sum_{j=0}^{k_i} x^j$.

Since all zero runs have odd length (the 1s appear at even positions from $[0]_2$), this polynomial consists of an even number of consecutive coefficients 1, or $(k_i + 1)/2$ patterns '11'. The whole $\pi(\hat{b}'_{2i-1}/(x + 1))$ thus consists of a mix of patterns '00' and '11'. The same is (trivially) true for $\pi(\hat{b}'_{2i} \cdot (x + 1))$, and we obtain $t_{2n-1} = t_{2n}, \forall n \in \mathbb{N}$.

The general case $u \in \mathbb{Z}$ follows as in the proof of Main Theorem 6 by induction and $\mathbf{K}$ being an isometry. □

5 The $\widehat{K}$ Isometry and its Tree Complexity

In this section, we apply Theorems 6 and 9, showing *why* the tree complexity of the isometry induced by linear complexity is so small, compared to those of 2-adic and rational complexity, following the isometric approach as expounded at SETA 2004, [14].

Tree complexity of Isometries

The three complexity measures K (linear), A (2-adic) [5] [6], and R (rational) [16] [17] [18] can be compared via their induced isometries $\mathbf{Y} \in \{\mathbf{K}, \mathbf{A}, \mathbf{R}\}$, determining their tree complexity ([10][14]).

Let an infinite regular binary tree with labels be indexed by $v \in A^*$. Starting with $v = \varepsilon$ at the root, each node v has its left and right child nodes indexed by $v0$ and $v1$, respectively. The label at node v, $\widehat{\mathrm{Y}}(v) := \mathbf{Y}(v0^\omega)_{|v|+1} \in A$ is the result of the mapping $v0\ldots \overset{\mathbf{Y}}{\longmapsto} w\hat{Y}(v)\ldots$. The tree complexity of the labeling (lower bounds from first 36 levels) is given in Table 2.

$\widehat{Y}$	$h=1$	2	3	4	5	6
$\widehat{\mathrm{K}}$	2	8	48	480	2816	21760
$\widehat{\mathrm{A}}$	2	8	128	10506	1931K	91M
$\widehat{\mathrm{R}}$	2	8	118	12244	2195K	45M

Table 2: Tree complexities of induced isometries, $K_B(\widehat{Y}, h)$ for $h = 1, \ldots, 6$.

Apparently, **K** is by far the least complex (in terms of tree complexity) of the three isometries. **A** and **R** are of comparable complexity, also suggested by the fact $\mathbf{A}(v^\omega) = \mathbf{R}(\overleftarrow{v}^\omega), \forall v \in A^+$ (see [18, Thm. 13]).

The Results of Massey/Wang and Carter

We now show that Theorems 6 and 9 together with results by Massey and Wang [19] and by Carter [3] fix a large part of the initial part of the isometry **K**.

Theorem 10. (*Massey and Wang* [19])
A sequence $s \in A^\omega$ has perfect linear complexity profile, i.e. all PDs are of degree 1, if and only if $s_1 = 1$, and $s_{2i+1} = s_i + s_{2i}$ for $i \in \mathbb{N}$. The s_{2i} can be chosen arbitrarily.

Proof. See [19]. □

Theorem 11. (*Carter* [3])
(*i*) *A sequence $s \in A^\omega$ with $s_1 = 0$, and $s_{2i+1} = s_i + s_{2i}$ for $i \in \mathbb{N}$ (where the s_{2i} can be chosen arbitrarily) has only PDs of even degree, or of degree 1. No two consecutive PDs have degree 1.*

(*ii*) *A sequence $s \in A^\omega$ with $s_2 = 1$, and $s_{2i+2} = s_{i+1} + s_{2i+1}$ for $i \in \mathbb{N}$ (where the s_{2i-1} can be chosen arbitrarily) has only PDs of odd degree, or of degree 2.*

(*iii*) *A sequence $s \in A^\omega$ with $s_2 = 0$, and $s_{2i+2} = s_{i+1} + s_{2i+1}$ for $i \in \mathbb{N}$ (where the s_{2i-1} can be chosen arbitrarily) has only PDs of odd degree.*

Proof. See [3], Theorems 4.3.3, 4.3.4 for (*i*), 4.4.3 for (*ii*) and 4.4.2 for (*iii*). □

0,1 :	fixed value	! :	value fixed, depending on some previous entries
* :	arbitrary value	= :	value repeats the entry immediately before

Source	Pattern in s	Permitted PD degrees in $\mathbf{K}(s)$
MW [19]	`1*!*!*!*!*`	1
C_1 [3]	`0*!*!*!*!*`	1; 2,4,6,..., not 1|1
C_2 [3]	`*1*!*!*!*!`	2; 1,3,5,...
C_3 [3]	`*0*!*!*!*!`	1,3,5,...
$[0]_2$	`0*0*0*0*0*`	2,4,6,...
$[1]_2$	`*0*0*0*0*0`	1,3,5,...
Thm. 9	`*=*=*=*=*=`	1,3,5,...
$[0]_3$	`00*00*00*0`	3,6,9,...
$[1]_3$	`0*00*00*00`	$((2,5,8,\dots)(1,4,7,\dots))^\omega$
$[2]_3$	`*00*00*00*`	$((1,4,7,\dots)(2,5,8,\dots))^\omega$
$[0]_7$	`000000*000`	7,14,21,...
$[1]_7$	`*000000*00`	$((1,8,15,\dots)(6,13,20,\dots))^\omega$
$[5]_7$	`0000*00000`	$((5,12,19,\dots)(2,9,16,\dots))^\omega$

Figure 1: Patterns in s and PD degrees in its Continued Fraction.

Regularity of the isometry induced by K

Summarizing the results of Massey and Wang, Carter, the $[r]_n$ cases of Theorem 6 and Theorem 9, we have the invariant patterns for the support given in Figure 1.

We therefore have the restrictions shown in Figure 2 (**a?** unknown bit, but same **a!** at child nodes) for the tree complexity of $\widehat{K}$, from the following patterns, where the underlined value is mandatory and $va \xrightarrow{\mathbf{K}} wb$ gives $\widehat{K}(v) = a + b$. Theorems 6 and 9 fix 38 out of the first 63 entries of the $\widehat{K}$ tree, and also including the results by Wang and Massey and by Carter as well as LFSR theory, we account for 47 out of these 63 entries in the first 6 levels of the $\hat{K}$ tree:
LFSR theory, LF: $v^\omega \mapsto *^{2|v|}\underline{0^\omega}$, *e.g.* $101010 \mapsto 101\underline{00}$
Thm 6, $[r]_n$: $\forall 0 \le r < n \in \mathbb{N}, \forall v \in A^*$: $(\mathrm{supp}(v) \subset [r]_n) \wedge (|v| + 1 \notin [r]_n) \Rightarrow \mathbf{K}(v) = 0$
Thm 9: $\forall a, b, c, \dots, \exists \alpha, \beta, \gamma, \dots : aabbcc\dots \mapsto \alpha\underline{\alpha}\beta\underline{\beta}\gamma\underline{\gamma}\dots$, *e.g.* $110011 \mapsto 1\underline{1}1\underline{1}1\underline{1}$
Massey-Wang, MW: $(1, a, a+1, b, b+a, c, c+a+1, \underline{d}, d+b, e, e+b+a, \dots)$
$\mapsto \underline{1} * \underline{1} * \underline{1} * \underline{1} * \underline{1} * \dots$, hence $\widehat{K}(\varepsilon) = 1 + 1 = 0, \widehat{K}(1a) = a + 1 + 1 = a$
Carter (i), C_1: $\{(0, a, a+0, b, b+a, c, \dots)\} \to \{00\underline{0}\underline{0}, 1*\underline{0}\underline{0}\underline{0}, \dots\}$
Carter (iii), C_3: $\{(a, 0, b, b+0, c, c+b, \dots)\} \to \{1*1*0\underline{0}, 1*0\underline{0}\underline{0}\underline{0}, 0\underline{0}\underline{0}\underline{0}\underline{0}\underline{0}, \dots\}$

Proposition 12. *Asymptotically, in row $N \in \mathbb{N}$, $\Theta(2^{N/2})$ out of the 2^{N-1} prefixes $v \in A^{N-1}$ have a value $\widehat{K}(v)$ that is determined by one of the cases $[r]_2$, Theorem 9, or MW.*

Proof. For even $|v|$, both $[0]_2$ and MW yield $2^{|v|/2}$ cases where $\mathbf{K}(va)_{|v|+1}$ is restricted to 0, respectively 1. For odd $|v|$, both $[1]_2$ and Theorem 9 yield $2^{(|v|+1)/2}$ cases by restricting $\mathbf{K}(va)_{|v|+1}$ to 0, respectively $\mathbf{K}(va)_{|v|}$. □

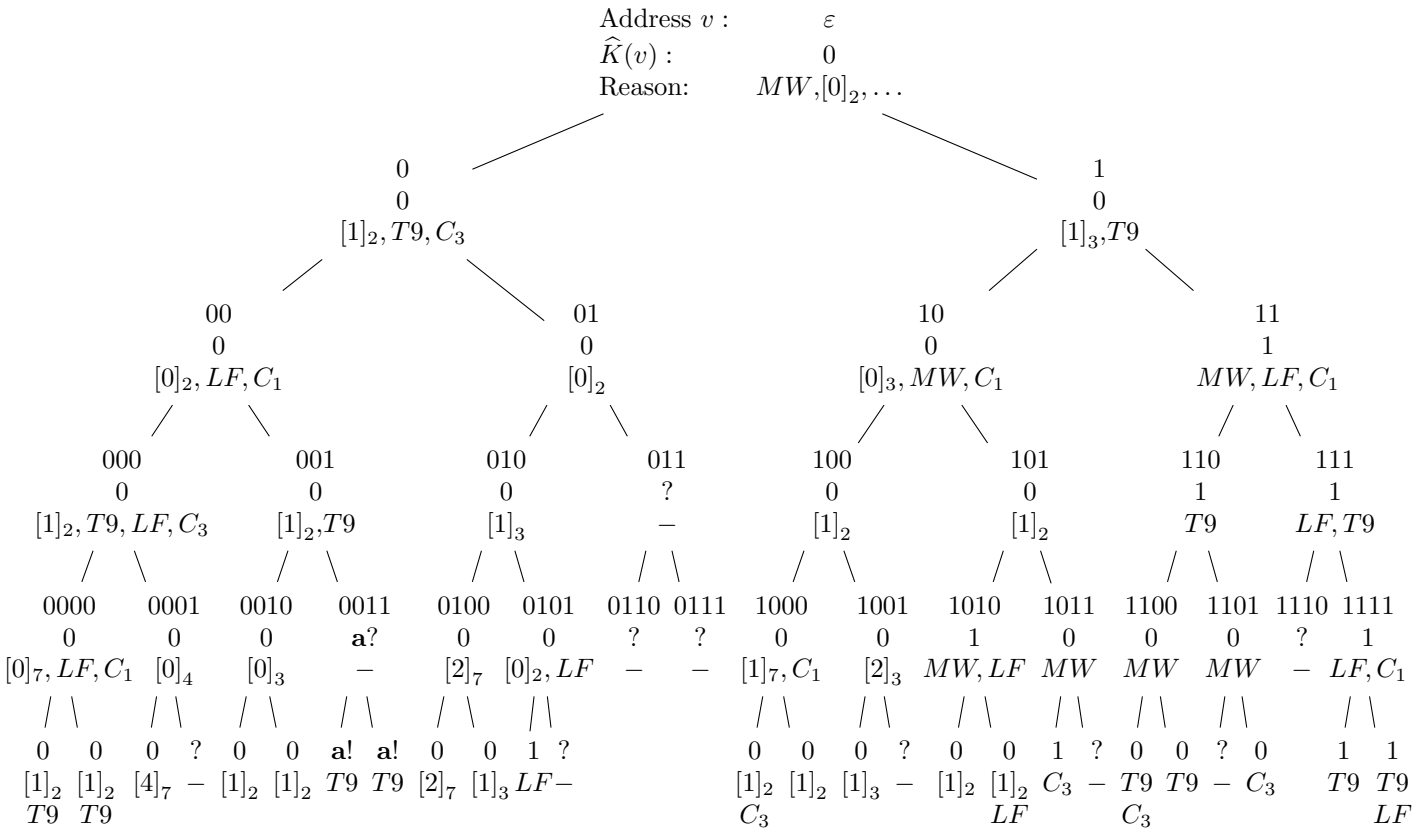


Figure 2: Address $v \in A^*$, $\widehat{K}(v)$, and reason for $\widehat{K}(v)$.

Conjecture 13. Including all $[r]_n$ of Theorem 6 (prime n is sufficient), Carter (i, ii, iii) and LFSR theory does not change the asymptotic result of Proposition 12.

Conclusion

We have shown that for all binary sequences $s \in A^\omega$, the properties $\mathrm{supp}(s) \subset [r]_n$ for any residue class, and $s_{2k-1} = s_{2k}, \forall k \in \mathbb{N}$ are preserved under forward and backward application of the continued fraction operator $\mathbf{K}$ (the modified Berlekamp-Massey Algorithm). We applied the result to the $\widehat{K}$ tree associated with the isometry $\mathbf{K}$.

References

[1] J.-P. Allouche, J. Shallit, *Automatic Sequences*, CUP, 2003.

[2] M. del P. Canales Chacón, M. Vielhaber. Structural and Computational Complexity of Isometries and their Shift Commutators. *Electronic Colloquium on Computational Complexity*, ECCC TR04–057, 2004.

[3] G. D. Carter. Aspects of local linear complexity. *PhD Thesis. Royal Holloway and Bedford New College, London*, 1989.

[4] J. L. Dornstetter. On the equivalence between Berlekamp's and Euclid's algorithm. *IEEE Trans IT*, 33(3):428-431, 1987.

[5] A. Klapper, M. Goresky. Cryptanalysis Based on 2-Adic Rational Approximation. *Crypto '95, LNCS*, 963:262–273, 1995.

[6] A. Klapper, M. Goresky. Feedback shift registers, 2-adic span, and combiners with memory. *J Crypt*, 10:111–147, 1997.

[7] J. L. Lagrange, *Additions au mémoire sur la réduction des equations numériques*. Mémoires de l'Académie royale des sciences et belles-lettres (de Berlin) 24, 1770.

[8] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, CUP, 1994.

[9] J. Massey. Shift-register synthesis and BCH decoding. *IEEE IT*, 15(1):122-127, 1969.

[10] H. Niederreiter, M. Vielhaber. Tree complexity and a doubly exponential gap between structured and random sequences. *J Complexity*, 12(3):187-198, 1996.

[11] H. Niederreiter, M. Vielhaber. Simultaneous shifted continued fraction expansions in quadratic time. *AAECC*, 9(2):125-138, 1998.

[12] H. Niederreiter, M. Vielhaber. An algorithm for shifted continued fraction expansions in parallel linear time. *TCS* 226(1-2):93-104, 1999.

[13] O. Perron. Die Lehre von den Kettenbrüchen, Bd. I. *Teubner, Stuttgart 1954/1977.*

[14] M. Vielhaber. A Unified View on Sequence Complexity Measures as Isometries. **SETA** 2004, *LNCS*, 3486:143-153, 2004.

[15] M. Vielhaber. Continued Fraction Expansion as Isometry - The Law of the Iterated Logarithm for Linear, Jump, and 2-Adic Complexity. *IEEE Trans IT*, 53(11):4383-4391, 2007. (Preprint: `arXiv:cs/0511089`)

[16] M. Vielhaber. V Tree — Continued Fraction Expansion, Stern-Brocot Tree, Minkowski's ?($\mathbf{x}$) Function In Binary: Exponentially Faster. `arXiv:2008.08020`, 2020.

[17] M. Vielhaber, M. del P. Canales, S. Jara. Feedback in Q Shift Registers FQSR: Pseudo-Ultrametric Continued Fractions in R. **SETA** 2020.

[18] M. Vielhaber, M. del P. Canales, S. Jara. Rational complexity of binary sequences, FQSRs, and pseudo-ultrametric continued fractions in $\mathbb{R}$. *Cryptography and Communications*, 14(2):433-457, 2022.

[19] M.-Z. Wang, J. Massey. The characterization of all binary sequences with a perfect linear complexity profile. EUROCRYPT '86, Linköping, 1986.

RW-9: A Family of Random Walk Tests

Muhidin Uğuz
Middle East Technical University
Ankara, TURKEY
muhid@metu.edu.tr

Fatih Sulak
Atilim University
Ankara, TURKEY
fatih.sulak@atilim.edu.tr

Ali Doğanaksoy
Middle East Technical University
Ankara, TURKEY
aldoks@metu.edu.tr

Onur Koçak
TÜBİTAK
Ankara, TURKEY
onur.kocak@tubitak.gov.tr

Abstract

In this work, we define a family of 9 statistical randomness tests for collections of short binary strings, by making use of random walk statistics. For a binary sequence of length n we consider the probability of intersecting the line $y = t$ exactly at k distinct points. In the literature there are some explicit formulas for these probability values but the ones for short sequences are not feasible for computations concerning sequences of length 256 or more. On the other hand, approximation techniques, or asymptotic approaches that should be used only when testing long sequences, are not useful for testing sequences of length between 256 and 4096. Recursive formulas, derived in this paper, made it possible to obtain exact values of the corresponding probability distribution functions. Employing these formulas, we have provided necessary figures for testing collections of strings of length 2^7, 2^8, 2^{10} and 2^{12} bits. Finally we have applied these 9 tests to several collections of strings obtained from different pseudorandom number generators and to biased sequences in order to see if the tests introduced can detect non-random data.

Keywords: Cryptography, Random Walk, Statistical Randomness Testing, NIST Test Suite

1 Introduction

The quality of a binary sequence, produced by a pseudorandom number generator to be used as a seed for cryptosystems, has a vital importance. It should be random looking, that is, should not follow any pattern that may give rise to an attack to the system. Moreover, outputs of encryption algorithms must also be indistinguishable from a true random sequence. Thus, in evaluation of a binary sequence, a pseudorandom number

generator or an encryption algorithm in terms of randomness of its output, one needs a statistical randomness test or even a package of tests that evaluates the randomness property. Since any periodic sequence may appear as an output of a true random source, there is no mathematical method to decide whether the sequence under consideration is in fact an output of a true random generator or not, for sure. On the other hand, one can give decision depending on the observed statistical values of the sequence, comparing it with the expected values and distributions. There are many statistical randomness tests and test suites in the literature ([1], [2], [3]). Moreover there are many studies about the independence of the statistical randomness tests ([4], [5]). Different point of views yields different statistical tests. One of these point of views is random walk statistics. In the literature there are various randomness tests concerning random walk statistics, however these tests can either be applied to a very long sequence (a sequence of length at least 10^6), such as the tests included in the NIST Test Suite [6], or to a collection of very short sequences (sequences of length at most 256), as stated in [7]. Random walk tests are included in the NIST Test Suite in the name of Random Excursion and Random Excursion Variant Tests [6]. These tests use approximations in the computations of the cumulative probability distribution of the corresponding random variables and therefore can be applied only to sequences of length longer than 10^6. In this work, we revisit the distribution function of the test and give the exact probability values for sequences of size less then 4096.

The organization of the paper is as follows. In section 2, we give preliminaries. The recursive relation satisfied by the number of sequences of length n, having exactly k balanced points is derived first for balanced sequences in section 3, and then for general sequence in section 4, to be used for the random excursion statistics. In section 5, using the results obtained in sections 3 and 4, we derive recursive relations for the number of strings intersecting the line $y = t$, exactly k times. In section 6, we define new randomness tests based on these statistics. In section 7, we apply the proposed tests to random and non-random data. Finally in section 8, we conclude the paper. We omitted the proofs of Lemma 4, Theorem 11, Proposition 12 and Theorem 13 due to the page limitations.

2 Preliminaries

First, we will introduce the notations used in this article. σ denotes a binary string $s_1, s_2, \cdots, s_n$ of length n. A string σ is called *balanced* if the number of its terms, that is s_i's, equal to 0 is the same as the number of its terms equal to 1; we call a term s_k $(k \leq n)$ a *balance point* if the substring $s_1, \ldots, s_k$ is balanced. Obviously a string is balanced if and only if the last term s_n is a balance point.

To give a motivation for the following definitions, consider a binary string $\sigma = s_1, \cdots, s_n$ of length n, and its graph. The graph of a sequence σ, regarded as a continuous function, is drawn by joining the gaps between dots (i, s_i) with line segments. These line segments start from the origin, and the part of it between $(i-1, s_{i-1})$ and (i, s_i) has slope equal to $a_i = (-1)^{s_i} = 1 - 2s_i$. The graph of the sequence $\sigma = 0, 1, 1, 0, 0, 1, 0, 0$ is given below to illustrate this method of drawing graph of a discrete binary sequence, regarding

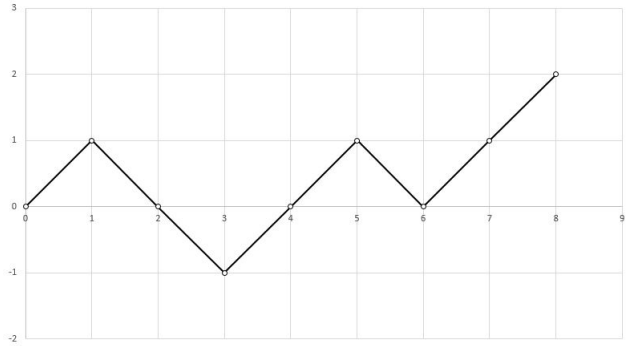


Figure 1: Graph of the sequence $\sigma = 0, 1, 1, 0, 0, 1, 0, 0$

it as a continuous function.

Definition 1. A string σ is said to **intersect** (meet or touch) the line $y = t$ at $x = i$ if $2(s_1 + \cdots + s_i) = i - t$, that is the difference between the ones and zeroes in the ordered set $\{s_1, s_2, \ldots, s_i\}$ is t.

Note that s_i is a *balance point* of the binary sequence σ if and only if the graph of σ intersects the line $y = 0$ at $x = i$.

Definition 2. Here we list some definitions and notations that will be used throughout the paper.

- $\mathbf{X_t(n, k)}$ denotes the set of all strings of length n which intersect the line $y = t$ exactly at k distinct terms and denote the number of elements of this set, that is $|X_t(n, k)|$, by $x_t(n, k)$. As a special case, for $k = 0$, we write $X_t(n) = X_t(n, 0)$ and similarly, $x_t(n) = |X_t(n, 0)|$. Since $X_t(n)$ is the set of strings of length n which do not intersect the line $y = t$, the complement $\overline{X}_t(n)$ of this set consists of strings which intersect the line $y = t$ at least in one point. We write $\overline{x}_t(n) = |\overline{X}_t(n)|$.

- $\mathbf{B(n, k)} \subset X_0(n, k)$ denotes the set of balanced strings of length n which contain exactly k balance points and $b(n, k)$ is the number of such strings.

- $\mathbf{B_t(n)}$ stands for the set of strings of length n which touch the line $y = t$ for the first time at the last term and $b_t(n) = |B_t(n)|$. Note that $B_0(n) = B(n, 1)$ and if $t \neq 0$, then no string in $B_t(n)$ is balanced. In fact, if $\sigma \in B_t(n)$, then $\dfrac{n + t}{2}$ of the terms of σ are equal to zero.

- $\mathbf{X(n, k)}$ denotes the set of strings which contain exactly k balance points and $x(n, k)$ is the number of such strings.

- The probability of a string of length n to have exactly k intersections with the line $y = t$ (or $y = -t$) will be denoted by $\mathbf{p_t(n, k)} = prob(\sigma \in X_t(n, k)) = x_t(n, k)/2^n$.

- Let n and k be positive integers and let $a(i,j)$ be a two dimensional array, $i = 1,\ldots,n$ and $j = 1,\ldots,k$. By $[\mathbf{a}(\mathbf{n},\mathbf{k})]$ we denote the table (matrix) whose rows are indexed by $i = 1,\ldots,n$ and columns are indexed by $j = 1,\ldots,k$. In certain circumstances row and/or column indices are allowed to start with 0 rather than 1.

From the definition it follows that $x_0(n,k) = x(n,k)$ and $x_t(n,k) = x_{-t}(n,k)$ for any $t = 1,\ldots,n$.

One of the basic tools we are going to employ is the sequence $\{C_n\}_{n=0}^{\infty}$of Catalan numbers defined by $C_n = \dfrac{1}{n+1}\binom{2n}{n}$ for any non negative integer n. The first few terms of this sequence are 1, 1, 2, 5, 14,....

Now we will summarize some well known identities about Catalan numbers. It is straightforward to see that the Catalan numbers satisfy the following recursion:

$$C_n = \frac{4n-2}{(n+1)}C_{n-1}\ \forall n > 1. \tag{1}$$

Another important property of the Catalan numbers is that, convolution of the sequence $\{C_n\}_{n=0}^{\infty}$ with itself is again itself, that is, for any non negative integer n, $C_{n+1} = \sum_{i=0}^{n} C_i C_{n-i}$. Moreover, using this convolution property, it is east to show that the generating function of this sequence,

$$C(z) = \sum_{i=0}^{\infty} C_i z^i = 1 + z + 2z^2 + 5z^3 + 14z^4 + \cdots$$

satisfies the equation

$$zC^2(z) = C(z) - 1 \tag{2}$$

and from which it follows that $C(z) = \frac{1-\sqrt{1-4z}}{2z}$.

By differentiating both sides of the equation (2) one obtains

$$\frac{d}{dz}C(z) = \frac{C^2(z)}{1-2zC(z)} = \frac{C(z)-1}{z(1-2zC(z))} \tag{3}$$

and by differentiating the product

$$zC(z) = \sum_{i=0}^{\infty} \frac{1}{i+1}\binom{2i}{i} z^{i+1}$$

we obtain the generating function of the sequence $\left\{\binom{2n}{n}\right\}_{n=0}^{\infty}$ as:

$$C(z) + z\frac{d}{dz}C(z) = \sum_{i=0}^{\infty}\binom{2i}{i} z^i. \tag{4}$$

The following lemma presents a result which will be the basis of many computations throughout the work.

Lemma 3. *Let n, t and q be positive integers with $t \leq q \leq n$. The number of strings of length n which contain q zeros and which intersect the line $y = t$ at least once is given by*

$$\begin{cases} \binom{n}{q-t} & if\ q < \dfrac{n+t}{2}, \\ \binom{n}{q} & if\ \frac{n+t}{2} \leq q \leq n. \end{cases}$$

Proof. Given a string σ of length n which intersects the line $y = t$, depending on q we consider two cases:

1. $\dfrac{n+t}{2} < q \leq n$. In this case σ necessarily intersects the line $y = t$ and number of such strings is $\binom{n}{q}$.

2. $t \leq q \leq \dfrac{n+t}{2}$. Let A be the set of strings of length n which have q zeros and which intersect the line $y = t$, and let B be the set of strings of length n which have $q - t$ zeros. We will show that these two sets have the same number of elements, so that the number of strings in A is $\binom{n}{q-t}$.

   Given $\sigma \in A$. Let i_0 be the smallest integer such that σ intersects the line $y = t$ at s_{i_0}. The string $\overline{\sigma} = \overline{s}_1 \cdots \overline{s}_{i_0} s_{i_0+1} \cdots s_n$ where $\overline{s}_i = 1 - s_i, i = 1, \ldots, i_0$ has $q - t$ zeros, hence $\sigma \in B$. Thus, to each $\sigma \in A$, there corresponds a unique string $\overline{\sigma} \in B$. Conversely, any string τ in B has $q - t$ zeros, hence $n - q + t$ ones. On the other hand, the condition $q \leq (n + t)/2$ implies that $n - q + t \geq (n + t)/2$, which means that the string τ intersects the line $y = -t$. Now in the string τ, starting with the first term replace each one with a zero and each zero with a one up to the term at which the string intersects the line $y = -t$ for the first time. The resulting string intersects the line $y = t$ and has q zeros, hence is in A. Then the correspondence given above is one to one and the sets A and B have the same number of elements.

□

Lemma 4. *Let n and t be positive integers with $t \leq n$. The number of strings of length n which intersect the line $y = t$ at least once is given by*

$$\overline{x}_t(n) = \begin{cases} 2\displaystyle\sum_{i=0}^{\frac{n-t}{2}} \binom{n}{i} - \binom{n}{\frac{n-t}{2}} & if\ n+t\ is\ even, \\ 2\displaystyle\sum_{i=0}^{\frac{n-t-1}{2}} \binom{n}{i} & if\ n+t\ is\ odd. \end{cases} \tag{5}$$

3 Recursive Relations Satisfied by $b(n,k)$

We first give an explicit expression for $b(n,1)$, the number of balanced sequences which have no balance points other than the last term. It is obvious that a balanced sequence must be of even length, therefore $b(n,1)=0$ for any odd integer n. For sequences of even length we have the following proposition.

Proposition 5. *For any positive integer m, $b(2m,1)=2C_{m-1}$ where C_{m-1} denotes the corresponding Catalan number.*

Proof. Any $\sigma = s_1 \cdots s_{2m} \in B(2m,1)$ is balanced and has only one balance point (necessarily the last term) and none of the terms $s_1,\ldots,s_{2m-1}$ is a balance point. For $m=1$ the claim is apparent: $b(2,1)=2=2C_0$. Now assume that $m>1$ and $s_1=1$ (hence, $s_{2m}=0$). It easy to see that the string $s_2,\ldots,s_{2m-1}$ is balanced and it cannot intersect the line $y=1$. Thus, to each such string, there corresponds a unique string $\sigma \in B(2m,1)$ with $s_1=1$. Since the converse relation holds also, the number of strings in $B(2m,1)$ is equal to the number of strings of length $2m-2$ which have $q=m-1$ zeros and which do not intersect the line $y=1$. Then, from Lemma 3 we obtain

$$b(2m,1)=\binom{2m-2}{m-1}-\binom{2m-2}{m-2}$$

which simplifies into C_{m-1}. By including the strings with initial term 0, the assertion follows. □

As a result, for any nonnegative integer we have

$$b(n,1)=\begin{cases} 0 & if\ n=0\ or\ n\ is\ odd,\\ 2C_{\frac{n}{2}-1} & if\ n>0\ is\ even. \end{cases} \tag{6}$$

Proposition 6. *For any positive integers m and $k>1$, the sequence $\{b(2m,k)\}_{n=0}^{\infty}$ is the convolution of the sequences $\{b(n,1)\}_{n=0}^{\infty}$ and $\{b(n,k-1)\}_{n=0}^{\infty}$, that is*

$$b(2m,k)=\sum_{i=0}^{m-1} b(2i,1)b(2m-2i,k-1).$$

Proof. Let $k>1$ and consider a string $\sigma \in B(n,k)$. Assume that the first balance point is s_{2i}. Then, σ can be separated into two substrings $\sigma_1 = s_1 \cdots s_{2i}$ and $\sigma_2 = s_{2i+1}\cdots s_{2m}$ such that $\sigma_1 \in B(2i,1)$ and $\sigma_2 \in B(2m-2i,k-1)$. □

Now, we focus on the generating function of the sequence $\{b(n,k)\}_{n=0}^{\infty}$. First we find the generating function $B(z)$ of $\{b(n,1)\}_{n=0}^{\infty}$:

$$\begin{aligned} B(z) &= \sum_{i=0}^{\infty} b(i,1)z^i = \sum_{i=1}^{\infty} b(2i,1)z^{2i} = 2\sum_{i=1}^{\infty} C_{i-1}z^{2i} = 2z^2\sum_{i=0}^{\infty} C_i z^{2i} = 2z^2C(z^2)\\ &= 1-\sqrt{1-4z^2}. \end{aligned}$$

Proposition 7. *Let k be a positive integer. Then generating function of the sequence $\{b(n,k)\}_{n=0}^{\infty}$ is $B^k(z) = 2^k z^{2k} C^k(z^2)$.*

Proof. Proposition 6 implies that the generating function of $\{b(n,k)\}_{n=0}^{\infty}$ is the product of $B(z)$ and the generating function of $\{b(n,k-1)\}_{n=0}^{\infty}$. Then,the proof follows inductively: generating function of $\{b(n,k)\}_{n=0}^{\infty}$ for $k=2$ is $B(z)B(z) = B^2(z)$. For $k=3$ we have $B(z)B^2(z) = B^3(z)$ and so on. □

For the sake of completeness we let $B^0(z)$ be the identity function.

Theorem 8. *For any positive integers n and k, the quantities $b(n,k)$ satisfy the following recursions subject to the given initial conditions.*

1. *For $k=1$*

$$b(n,1) = \begin{cases} 0 & if\ n=1, \\ 2 & if\ n=2, \\ \dfrac{4(n-3)}{n} b(n-2,1) & if\ n \geq 3. \end{cases}$$

2. *For $k=2$*

$$b(n,2) = \begin{cases} 0 & if\ n \leq 2, \\ 2b(n,1) & if\ n \geq 3. \end{cases}$$

3. *For $k \geq 3$*

$$b(n,k) = \begin{cases} 0 & if\ n < 2k, \\ 2b(n,k-1) - 4b(n-2,k-2) & if\ n \geq 2k. \end{cases}$$

Proof. 1. Initial terms are obvious and the recursion follows from (1) and (4).

2. Initial terms are obvious. Generating function of $\{b(n,2)\}_n$ satisfies

$$\begin{aligned} B^2(z) &= 4x^4 C^2(z^2) = 4z^2 \left(z^2 C^2(z^2)\right) = 4z^2 \left(C(z^2) - 1\right) = 4z^2 C(z^2) - 4z^2 \\ &= 2B(z) - 4z^2 \end{aligned}$$

which means that $b(2,2) = 2b(2,1) - 4 = 0$ and for $n > 2$, $b(n,2) = 2b(n,1)$.

3. Initial terms are obvious. For any integer $k > 2$ we have

$$\begin{aligned} B^k(z) &= 2^k z^{2k} C^k(z^2) = 2^k z^{2k-2} [C^{k-2}(z^2)][z^2 C^2(z^2)] = 2^k z^{2k-2} [C^{k-2}(z^2)][C(z^2) - 1] \\ &= 2\left(2^{k-1} z^{2k-2} C^{k-1}(z^2)\right) - 4z^2 \left(2^{k-2} z^{2k-4} C^{k-2}(z^2)\right) \\ &= 2B^{k-1}(z) - 4z^2 B^{k-2}(z) \end{aligned}$$

which implies that $b(n,k) = 2b(n,k-1) - 4b(n-2,k-2)$ for any integer $n > 2$. □

4 Recursive Relations Satisfied by $x(n,k)$

Given a positive integer n, by substituting $t=1$ in Equation (5) we observe that

$$\overline{x}_1(n)=\begin{cases} 2^n-\binom{n}{\frac{n-1}{2}} & if\ n\ is\ odd \\ 2^n-\binom{n}{\frac{n}{2}} & if\ n\ is\ even \end{cases}$$

which can be written simply as $\overline{x}_1(n)=2^n-\binom{n}{\lfloor\frac{n}{2}\rfloor}$. On the other hand, by definition, $x_1(n)=2^n-\overline{x}_t(n)$ which gives the number of strings which do not intersect the line $y=1$ as

$$x_1(n,0)=x_1(n)=\binom{n}{\lfloor\frac{n}{2}\rfloor}. \tag{7}$$

Now, let $\sigma\in X_0(n)$ and assume that $s_1=1$, then $s_2\dots s_n\in X_1(n-1,0)$. It follows that the number of strings in $X_0(n)$ with the first term 0 is $x_1(n-1,0)=\binom{n-1}{\lfloor\frac{n-1}{2}\rfloor}$. Since the same holds for the strings with the first term 1, we obtain the number of strings which do not intersect the line $y=0$ as

$$x_0(n,0)=x_0(n)=2\binom{n-1}{\lfloor\frac{n-1}{2}\rfloor}. \tag{8}$$

Let $X_k(z)$ be the generating function of the sequence $\{x(n,k)\}_{n=0}^{\infty}$ and for the special case $k=0$ write $X(z)=X_0(z)$. We have $X(z)=\sum_{i=0}^{\infty}x(i,0)z^i$, where we let $x(0,0)=1$. We can write this function as $X(z)=\sum_{i=0}^{\infty}x(2i,0)z^{2i}+x(2i+1,0)z^{2i+1}$. From (5) we obtain $x(2i,0)=2\binom{2i-1}{i}=\binom{2i}{i}$ and $x(2i+1,0)=2\binom{2i}{i}$, thus

$$X(z)=\sum_{i=0}^{\infty}\left(\binom{2i}{i}+2\binom{2i}{i}z\right)z^{2n}=(1+2z)\sum_{i=0}^{\infty}\binom{2i}{i}z^{2i}.$$

Now, from (3) we write $\sum_{i=1}^{\infty}\binom{2i}{i}z^{2i}=C(z^2)+z^2C'(z^2)$ which leads to

$$X(z)=(1+2z)(C(z^2)+z^2C'(z^2)). \tag{9}$$

Using the substitutions $z^2C'(2)=\frac{C(z^2)-1}{1-2z^2C(z^2)}$ and $z^2C^2(z^2)=C(z^2)-1$ in (8):

$$\begin{aligned} X(z) &= (1+2z)\left(C(z^2)+\frac{C(z^2)-1}{1-2z^2C(z^2)}\right)=(1+2z)\left(\frac{2C(z^2)-2z^2C^2(z^2)-1}{1-2z^2C(z^2)}\right) \\ &= \frac{1+2z}{1-2z^2C(z^2)}=\frac{1+2z}{1-B(z)}=\frac{1+2z}{\sqrt{1-4z^2}}=\sqrt{\left(\frac{1+2z}{1-2z}\right)} \end{aligned}$$

Proposition 9. *For any positive integer n, $x(n,0)=2\binom{n-1}{\lfloor\frac{n-1}{2}\rfloor}$, and for any integer $k>1$, $x(n,k)=\sum_{i=1}^{\lfloor n/2\rfloor}b(2i,k-1)x(n-2i,0)$.*

Proof. Let $k > 1$ and consider a string $\sigma \in X(n,k)$. Assume that the last balance point is s_{2i}. Then, σ can be separated into two substrings $\sigma_1 = s_1 \cdots s_{2i}$ and $\sigma_2 = s_{2i+1} \cdots s_n$ such that $\sigma_1 \in B(2i,k)$ and $\sigma_2 \in B(n-2i, k-1)$.

□

Proposition 10. *For any positive integer k, generating function of the sequence $\{x(n,k)\}_{n=0}^{\infty}$ is $X_k(z) = X(z)B^k(z)$.*

Proof. Previous proposition implies that $X_k(z) = X_{k-1}(z)B(z)$. Then, for $X_1(z) = X(z)B(z)$ and the assertion follows inductively. □

With the notation of the above proposition, if we substitute $k = 0$, we see that $X_0(z) = X(z)B^0(z) = X(z)$.

Theorem 11. *For any nonnegative integers n and k, the quantities $x(n,k)$ satisfy the following recursions subject to the given initial conditions:*

$$k = 0 \implies x(n,0) = \begin{cases} 1 & if\ n = 0 \\ 2 & if\ n = 1 \\ 2(1 - \dfrac{1}{n})x(n-1,0) & if\ n \geq 2\ is\ even \\ 2x(n-1,0) & if\ n \geq 3\ is\ odd \end{cases}$$

$$k = 1 \implies x(n,1) = \begin{cases} 0 & if\ n \leq 1 \\ x(n,0) & if\ n \geq 2 \end{cases}$$

$$k \geq 2 \implies x(n,k) = \begin{cases} 0 & if\ n < 2k \\ 2x(n,k-1) - 4x(n-2,k-2) & if\ n \geq 2k \end{cases}$$

5 Recursive Relations Satisfied by $x_t(n,k)$

We have defined $X_t(n,k)$ to be the set of strings which intersect the line $y = t$ at exactly k terms. For $t = 0$ we have already obtained recursive relations by which $[x_0(n,k)]$ can be computed effectively. So, we focus on the case $t \neq 0$ and since $x_{-t}(n,k) = x_t(n,k)$, without loss of generality we can assume that t is positive.

Proposition 12. *Given integers $n, k \geq 0$ and $t > 0$. If $n < t + 2k - 2$, then $x_t(n,k) = 0$. If $n \geq t + 2k - 2$, then $x_1(n,k) = \frac{1}{2}x(n+1,k)$,*

$$x_2(n,k) = \begin{cases} x_1(n+1,0) & if\ k = 0 \\ x_1(n+1,k) - x(n,k-1) & if\ k \geq 1 \end{cases}$$

$$x_t(n,k) = x_{t-1}(n+1,k) - x_{t-2}(n,k) \qquad (t \geq 3)$$

Theorem 13. *Let $n \geq 0, k \geq 0$ and $t \geq 1$ be integers. The numbers $x_t(n,k)$ satisfy the following recursions:*

$$x_t(n,k) = \begin{cases} x_1(n,k) = \dfrac{1}{2}x(n+1,k) & if\ t = 1 \\ \dfrac{1}{2}(x_{t-1}(n+1,0) + x_{t-1}(n+1,1)) & if\ t \geq 2\ and\ k = 0 \\ x_t(n,k) = \dfrac{1}{2}x_{t-1}(n+1,k+1) & if\ t \geq 2\ and\ k \geq 1 \end{cases}$$

Theorem 14. *Let n, k, and t be nonnegative integers. The table $[p_t(n,k)]$ can be constructed by the following recursions*

i. $t = 0$ *and* $k = 0 \implies p_0(n,0) = \begin{cases} 1 & if\ n = 0, \\ 1 & if\ n = 1, \\ (1 - \frac{1}{n})x_0(n-1,0) & if\ n \geq 2\ is\ even, \\ p_0(n-1,0) & if\ n \geq 3\ is\ odd. \end{cases}$

ii. $t = 0$ *and* $k = 1 \implies p_0(n,1) = \begin{cases} 0 & if\ n \leq 1, \\ p_0x(n,0) & if\ n \geq 2. \end{cases}$

iii. $t = 0$ *and* $k \geq 2 \implies p_0(n,1) = \begin{cases} 0 & if\ n < 2k, \\ 2p_0(n,k-1) - p_0(n-2,k-2) & if\ n \geq 2k. \end{cases}$

iv. $t = 1 \implies p_1(n,k) = p_0(n+1,k)$.

v. $t \geq 2$ *and* $k = 1 \implies p_t(n,0) = p_{t-1}(n+1,0) + p_{t-1}(n,1)$.

vi. $t \geq 2$ *and* $k \geq 2 \implies p_t(n,k) = p_{t-1}(n+1,k+1)$.

Proof. Just substitute $p_t(n,k) = 2^{-n}x_t(n,k)$ in Theorem 11 and Theorem 13. □

6 RW-9 Random Walk Tests

We propose a family of randomness tests based on random walk statistics, namely RW-9 random walk tests. RW-9 random walk tests first convert a binary string to a random walk and then count the number of times that a random walk intersect the line $y = t$. The input of the test is a collection of binary strings with equal length n. We apply the test function to determine the number of intersections with the line $y = t$ in each string, and call them as observed values. Afterwards, we apply χ^2 test and produce p-value using the bin probability tables (as described in [8]). We give the probabilities for $n \in \{128, 256, 1024, 4096\}$. It should be noted that the 9 test statistics defined in this paper are not necessarily independent.

6.1 Walkthrough

Tables 2, 3, 4, and 5 present the number of bins, bin values and the probabilities corresponding to each bins, for $n = 128, 256, 1024$ and 4096 respectively. As an example, to test the randomness of a collection of N binary strings of length $n = 128$, the first row of Table 2, that is the line labeled as "$y = 0$" suggests the use of 8 bins, and gives the expected values of the number of excursions to be 0 or 1 as $0.140772 \times N$, to be 2 or 3 as $0.138555 \times N$, ..., to be between 17 and 128 as $0.107782 \times N$.

The procedure to test a collection of N binary strings of length n, using the Random Walk Tests family can be summarized as follows:

1. Determine the corresponding number of bins for each of the test functions, that is, the number of intersections of the random walk with the line $y \in \{0, \pm1, \pm2, \pm3, \pm4\}$.
2. Apply χ^2 Goodness of Fit Test, that is evaluate

$$\chi^2 = \sum_{i=1}^{B} \frac{(O_i - N \cdot p_i)^2}{N \cdot p_i} \quad \text{and} \quad p\text{-value} = \texttt{igamc}\left(\frac{B-1}{2}, \frac{\chi^2}{2}\right)$$

   where p_i's are obtained from bin probability tables 2, 3, 4, and 5.
3. If p-value$< \epsilon$, conclude that the null hypothesis H_0 (the randomness hypothesis) is rejected, otherwise accepted. In cryptographic applications, ϵ is usually set to 0.01.

7 Application

This section reveals the results obtained from the application of the Random Walk Tests to various collections of strings in order to show the sensitivity of the tests. For this purpose, we generate pseudorandom and non-random data sets. The details are as follows.

First, we apply the tests on the outputs of AES-128, SHA-2 Family and MD5 which are considered as random looking. For generating AES-128 outputs, 128-bit representations of the numbers from 0 to 100,000 are encrypted with all-zero key. Note that the data is encrypted using ECB mode and padding is discarded. The resulting sequence is used for 128-bit testing. Moreover, additional sets of 128, 256 and 512-bit sequences are generated using the iteration $S_i = H(S_{i-1})$ where $S_0 = H(\overline{0})$ and H is the hash function MD5, SHA-2 256 and SHA-2 512 respectively. In this case, the length of $\overline{0}$ is the message block size of the hash function H. Then, the binary representations of the decimal parts of π and $\sqrt{2}$ are tested. For each number, we take as many bits so that 100,000 1024-bit and 4096-bit sequences are generated respectively.

The above mentioned strings measure the behavior of the test on random data. We also generate a *1% weight biased* sequence in order to see if the tests can detect non-random data. For this purpose, using the random number generator of Microsoft .Net Framework, we generate 100,000 128 bit sequences where each bit is 1 with probability 50,5% and 0 with probability 49,5%. The results are given in Table 1. According to the results the first five generators pass all the tests (since all the p values are greater than 0.01) while the biased sequence fails all the tests.

Table 1: Application of randomness tests to different pseudorandom number generators and biased sequences for $N = 100,000$

a	$\sqrt{2}$(4096-Bit)	π(1024-Bit)	SHA-2(256-Bit)	MD5(128-Bit)	AES(128-Bit)	1% Biased(128-Bit)
$y = 0$	0.651536	0.765225	0.723788	0.595462	0.794321	0.000121
$y = 1$	0.261310	0.257546	0.111009	0.785019	0.627966	1.01E-92
$y = -1$	0.862806	0.795376	0.014390	0.495422	0.664016	1.56E-37
$y = 2$	0.176344	0.452462	0.936082	0.728649	0.947433	7.30E-262
$y = -2$	0.631532	0.062998	0.717032	0.864984	0.545166	5.62E-181
$y = 3$	0.708952	0.226330	0.277121	0.788715	0.570326	0
$y = -3$	0.431498	0.127274	0.027632	0.670893	0.519191	4.25E-253
$y = 4$	0.581227	0.780811	0.116235	0.317354	0.452234	0
$y = -4$	0.689942	0.020685	0.097331	0.720714	0.654505	0

8 Conclusion

In this work, we define a family of randomness tests based on random walk statistics. We give recursive formulas that are feasible to compute to obtain the exact probabilities for the number of excursions in a string, namely, the number of strings which intersect the line $y = t$ exactly k times. Moreover, using the exact distributions for all random walk statistics obtained, we introduce a new statistical randomness test suite, RW-9, consisting of 9 tests. Afterwards, we apply the family of these randomness tests to various collections of strings, consisting of accepted as random looking ones and biased ones. The results suggest that the tests defined are all sensitive to both random and non-random data. The sequences generated by $\sqrt{2}$, π, SHA-2 512, SHA-2 256, MD-5 and AES-128 produced p-values greater than 0.01 for all tests, while, biased sequence failed in all 9 tests. As a future work, the correlations and the dependencies of the defined randomness tests will be studied.

References

[1] Maurer U. A universal statistical test for random bit generators. J Cryptol 1992;5:89-105.

[2] L'Ecuyer P, Simard R. Testu01: A c library for empirical testing of random number generators. ACM T Math Software 2007;33(4):22.

[3] Doğanaksoy A, Sulak F, Uğuz M, Şeker O, Akcengiz Z. New Statistical Randomness Tests Based on Length of Runs. Math Probl Eng 2015.

[4] M. Sönmez Turan, A. Doğanaksoy, and S. Boztaş. On independence and sensitivity of statistical randomness tests. In International Conference on Sequences and Their Applications (SETA), 2008.

[5] Sulak F, Uğuz M, Koçak O, and Doğanaksoy A (2017) "On the independence of statistical randomness tests included in the NIST test suite," Turkish Journal of Electrical Engineering and Computer Sciences: Vol. 25: No. 5, Article 15.

[6] Rukhin AL, Soto J, Nechvatal J, Smid M, Barker E, Leigh S, Levenson M, Vangel M, Banks D, Heckert A et. al. A statistical test suite for random and pseudorandom number generators for cryptographic applications Sp 800-22 rev. 1a. Gaithersburg, MD, USA: Booz-Allen and Hamilton Inc Mclean Va, 2010.

[7] Doğanaksoy A, Çalık Ç, Sulak F, Turan MS. New Randomness Tests Using Random Walk. In 2nd National Conference Proceedings; 15-17 December 2006; Ankara, Turkey.

[8] Sulak F, Doğanaksoy A, Ege B, Koçak O. Evaluation of randomness test results for short sequences. In: Carlet C, Pott A editors. Sequences and Their Applications - SETA10 6th International Conference Proceedings; 13-17 September 2010; Paris, France. Berlin:Springer-Verlag, 2010, pp.309-319.

[9] Daeman J, Rijmen V. The Design of Rijndael: AES - The Advanced Encryption Standard. Berlin, Germany:Springer-Verlag Berlin Heidelberg, 2002.

Appendix

Table 2: Bin values and expected probabilities for $n = 128$.

	Bin-1	Bin-2	Bin-3	Bin-4	Bin-5	Bin-6	Bin-7	Bin-8
y=0,1,-1	0-1	2-3	4-5	6-7	8-9	10-12	13-16	17-128
	0.140772	0.138555	0.131984	0.121481	0.107849	0.132083	0.119493	0.107782
y=2,-2	0	1-2	3-4	5-6	7-8	9-11	12-15	16-128
	0.139689	0.137524	0.131103	0.120833	0.107487	0.132098	0.120326	0.110939
y=3,-3	0	1-2	3-4	5-6	7-8	9-11	12-15	16-128
	0.208993	0.134829	0.126409	0.114484	0.099982	0.119954	0.105395	0.089954
y=4,-4	0	1-2	3-4	5-6	7-9	10-13	14-128	-
	0.275146	0.130239	0.120194	0.107125	0.132093	0.12112	0.114083	-
y=5,-5	0	1-3	4-6	7-10	11-128	-	-	-
	0.341299	0.18428	0.155113	0.152257	0.167051	-	-	-

Table 3: Bin values and expected probabilities for $n = 256$.

	Bin-1	Bin-2	Bin-3	Bin-4	Bin-5	Bin-6	Bin-7	Bin-8
y=0,1,-1	0-2	3-4	5-7	8-10	11-13	14-17	18-23	24-256
	0.149262	0.097882	0.140597	0.129088	0.114006	0.124929	0.128544	0.115691
y=2,-2	0-1	2-4	5-7	8-10	11-13	14-17	18-22	23-256
	0.148685	0.145223	0.136791	0.124096	0.108276	0.116979	0.102695	0.117257
y=3,-3	0	1-3	4-6	7-9	10-12	13-16	17-21	22-256
	0.148685	0.145223	0.136791	0.124096	0.108276	0.116979	0.102695	0.117257
y=4,-4	0	1-2	3-5	7-8	9-11	12-15	16-21	22-256
	0.196977	0.09583	0.136356	0.123798	0.108137	0.117033	0.118411	0.103459
y=5,-5	0	1-2	3-4	5-7	8-10	11-14	15-20	21-256
	0.245269	0.094143	0.08975	0.123798	0.108137	0.117033	0.118411	0.103459

Table 4: Bin values and expected probabilities for $n = 1024$.

	Bin-1	Bin-2	Bin-3	Bin-4	Bin-5	Bin-6	Bin-7	Bin-8
y=0,1,-1	0-4	5-9	10-14	15-20	21-27	28-35	36-47	48-1024
	0.124395	0.121977	0.116671	0.129449	0.132296	0.122905	0.127728	0.124579
y=2,-2	0-3	4-8	9-13	14-19	20-26	27-34	35-46	47-1024
	0.124275	0.121863	0.116572	0.12936	0.13224	0.122904	0.127822	0.124965
y=3,-3	0-2	3-7	8-12	13-18	19-25	16-33	34-45	46-1024
	0.124275	0.121863	0.116572	0.12936	0.13224	0.122904	0.127822	0.124965
y=4,-4	0-1	2-6	7-11	12-17	18-24	25-32	33-44	45-1024
	0.124154	0.121749	0.116474	0.129271	0.132184	0.122903	0.127915	0.12535
y=5,-5	0	1-5	6-10	11-16	17-23	24-31	32-43	44-1024
	0.124154	0.121749	0.116474	0.129271	0.132184	0.122903	0.127915	0.12535

Table 5: Bin values and expected probabilities for $n = 4096$.

	Bin-1	Bin-2	Bin-3	Bin-4	Bin-5	Bin-6	Bin-7	Bin-8
y=0,1,-1	0-9	10-19	20-30	31-42	43-55	56-72	73-96	97-4096
	0.124297	0.121591	0.127252	0.1274	0.121105	0.128538	0.124726	0.125092
y=2,-2	0-8	9-18	19-29	30-41	42-54	55-71	72-95	96-4096
	0.124267	0.121562	0.127226	0.127379	0.121093	0.128538	0.124749	0.125186
y=3,-3	0-7	8-17	18-28	29-40	41-53	54-70	71-94	95-4096
	0.124267	0.121562	0.127226	0.127379	0.121093	0.128538	0.124749	0.125186
y=4,-4	0-6	7-16	17-27	28-39	40-52	53-69	70-93	94-4096
	0.124237	0.121534	0.127199	0.127357	0.121081	0.128538	0.124773	0.12528
y=5,-5	0-5	6-15	16-26	27-38	39-51	52-68	69-92	93-4096
	0.124237	0.121534	0.127199	0.127357	0.121081	0.128538	0.124773	0.12528

Invited Talk: Pseudorandom Sequences for Grant-Free Access in Massive Machine-Type Communications

Nam Yul Yu

Gwangju Institute of Science and Technology (GIST), Gwangju, South Korea

Abstract. Massive machine-type communications (mMTC) is an important use case of 5G and beyond wireless technology for concretizing the Internet of Things (IoT). In mMTC, grant-free access is a key enabler for connecting wireless devices with low latency and low signaling overhead. In uplink grant-free access, user-specific, non-orthogonal sequences are uniquely assigned to devices for non-orthogonal multiple access (NOMA), where each active device attempts to access a base station (BS) using its own sequence. Then, a BS receiver has to identify active devices, estimate channel profiles, and detect transmitted data, through the superimposed sequences from active devices. Exploiting the sparse activity, the principle of compressed sensing (CS) has been widely used to perform joint activity detection, channel estimation, and data detection for uplink grant-free access in mMTC.

In this talk, some applications of pseudorandom sequences for uplink grant-free access in mMTC are introduced. First of all, Golay complementary sequences are used for spreading sequences in uplink grant-free NOMA. From the properties of Golay complementary sequences, the spreading sequences provide low peak-to-average power ratio (PAPR) for multicarrier transmission. Also, a theoretical connection to Reed-Muller codes shows that the spreading sequences guarantee theoretically bounded low coherence for the spreading matrix. Second, a design framework is presented for non-orthogonal signature sequences, where the design principle relies on unimodular masking sequences represented by characters over finite fields. The Weil bounds on character sums are leveraged to show that the signature sequence matrix has theoretically bounded low coherence. Simulation results demonstrate that the spreading and the signature sequences achieve excellent performance of joint activity detection, channel estimation, and data detection for uplink grant-free access in mMTC. Thanks to the algebraic structure, the non-orthogonal sequences enjoy the benefits of small phases and small storage space in practical implementations. Finally, potential applications of pseudorandom sequences for mMTC will be discussed as a future research topic.

Multiple Spectrally Null Constrained Complete Complementary Codes of Various Lengths Over Small Alphabet

Rajen Kumar*, Palash Sarkar†, Prashant Kumar Srivastava‡, Sudhan Majhi §

Abstract

Complete complementary codes (CCCs) are highly valuable in the fields of information security, radar and communication. The spectrally null constrained (SNC) problem arises in radar and modern communication systems due to the reservation or prohibition of specific spectrums from transmission. The literature on SNC-CCCs is somewhat limited in comparison to the literature on traditional CCCs. The main objective of this paper is to discover several configurations of SNC-CCCs that possess more flexibility in their parameters. The proposed construction utilised the existing CCCs and mutually orthogonal sequences. The proposed construction can cover almost all lengths with the smallest alphabets $\{-1, 0, 1\}$. Further, the idea of SNC-CCC is extended to multiple SNC-CCCs with an inter-set zero cross-correlation zone (ZCCZ). Through the propose construction, we could control the cross-correlation magnitude outside the ZCCZ. Consequently, the resulting codes possess both aperiodic and periodic inter-set ZCCZ and feature a low magnitude of cross-correlation value outside the ZCCZ.

A Golay complementary pair (GCP) indicates a pair of sequences whose sum of aperiodic auto-correlation functions (AACFs) results in zero at nonzero time shifts. Golay uncovered a sequence pair that can be used during the research of multislit spectroscopy [1, 2]. GCPs are comprehensively utilised in engineering applications, particularly in radar systems and communication systems. These applications include channel estimation [3, 4], design of the physical uplink control channel [5], non-orthogonal multiple access [6], radar

*Rajen Kumar is with the Department of Mathematics, Indian Institute of Technology Patna, India, email:rajen_2021ma04@iitp.ac.in. The work of Rajen Kumar was supported in part by the CSIR, India, under award letter 09/1023(0034)/2019-EMR-I.

†Palash Sarkar is with the Department of Informatics, Selmer Center, University of Bergen, Norway, email:palash.sarkar@uib.no. The work of Palash Sarkar was supported by the Research Council of Norway under Grant 311646/O70.

‡Prashant Kumar Srivastava is with the Department of Mathematics, Indian Institute of Technology Patna, India, email:pksri@iitp.ac.in.

§Sudhan Majhi is with the Department of Electrical Communication and Engineering, Indian Institute of Science Bangalore, India, email:smajhi@iisc.ac.in. The work of Sudhan Majhi was supported by the SERB, Govt. of India, under grant no. CRG/2022/000529 and EEQ/2022/001018.

waveform design [7], control of peak-to-average power ratio for multi-carrier communication systems [8], and more. Tseng and Liu presented the idea of a Golay complementary set (GCS) comprising more than two sequences. The sum of the AACFs for all sequences is zero except at zero time shift [9]. Due to their similar characteristics to GCPs, GCSs are also utilised in several communication and radar systems [10, 11]. Furthermore, GCS has the added benefit of a greater code rate compared to GCP, in addition to its variable length advantage [12–14].

A mutually orthogonal Golay complementary set (MOGCS) is a collection of K GCSs. Each GCS in the MOGCS has M sequences, each of length L. Additionally, the cross-correlation function between distinct GCSs is zero. A MOGCS is referred to as a complete complementary code (CCC) when K is equal to M [15]. For implementing multi-antenna or multi-user systems, it is important to consider the cross-correlation characteristics across sets of sequences. This is particularly relevant for systems such as CCC based code division multiple access (CDMA) and multi-input multi-output (MIMO) radar [16–19]. The idea of CCC extended to multiple CCC with an inter-set zero cross-correlation zone (ZCCZ) [20, 21], which is similar to the Z complementary code set (ZCCS). The idea of CCC also extended to multiple CCC with inter-set low cross-correlation, which is similar to the Quasi complementary code set (QCCS).

In systems that use orthogonal frequency division multiplexing (OFDM), some sub-carriers are designated as reserved and are not allowed to transmit signals [22]. For instance, the direct current sub-carrier is specifically allocated, known as spectrally null constrained (SNC), to prevent any discrepancies in the D/A and A/D converters during radio frequency transmission [23]. The increasing need for OFDM or multi-carrier CDMA sequences with spectrum null constraints, also known as non-contiguous sequences, is primarily motivated by their potential applications in cognitive radio (CR) communications [24]. Transmission on sub-carriers not used by primary users constrains secondary users in OFDM-based CR transmissions. The Third-Generation Partnership Project Long-Term Evolution enhanced licenced-assisted access and the New Radio in Unlicenced (NR-U) implemented interlaced transmission, with the null locations of the SNC sequences being regularly distributed (although the nulls in NR-U are unevenly spaced). It is also important to think about the spectral null constraint when using the CCC as omnidirectional precoding for a rectangular array that is not all the same size. In the IEEE P802.15.4z standard, the average power permitted in ultra-wide-band is very low. Therefore, the sequence design will consider the inclusion of null to decrease the average power. To summarise, several situations in sequence design require the use of null constraints.

Only a few of the conventional GCSs and CCCs take into account this limitation, which has been addressed in [5, 23, 25–29]. Sahin and Yang extended the conventional GCPs to address the SNC problem, as described in [5] and [26]. In [23], Zhou *et al.* sequentially built the SNC-MOGCSs/SNC-GCSs using an iterative approach. They used two sequences extracted from a GCP as the initial seed sequence and then introduced a certain amount of zeros into these two sequences. As a result, new sequences were obtained with a zero correlation zone. Hence, a challenging issue arises regarding the methodology for constructing SNC-CCC. Shen *et al.* proposed a method for constructing SNC-CCC using extended Boolean functions and graphs [28]. However, the parameters are only in

the power of p when elements of code are considered from the qth root of unity and zero, for $p \mid q$ and $p \geq 2$. In machine-type communication, alphabet size plays a major role and must be minimum [30]. However, there are gaps in the SNC-CCC proposed in [28] in terms of lengths and alphabet sizes. For example, when the alphabets are $-1, 1, 0$, set size, code size and length are restricted to in the form of the power-of-two. We are strongly motivated to include a greater range of parameters for SNC-CCC in comparison to existing literature. The proposed construction not only provides SNC-CCCs with new parameters but also provides flexibility in the alphabet and the length of the constituent sequences. It may be noted that codes are referred to as CCC, when it is a traditional CCC, and codes with nulls are referred to as SNC-CCC.

In the proposed construction, we use existing CCCs and mutually orthogonal sequences (MOSs) as seeds. By performing the concatenation operation in a specific way, as described in Section 2, we obtain multiple SNC-CCCs over a small alphabet. It may be noted that our smallest alphabet is $\{-1, 0, 1\}$, on which the proposed construction is capable of generating almost all possible lengths. The proposed multiple SNC-CCCs also have a ZCCZ property with respect to both periodic and aperiodic correlation. With these properties, the obtained code set is useful for multi-cell MC-CDMA systems, where the users inside a cell enjoy interference-free communication due to the ideal correlation property of a SNC-CCC and the users from two different cells also enjoy interference-free communication within the ZCCZ. Our study also revealed that we can control non-zero inter-set cross-correlation magnitude values outside the ZCCZ. We consider this an opportunity to minimise the upper bound for inter-set cross-correlation magnitude values of the proposed multiple SNC-CCCs.

We structure the subsequent sections of the paper as follows: Section 1 establishes appropriate notations and definitions. Section 2 introduces new constructions for SNC-CCC and multiple SNC-CCC and provides an example to illustrate this. Further, we explain the ZCCZ width of the multiple SNC-CCC and conclude with the low inter-set cross-correlation value. In Section 3, a comparison has been given with existing literature. Based on the proposed work, we have highlighted three problems that we may consider as our future work in Section 4. The paper is concluded in Section 5.

1 Preliminaries

Before anything starts, let us specify the notation and definitions that will be utilised consistently throughout this paper.

Definition 1. Let $\mathbf{a} = (a_1, a_2, \ldots, a_L)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_L)$ be two complex-valued sequences of length L and τ be an integer. Define

$$\mathcal{C}(\mathbf{a}, \mathbf{b})(\tau) = \begin{cases} \sum_{i=1}^{L-\tau} a_{i+\tau} b_i^*, & 0 \leq \tau < L, \\ \sum_{i=1}^{L+\tau} a_i b_{i-\tau}^*, & -L < \tau < 0, \\ 0, & \text{otherwise}, \end{cases} \tag{1}$$

is called ACCF of $\mathbf{a}$ and $\mathbf{b}$ at time shift τ, where $(\cdot)^*$ represents complex conjugation. When $\mathbf{a} = \mathbf{b}$, $\mathcal{C}(\mathbf{a}, \mathbf{b})(\tau)$ is called AACF of $\mathbf{a}$ and is denoted by $\mathcal{C}(\mathbf{a})(\tau)$. Further, periodic

cross-correlation function (PCCF) of $\mathbf{a}$ and $\mathbf{b}$ at time shift τ is defined as

$$\Theta(\mathbf{a},\mathbf{b})(\tau) = \mathcal{C}(\mathbf{a},\mathbf{b})(\tau) + \mathcal{C}(\mathbf{a},\mathbf{b})(\tau - L). \tag{2}$$

Definition 2. Let $\mathbf{C} = \{C_k : 1 \le k \le M\}$ be a set of M matrices (codes), each having order $M \times L$. And C_k is defined as

$$C_k = \begin{bmatrix} \mathbf{c}_1^k \\ \mathbf{c}_2^k \\ \vdots \\ \mathbf{c}_M^k \end{bmatrix}_{M\times L}, \tag{3}$$

where $\mathbf{c}_j^k (1 \le j \le M, 1 \le k \le K)$ is the j-th row sequence of C_k.Then ACCF between C_{k_1} and C_{k_2} is defined by

$$\mathcal{C}\left(C_{k_1}, C_{k_2}\right)(\tau) = \sum_{\nu=1}^{M} \mathcal{C}\left(\mathbf{c}_\nu^{k_1}, \mathbf{c}_\nu^{k_2}\right)(\tau). \tag{4}$$

When $C_{k_1} = C_{k_2}$, $\mathcal{C}(C_{k_1}, C_{k_2})(\tau)$ is called AACF of C_{k_1} and is denoted by $\mathcal{C}(C_{k_1})(\tau)$. Similarly, the PCCF of between C_{k_1} and C_{k_2} is defined by

$$\Theta\left(C_{k_1}, C_{k_2}\right)(\tau) = \sum_{\nu=1}^{M} \Theta\left(\mathbf{c}_\nu^{k_1}, \mathbf{c}_\nu^{k_2}\right)(\tau). \tag{5}$$

Definition 3. Let $\mathbf{a} = (a_1, a_2, \ldots, a_L)$ be any complex-valued sequence and $N = \{x \in \mathbb{N} : a_x = 0\}$ is non-empty set, $\mathbf{a}$ is called a SNC sequence. A CCC is called an SNC-CCC if there is at least one SNC sequence in the CCC [28].

Definition 4. Let $\mathbf{C} = \{C_k : 1 \le k \le M\}$ be a set of M codes of order $M \times L$ and it follows

$$\mathcal{C}(C_{k_1}, C_{k_2})(\tau) = \begin{cases} ML - \epsilon & k_1 = k_2, \tau = 0 \\ 0 & \text{otherwise,} \end{cases} \tag{6}$$

where, ϵ is the number of zeros in a code. When $\epsilon = 0$, it is referred to as traditional aperiodic CCC and for $\epsilon \ge 1$, we refer to it as aperiodic SNC-CCC. It is trivial that aperiodic CCC also satisfies the ideal periodic correlation properties. Therefore, an aperiodic CCC can also be called a periodic CCC. To avoid possible confusion between the terms aperiodic and periodic CCC, we will exclusively use the term CCC throughout this paper.

Definition 5. Let $\mathfrak{C} = \{\mathbf{C}^j : 1 \le j \le P\}$ be a collection of P many (M, L)-CCCs, i.e., $\mathbf{C}^j = \left\{C_k^j : 1 \le k \le M\right\}$, where $1 \le j \le P, P \ge 2$. If any two codes from different CCCs $\mathbf{C}^{j_1}$ and $\mathbf{C}^{j_2}$ with $1 \le j_1 \ne j_2 \le P$ follows

$$\begin{aligned} &\mathcal{C}(C_{k_1}^{j_1}, C_{k_2}^{j_2})(\tau) = 0, \ |\tau| < Z_A, \\ &\qquad \delta_A = \max\left\{|\mathcal{C}(C_{k_1}^{j_1}, C_{k_2}^{j_2})(\tau)| : j_1 \ne j_2, 1 \le k_1, k_2 \le M, Z \le |\tau| \le L-1\right\}, \end{aligned} \tag{7}$$

where $1 \le k_1, k_2 \le M$, then we denote $\mathfrak{C}$ as aperiodic (P, M, L, Z_A, δ_A)-CCCs. Similarly,

$$\begin{aligned}\Theta(C_{k_1}^{j_1}, C_{k_2}^{j_2})(\tau) = 0,\ |\tau| < Z_P,\\ \delta_P = \max\left\{|\Theta(C_{k_1}^{j_1}, C_{k_2}^{j_1})(\tau)| : j_1 \ne j_2, 1 \le k_1, k_2 \le M, Z \le |\tau| \le L-1\right\},\end{aligned} \tag{8}$$

where $1 \le k_1, k_2 \le M$, then we denote $\mathfrak{C}$ as periodic (P, M, L, Z_P, δ_P)-CCCs.

Let $\mathbf{a}$ and $\mathbf{b}$ be two complex sequences of identical length and said to be orthogonal if the dot product $\langle \mathbf{a}, \mathbf{b} \rangle$ is equal to 0. We refer to the set of sequences as MOSs when the number of sequences exceeds two and the dot product of any two sequences is zero. A construction of P many MOSs with length P is suggested in [31].

2 Proposed Construction

In this section, we describe our main method of construction. First, we provide a new method, which involves the concatenation of zeros and matrices with some scalar multiplications. Scalars must be selected meticulously to ensure they do not impact the elements of matrices following multiplication.

Construction 6. *Let $C_1, C_2, \ldots, C_P$ be a set of $M \times L$ matrices and $\mathbf{b} = (b_1, b_2, \ldots, b_P)$ be a sequence of length P. For $K > P$, then we define*

$$\mathcal{R}^{\mathcal{P}(n)}(C_1, C_2, \ldots, C_P; \mathbf{b}) = \left[\mathbf{0}^{n_1} \parallel b_1 C_1 \parallel \mathbf{0}^{n_2} \parallel b_2 C_2 \parallel \mathbf{0}^{n_3} \parallel \cdots \parallel \mathbf{0}^{n_P} \parallel b_P C_P \parallel \mathbf{0}^{n_{P+1}}\right], \tag{9}$$

where, $\mathcal{P}(n) = (n_1, n_2, \ldots, n_{P+1})$, partition of n with $P+1$ non-negative integers, $n = n_1 + n_2 + \cdots + n_{P+1}$, $\mathbf{0}^{n_1}$ represents a zero matrix of size $M \times n_1$ and $\parallel$ represents concatenation of two matrices.

First we consider a (M, L)-CCC, $P \le M$, such that $P \mid M$ and MOSs of length P. Now, for any positive integers n, we take a partition with $P+1$ non-negative integers. The partition of n decides the position and numbers of nulls in the proposed codes.

Theorem 7. *Let $\mathbf{C}$ be a (M, L)-CCC, $P \mid M$, $\mathbf{b}^1, \mathbf{b}^2, \ldots, \mathbf{b}^P$ be MOSs of length P. Now, define*

$$B_{\nu P+\mu} = \mathcal{R}^{\mathcal{P}(n)}(C_{\nu P+1}, C_{\nu P+2}, \ldots, C_{(\nu+1)P}; \mathbf{b}^\mu), \tag{10}$$

for $0 \le \nu < \frac{M}{P}$, $1 \le \mu \le P$. Then $\mathbf{B} = \{B_1, B_2, \ldots, B_M\}$ is a $(M, PL+n)$ SNC-CCC.

Since the alphabets of CCC and MOSs are identical, the resulting SNC-CCCs likewise possess the same alphabets, with an additional zero. The position of nulls can be determined by the partition of n, which is employed in the construction.

Example 8. Let

$$C_1 = \begin{bmatrix} + & + & + \\ + & + & - \\ - & + & - \\ - & + & - \end{bmatrix}, C_2 = \begin{bmatrix} + & - & + \\ + & + & - \\ - & - & + \\ + & + & + \end{bmatrix}, C_3 = \begin{bmatrix} + & - & - \\ + & + & + \\ - & + & - \\ + & - & - \end{bmatrix} \text{ and } C_4 = \begin{bmatrix} + & - & - \\ + & - & + \\ + & + & + \\ - & + & + \end{bmatrix},$$

be a $(4,3)$-CCC from [32], where $+$ and $-$ represent 1 and -1, respectively. Now, assume $P=2$, $\mathbf{b}^1=(1,1)$, $\mathbf{b}^2=(1,-1)$, $n_1=0, n_2=3$ and $n_3=0$. Then from **Theorem** 7,

$$B_1=\begin{bmatrix}++{+}000+-{+}\\ ++{-}000+{+}-\\ ++{-}000-{-}+\\ -+{-}000+{+}+\end{bmatrix},\qquad B_2=\begin{bmatrix}++{+}000-{+}-\\ ++{-}000-{-}+\\ ++{-}000+{+}-\\ -+{-}000-{-}-\end{bmatrix},$$
$$B_3=\begin{bmatrix}+-{-}000+{-}-\\ ++{+}000+{-}+\\ -+{-}000+{+}+\\ +-{-}000-{+}+\end{bmatrix},\text{ and }\quad B_4=\begin{bmatrix}+-{-}000-{+}+\\ ++{+}000-{+}-\\ -+{-}000-{-}-\\ +-{-}000+{-}-\end{bmatrix}, \tag{11}$$

is a $(4,9)$ SNC-CCC.

Remark 9. In the **Example** 8, there is the freedom to decide on various values n_1, n_2 and n_3.

Let $\pi_1, \pi_2, \ldots$ be permutations of $\{1,2,\ldots,M\}$ such that

$$\pi_{j_1}(i_1P+\mu)\neq\pi_{j_2}(i_2P+\mu), \tag{12}$$

for $j_1\neq j_2$, $0\leq i_1,i_2<\frac{M}{P}$ and $1\leq\mu<P$, we have P many such permutations.

Theorem 10. *Let* $\mathbf{C}$ *be a* (M,L)*-CCC,* $P\mid M$*,* $\mathbf{b}^1,\mathbf{b}^2,\ldots,\mathbf{b}^P$ *be MOSs of length* P *and* $\pi_0,\pi_1,\ldots,\pi_{P-1}$ *be permutations as defined in* (12)*. Now, define*

$$B_{jM+\nu P+\mu}=\mathcal{R}^{\mathcal{P}(n)}(C_{\pi_j(\nu P+1)},C_{\pi_j(\nu P+2)},\ldots,C_{\pi_j((\nu+1)P)};\mathbf{b}^\mu), \tag{13}$$

for $0\leq\nu<\frac{M}{P}$*,* $1\leq\mu\leq P$ *and* $0\leq j\leq P-1$*. Then, each* $\mathbf{B}^j=\{B_{jM+1},B_{jM+2},\ldots,B_{(j+1)M}\}$ *is a* $(M,PL+n)$ *SNC-CCC and by combining all SNC-CCCs it becomes a multiple CCCs with inter-set ZCCZ.*

Remark 11. The elements in the partition n can be used to obtain the ZCCZ width of multiple SNC-CCCs. $\lambda+L$ will be the periodic and aperiodic ZCCZ, where

$$\lambda=\min_{2\leq i\leq P}\{n_i\}. \tag{14}$$

Now, we present a method to decrease the magnitude of the cross-correlation value outside the ZCCZ.

Corollary 12. *Let* $\mathcal{P}(n)$ *be partition of* n *i.e.,* $n=n_1+n_2+\ldots+n_{P+2}$ *such that* $n_{i_1}\neq n_{i_2}$ *for* $2\leq i_1,i_2\leq P$ *in* ***Theorem*** *10 then* δ_A *become* LM*. Therefore, we have a aperiodic* $(P,M,PL+n,L+\lambda,LM)$*-CCCs. Further, if* $n_{i_1}\neq n_{i_2} \bmod L$ *for* $2\leq i_1,i_2\leq P$ *in* ***Theorem*** *10 then* δ_P *become* LM*. This type of* $\mathcal{P}(n)$ *is possible for* $n\geq\frac{P(P-1)}{2}$*. Therefore, we have a periodic* $(P,M,PL+n,L,LM)$*-CCCs.*

Let $\pi_1, \pi_2, \ldots, \pi_P$ be permutations of $\{1, 2, \ldots, M\}$ as define in (12), further for any two permutation π_{j_1} and π_{j_2}, when

$$\begin{aligned} \pi_{j_1}(i_1 P + \mu_1) =& \pi_{j_2}(i_2 P + \mu_2), \text{then} \\ \pi_{j_1}(i_1 P + \mu_1 + \alpha) \neq& \pi_{j_2}(i_2 P + \mu_2 + \alpha), \end{aligned} \tag{15}$$

for $1 \leq \mu_1 + \alpha, \mu_2 + \alpha \leq P$.

Corollary 13. ***Theorem*** *10 provides multiple SNC-CCCs such that cross-correlation is non-zero at only one time shift and the value is equal to LM when permutations satisfy* (15)*. Therefore, we have both aperiodic $(P, M, PL + n, L + \lambda, LM)$-CCCs and periodic $(P, M, PL + n, L, LM)$-CCCs.*

We are providing one more example to illustrate the multiple SNC-CCCs with ZCCZ.

Example 14. In **Example** 8, we consider as identity permutation ($\pi_1 = (1, 2, 3, 4)$) and construct a SNC-CCC. As $P = 2$, we have second permutation $\pi_2 = (4, 1, 2, 3)$ such that π_1 and π_2 satisfies (15). With the same $\mathbf{C}$, $\mathbf{b}^1$ and $\mathbf{b}^2$, we have one CCC as given in **Example** 8 and the other CCC is as given below

$$\begin{aligned} B_5 &= \begin{bmatrix} +-&-000&+&+ \\ +-&+000&+&- \\ ++&+000&-&- \\ -+&+000&-&- \end{bmatrix}, & B_6 &= \begin{bmatrix} +-&-000&-&- \\ +-&+000&-&+ \\ ++&+000&+&+ \\ -+&+000&+&+ \end{bmatrix}, \\ B_7 &= \begin{bmatrix} +-&+000&+&- \\ ++&-000&+&+ \\ --&+000&-&- \\ ++&+000&+&- \end{bmatrix}, \text{ and} & B_8 &= \begin{bmatrix} +-&+000&-&+ \\ ++&-000&-&- \\ --&+000&+&+ \\ ++&+000&-&+ \end{bmatrix}. \end{aligned} \tag{16}$$

Combining $B_1, B_2, \ldots, B_8$ is a multiple SNC-CCCs with aperiodic ZCCZ width is 6.

Choosing a set of permutations plays a role in a low correlation magnitude value. To ensure such permutation exists, we are providing an example. Let $M = 4$, $P = 4$ then $\pi_1 = (1, 2, 3, 4)$, $\pi_2 = (2, 3, 4, 1)$, $\pi_3 = (3, 4, 1, 2)$ and $\pi_4 = (4, 1, 2, 3)$, satisfy (12) but not (15). But $\pi_1 = (1, 2, 3, 4)$, $\pi_2 = (4, 3, 2, 1)$, $\pi_3 = (3, 1, 4, 2)$ and $\pi_4 = (2, 4, 1, 3)$ satisfies (15).

3 Comparison

3.1 Comparison with [26] and [33]

[26] and [33] generated SNC-GCS via generalised Boolean functions and generated parameters closely multiple of 2. Furthermore, their findings are restricted to SNC-GCSs and do not extend to SNC-CCCs. However, in the proposed construction, every code is SNC-GCSs, which are not restricted to a multiple of 2 only.

3.2 Comparision with [23]

The method in [23] implements an iterative strategy using an existing CCC to generate SNC-MOGCSs. Meanwhile, the proposed construction provides SNC-CCCs.

3.3 Comparision with [28]

SNC-CCCs has been constructed using an extended Boolean function in [28] with diversified parameters. Notably, these parameters consistently involve powers of p for $p \geq 2$, where the elements are obtained from the qth root of unity and zero for $(p \mid q)$. The given example demonstrates that the proposed construction offers more flexibility.

4 Future directions

Based on our contribution in this paper, we would like to introduce the following future works:

1. In **Corollary** 13, the set permutation used satisfying (15). However, constructing a set of permutations satisfying (15) is not straightforward. We consider it to be our future research problem.

2. In the current literature, we do not have sufficient information on the optimal collection of multiple SNC-CCCs in relation to their maximum magnitude of inter-set cross-correlation value. This limitation leads to a future direction on deriving a lower correlation bound for multiple collections of SNC-CCCs.

3. Besides, as we can see in our proposed construction of multiple SNC-CCCs, we also have a ZCCZ, which leads us to the natural question, "What will be the relationship between the ZCCZ width and the other parameters of our multiple collection of SNC-CCCs?"

5 Conclusion

In this paper, with the help of MOSs, we developed a method to construct SNC-CCCs, with flexible parameters. The proposed construction can cover almost all the possible lengths over the alphabet $\{-1, 0, 1\}$. Further, we have extended the construction to produce multiple SNC-CCCs with inter-set ZCCZ. The proposed construction includes a wider range of parameters in relation to length and alphabet size. Furthermore, we have shown that restriction can be made on the highest cross-correlation magnitude value outside the ZCCZ width, assuring that the multiple SNC-CCCs possess not only inter-set ZCCZ width but also exhibit a low cross-correlation magnitude value outside the ZCCZ width.

6 Proof of Theorems

In this section we complete the proof of Theorem 7 and Theorem 10.

Proof of Theorem 7. We complete the proof in two parts, one is for AACF and second is for ACCF values.

Case 1. Let $1 \leq t_1 = \nu_1 P + \mu_1 \leq M$ and $\tau \neq 0$, then $\mathcal{C}(B_{t_1})(\tau)$ is written as linear sum of AACF of a code at non-zero time shift and ACCF between two different codes from $\{C_{\nu_1+1}, C_{\nu_1+2}, \ldots, C_{\nu_1+P}\}$, which results $\mathcal{C}(B_{t_1})(\tau) = 0$ for any τ except at $\tau = 0$.

Case 2. Consider two distinct integer $n_1 = \nu_1 P + \mu_1$ and $n_2 = \nu_2 P + \mu_2$ such that $1 \leq \nu_1 P + \mu_1 \neq \nu_2 P + \mu_2 \leq M$, for $0 \leq \nu < \frac{M}{P}$, $1 \leq \mu \leq P$. Again, we consider two subcases on the basis of ν_1, ν_2 to complete the proof.

Subcase (i): $\nu_1 = \nu_2$. Since $\mathbf{b}^{\nu_1}$ is orthogonal to $\mathbf{b}^{\nu_2}$, it implies that $\langle \mathbf{b}^{\nu_1}, \mathbf{b}^{\nu_2} \rangle = 0$. Therefore,

$$\mathcal{C}(B_{t_1}, B_{t_2})(0) = \mathbf{b}^{\nu_1} \cdot \mathbf{b}^{\nu_2 *} \sum_{i=1}^{P} \mathcal{C}(C_{\nu_1+i})(0) = 0. \tag{17}$$

Now, assume $\tau \neq 0$, then $\mathcal{C}(B_{t_1}, B_{t_2})(\tau)$ is a linear sum of ACCF between two different codes from $\{C_{\nu_1+1}, C_{\nu_1+2}, \ldots, C_{\nu_1+P}\}$, which results $\mathcal{C}(B_{t_1}, B_{t_2})(\tau) = 0$.

Subcase (ii): $\nu_1 \neq \nu_2$, then $\mathcal{C}(B_{t_1}, B_{t_2})(\tau)$ is written as linear sum of AACF of a code at non-zero time shift and ACCF between two different codes from $\{C_{\nu_1+1}, C_{\nu_1+2}, \ldots, C_{\nu_1+P}$, $C_{\nu_2+1}, C_{\nu_2+2}, \ldots, C_{\nu_2+P}\}$, which results $\mathcal{C}(B_{t_1}, B_{t_2})(\tau) = 0$ for any τ.

From the above cases the proof is complete. □

Proof of Theorem 10. Each $\mathbf{B}^j$ is a $(M, PL + n)$ SNC-CCC, for $1 \leq j \leq P - 1$. Now, consider $B_{t_1}^{j_1} \in \mathbf{B}^{j_1}$ and $B_{t_2}^{j_2} \in \mathbf{B}^{j_2}$. The value of $\mathcal{C}(B_{t_1}^{j_1}, B_{t_2}^{j_2})(\tau)$ become non-zero when it include AACF of any code from $\{C_1, C_2, \ldots, C_M\}$, that happens only for $\tau = L + n_i$ for some $2 \leq i \leq P$. There for $\mathcal{C}(B_{t_1}^{j_1}, B_{t_2}^{j_2})(\tau) = 0$ for $|\tau| < L + \lambda$, where $\lambda = \min\{n_i : 2 \leq i \leq P\}$. This completes the proof. □

References

[1] Marcel J. E. Golay. Static multislit spectrometry and its application to the panoramic display of infrared spectra*. *J. Opt. Soc. Am.*, 41(7):468–472, Jul 1951.

[2] M. Golay. Complementary series. *IRE Transactions on Information Theory*, 7(2):82–87, 1961.

[3] P. Spasojevic and C.N. Georghiades. Complementary sequences for ISI channel estimation. *IEEE Trans. Inf. Theory*, 47(3):1145–1152, 2001.

[4] H.M. Wang, X.Q. Gao, B. Jiang, X.H. You, and W. Hong. Efficient MIMO channel estimation using complementary sequences. *IET Communications*, 1:962–969(7), October 2007.

[5] Alphan Şahin and Rui Yang. An uplink control channel design with complementary sequences for unlicensed bands. *IEEE Trans. Wireless Commun.*, 19(10):6858–6870, 2020.

[6] Nam Yul Yu. Binary Golay spreading sequences and Reed-Muller codes for uplink grant-free NOMA. *IEEE Trans. Commun.*, 69(1):276–290, 2021.

[7] Ali Pezeshki, A. Robert Calderbank, William Moran, and Stephen D. Howard. Doppler resilient Golay complementary waveforms. *IEEE Trans. Inf. Theory*, 54(9):4254–4266, 2008.

[8] J.A. Davis and J. Jedwab. Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes. *IEEE Trans. Inf. Theory*, 45(7):2397–2417, 1999.

[9] Chin-Chong Tseng and C. Liu. Complementary sets of sequences. *IEEE Trans. Inf. Theory*, 18(5):644–652, 1972.

[10] H. D. Nguyêñ and G. E. Coxson. Doppler tolerance, complementary code sets, and generalised thue–morse sequences. *IET Radar, Sonar & Amp; Navigation*, 10:1603–1610, 2016.

[11] JoaquíN Aparicio and Takuya Shimura. Asynchronous detection and identification of multiple users by multi-carrier modulated complementary set of sequences. *IEEE Access*, 6:22054–22069, 2018.

[12] K.G. Paterson. Generalized Reed-Muller codes and power control in OFDM modulation. *IEEE Trans. Inf. Theory*, 46(1):104–120, 2000.

[13] Kai-Uwe Schmidt. Complementary sets, generalized Reed–Muller codes, and power control for OFDM. *IEEE Trans. Inf. Theory*, 53(2):808–814, 2007.

[14] Palash Sarkar, Sudhan Majhi, and Zilong Liu. A direct and generalized construction of polyphase complementary sets with low PMEPR and high code-rate for OFDM system. *IEEE Trans. Commun.*, 68(10):6245–6262, 2020.

[15] N. Suehiro and M. Hatori. N-shift cross-orthogonal sequences. *IEEE Trans. Inf. Theory*, 34(1):143–146, 1988.

[16] Xiqing Liu, Yvonne Huang, Chih-Yu Chang, and Hsiao-Hwa Chen. Generalized complementary coded scrambling multiple access for MIMO communications. *IEEE Trans. Veh. Technol.*, 70(12):13047–13061, 2021.

[17] Si-Yue Sun, Hsiao-Hwa Chen, and Wei-Xiao Meng. A survey on complementary-coded MIMO CDMA wireless communications. *IEEE Communications Surveys & Tutorials*, 17(1):52–69, 2015.

[18] Jun Tang, Ning Zhang, Zhikun Ma, and Bo Tang. Construction of doppler resilient complete complementary code in MIMO radar. *IEEE Trans. Signal Process.*, 62(18):4704–4712, 2014.

[19] Si-Yue Sun, Hsiao-Hwa Chen, and Wei-Xiao Meng. A framework to construct three-dimensional complementary codes for multiuser MIMO systems. *IEEE Trans. Veh. Technol.*, 64(7):2861–2874, 2015.

[20] Xinyu Men and Yubo Li. New construction of multiple complete complementary codes with inter-set zero cross-correlation zone. *IEEE Signal Process. Lett.*, 29:1958–1962, 2022.

[21] Liying Tian, Yubo Li, and Chengqian Xu. Multiple complete complementary codes with inter-set zero cross-correlation zone. *IEEE Trans. Commun.*, 68(3):1925–1936, 2020.

[22] IEEE standard for wireless lan medium access control (MAC) and physical layer (PHY) specifications. *IEEE Std 802.11-1997*, pages 1–445, 1997.

[23] Yajing Zhou, Yang Yang, Zhengchun Zhou, Kushal Anand, Su Hu, and Yong Liang Guan. New complementary sets with low PAPR property under spectral null constraints. *IEEE Trans. Inf. Theory*, 66(11):7022–7032, 2020.

[24] Benjamin R. Hamilton, Xiaoli Ma, John E. Kleider, and Robert J. Baxley. OFDM pilot design for channel estimation with null edge subcarriers. *IEEE Trans. Wireless Commun.*, 10(10):3145–3150, 2011.

[25] A. Gavish and A. Lempel. On ternary complementary sequences. *IEEE Trans. Inf. Theory*, 40(2):522–526, 1994.

[26] Alphan Şahin and Rui Yang. A generic complementary sequence construction and associated encoder/decoder design. *IEEE Trans. Commun.*, 69(11):7691–7705, 2021.

[27] Roman N. Ipanov, Alexandr I. Baskakov, Nikolay Olyunin, and Min-Ho Ka. Radar signals with ZACZ based on pairs of D-code sequences and their compression algorithm. *IEEE Signal Process. Lett.*, 25(10):1560–1564, 2018.

[28] Bingsheng Shen, Yang Yang, Zhengchun Zhou, and Sihem Mesnager. Constructions of spectrally null constrained complete complementary codes via the graph of extended boolean functions. *IEEE Trans. Inf. Theory*, 69(9):6028–6039, 2023.

[29] Nishant Kumar, Palash Sarkar, and Sudhan Majhi. Construction of spectrally-null-constrained zero-correlation zone sequences with flexible support. *Cryptography and Communications*, May 2024.

[30] Palash Sarkar, Chunlei Li, Sudhan Majhi, and Zilong Liu. New correlation bound and construction of Quasi-complementary sequence sets. *IEEE Trans. Inf. Theory*, 70(3):2201–2223, 2024.

[31] Rajen Kumar, Prashant Kumar Srivastava, and Sudhan Majhi. A direct construction of type-II Z complementary code set with arbitrarily large codes, 2023.

[32] Yu Tao, Adhikari Avik, Ranjan, Wang Yanyan, and Yang Yang. New class of optimal Z-complementary code sets. *IEEE Signal Process. Lett.*, pages 1–1, 2022.

[33] Bingsheng Shen, Yang Yang, Pingzhi Fan, and Zhengchun Zhou. Constructions of non-contiguous complementary sequence sets and their applications. *IEEE Trans. Wireless Commun.*, 21(7):4871–4882, 2022.

Construction of multiple quasi-complementary sequence sets with low inter-set cross-correlation

Yushu Tian Tao Liu Xiuping Peng Yubo Li

School of Information Science and Engineering
Hebei Key Laboratory of Information Transmission and Signal Processing
Yanshan University
Qinhuangdao, China

tianyushu@stumail.ysu.edu.cn {liutaotao,pengxp,liyubo6316}@ysu.edu.cn

Abstract

Recently, quasi-complementary sequence sets (QCSSs) have attracted interests for supporting large number of users in multi-carrier code-division multiple-access (MC-CDMA) systems. In applications, QCSSs that possess large set size and low correlation properties are desired. This work has two main contributions. Firstly, we present a method for generating multiple asymptotically optimal aperiodic low correlation complementary sequence sets (LC-CSSs) with low inter-set cross-correlation. Secondly, the combination of proposed LC-CSSs can result in a large-capacity aperiodic LC-CSS.

1 Introduction

Mutually orthogonal complementary sequence sets (MOCSSs) [1] have found extensive applications in communication systems owing to their ideal correlation properties, particularly in the design of radar system waveforms [2], channel estimation [3], etc. It is well known, the disadvantage of MOCSSs is that the set size cannot exceed the flock size (the number of constituent sequences) [4], which will limit the applications of complementary sets in multi-carrier code-division multiple-access (MC-CDMA) systems with large users to support.

To address this issue, the concept of quasi-complementary sequence set (QCSS), of which low correlation complementary sequence set (LC-CSS) is one subtype, was initially introduced by Liu *et al.* in [5]. One can extend communication capacity and reduce interference by utilizing QCSSs in communications [6]. Numerous studies have been carried

Corresponding author: Tao Liu.

This work was supported in part by the National Natural Science Foundation of China under Grant 62241110, in part by the Central government guides local science and technology development Foundation under Grant 236Z0403G.

out in order to design periodic and aperiodic QCSSs. In 2013, Liu *et al.* [5] proposed periodic QCSSs over the Singer difference set. Furthermore, Li *et al.* [7] constructed periodic QCSSs based on almost difference sets. In [8], Luo *et al.* constructed three classes of periodic small-alphabet sizes QCSSs. Aperiodic QCSSs have the same important applications in communication systems. Design of aperiodic QCSSs with various parameters is an interesting problem. Li *et al.* [9] proposed three classes of aperiodic LC-CSSs and one class of low correlation zone complementary sequence sets (LCZ-CSSs). Later, Zhou *et al.* [10] constructed QCSSs with new asymptotically optimal parameters. Authors in [11] constructed aperiodic QCSSs with larger set size from Florentine rectangles. In [12], aperiodic QCSSs of length $p_1^{m_1}p_2^{m_2}$ were constructed by using multivariate functions. Recently, the concept of QCSS was extended to two dimension (2-D) and the theoretical bounds of 2-D quasi-complementary array sets was presented in [13].

On the other hand, to reduce inter-cell interference in multi-cell scene, multiple sequence sets possessing favorable inter-set correlation properties are needed. Multiple optimal zero correlation zone (ZCZ) sequence sets with good cross-correlation between the different sets were introduced in [14]. Liu *et al.* [15] constructed aperiodic LC-CSSs combining several sets of complete complementary codes (CCCs) in 2019. Very recently, the authors in [16] have derived a new correlation lower bound for QCSSs composed of several CCCs, and they presented a construction of such QCSSs with flexible-alphabet sizes, which are convenient for practical applications.

As far as the authors are aware, the design of large-capacity LC-CSSs with multiple subsets has yet been introduced in other literature. This is the primary motivation of this paper. In this paper, we construct multiple aperiodic (p^2, p, p, p)-LC-CSSs, achieving the theoretical bound of LC-CSSs presented in [17]. Furthermore, we propose a large-capacity aperiodic $(p^2(p-1), p, p, 2p)$-LC-CSS by combining these LC-CSSs.

This paper is structured as follows for the remainder. Fundamental definitions are presented in Sect. 2. In Set. 3, we present the construction of multiple aperiodic LC-CSSs. Furthermore, a large-capacity aperiodic LC-CSS is generated through the combination of these LC-CSSs into a new set. Lastly, the paper is summarized in Sect. 4.

2 Preliminaries

Let $\mathbf{c} = (c_0, c_1, \cdots, c_{N-1})$ and $\mathbf{d} = (d_0, d_1, \cdots, d_{N-1})$ denote two length-N complex-valued sequences. The aperiodic correlation between $\mathbf{c}$ and $\mathbf{d}$ at time-shift τ is defined as

$$\widetilde{R}_{\mathbf{c},\mathbf{d}}(\tau) = \begin{cases} \sum_{t=0}^{N-1-\tau} c_t d_{t+\tau}^*, & 0 \le \tau \le N-1 \\ \sum_{t=0}^{N-1+\tau} c_{t-\tau} d_t^*, & 1-N \le \tau \le -1 \\ 0, & |\tau| \ge N, \end{cases} \tag{1}$$

where d_t^* denotes the complex conjugation of d_t.

Consider $\mathcal{S} = \{\mathbf{S}^0, \mathbf{S}^1, \cdots, \mathbf{S}^{K-1}\}$, having K sequence sets, each sequence set $\mathbf{S}^k$ comprises M length-N sequences, i.e., $\mathbf{S}^k = \{\mathbf{s}_0^k, \mathbf{s}_1^k, \cdots, \mathbf{s}_{M-1}^k\}$, $\mathbf{s}_m^k = \left(s_{m,0}^k, s_{m,1}^k, \cdots, s_{m,N-1}^k\right)$, $0 \le k \le K-1$, $0 \le m \le M-1$. The sequence set can be written in a matrix form with

size $M \times N$, i.e.,

$$\mathbf{S}^k = \begin{bmatrix} s^k_{0,0}, & s^k_{0,1}, & \cdots & s^k_{0,N-1} \\ s^k_{1,0}, & s^k_{1,1}, & \cdots & s^k_{1,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ s^k_{M-1,0}, & s^k_{M-1,1}, & \cdots & s^k_{M-1,N-1} \end{bmatrix}. \tag{2}$$

The set $\mathcal{S}$ is called a $(K, M, N, \delta_{\max})$-QCSS if for any $\mathbf{S}^{k_1}, \mathbf{S}^{k_2} \in \mathcal{S}$, where $0 \le k_1, k_2 \le K-1$, we have

$$\left|\widetilde{R}_{\mathbf{S}^{k_1},\mathbf{S}^{k_2}}(\tau)\right| = \left|\sum_{m=0}^{M-1} \widetilde{R}_{\mathbf{s}^{k_1}_m,\mathbf{s}^{k_2}_m}(\tau)\right| \le \delta_{\max}, \tag{3}$$

for $k_1 \ne k_2, 0 \le \tau \le N-1$ or $k_1 = k_2, 0 < \tau \le N-1$. Notably, K, M, N, and $\delta_{\max}$ represent the set size, the flock size, the length of each constituent sequence, and the maximum aperiodic correlation magnitude, respectively. QCSSs are divided into two types: LC-CSS and LCZ-CSS. An LCZ-CSS represents a set of two-dimensional matrices whose correlation magnitudes are non-zero but relatively low for the non-trivial time-shifts within a low correlation zone (LCZ). An LC-CSS is produced when the length of the LCZ is equivalent to the length of each constituent sequence. Specially, when $\delta_{\max} = 0$, the QCSS reduce to (K, M, N)-MOCSS. If $\delta_{\max} = 0$ and $K = M$, we denote $\mathcal{S}$ as (M, M, N)-CCC.

Lemma 1 ([17]). *For an aperiodic $(K, M, N, \delta_{\max})$-QCSS, when $K \ge 3M, M \ge 2$ and $N \ge 2$, the parameters meet the inequality,*

$$\delta_{\max} \ge \sqrt{MN\left(1 - 2\sqrt{\frac{M}{3K}}\right)}. \tag{4}$$

To analyze the performance, the optimality factor ρ of QCSS is given in the following definition.

$$\rho = \frac{\delta_{\max}}{\sqrt{MN\left(1 - 2\sqrt{\frac{M}{3K}}\right)}}. \tag{5}$$

If $\rho = 1$, the aperiodic QCSS is optimal. The aperiodic QCSS is near-optimal when $1 < \rho \le 2$.

3 Main Results

In this section, we first construct multiple asymptotically optimal aperiodic LC-CSSs with low inter-set cross-correlation property. By combining these LC-CSSs, a large-capacity aperiodic LC-CSS can be generated as a byproduct. Our proposed construction is then compared to the other construction method.

3.1 Multiple aperiodic LC-CSSs with low inter-set cross-correlation property

Prior to that, we introduce the subsequent Lemma. Note that the design of permutation $\pi_k^r(t)$ is inspired by [18].

Lemma 2. *$\pi_{k_1}^{r_1}(t) = r_1t^2 + t + k_1$, $\pi_{k_2}^{r_2}(t) = r_2t^2 + t + k_2$, where $1 \le r_1, r_2 \le p-1$, $0 \le k_1, k_2 \le p-1$. $\pi_{k_1}^{r_1}(t)$ and $\pi_{k_2}^{r_2}(t)$ are permutations of $\mathbb{Z}_p$ with following properties:*

1. *When $r_1 = r_2$ and $k_1 \neq k_2$, we have $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t) \neq 0 \pmod p$, where $0 \le t \le p-1$;*
2. *When $r_1 \neq r_2$ and $k_1 = k_2$, there is only one solution t_1 with $t_1 = 0$ satisfying $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t) = 0 \pmod p$, where $0 \le t \le p-1$;*
3. *When $r_1 = r_2$ and $\tau \neq 0$, there is at most one solution t_1 with $0 \le t_1 \le p-1$ satisfying $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t+\tau) = 0 \pmod p$;*
4. *When $r_1 \neq r_2$, $k_1 = k_2$, $\tau \neq 0$ or $r_1 \neq r_2$, $k_1 \neq k_2$, there are at most two solutions t_1, t_2 with $0 \le t_1, t_2 \le p-1$ satisfying $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t+\tau) = 0 \pmod p$.*

Proof.

Case 1. When $1 \le r_1 = r_2 \le p-1$ and $0 \le k_1 \neq k_2 \le p-1$, $\pi_{k_1}^{r_1}(t)$ and $\pi_{k_2}^{r_2}(t)$ are both based on mapping from $\mathbb{Z}_p$ to $\mathbb{Z}_p$, thus $\pi_{k_1}^{r_1}(t) \neq \pi_{k_2}^{r_2}(t) \pmod p$. Therefore, the first property holds.

Case 2. When $1 \le r_1 \neq r_2 \le p-1$ and $0 \le k_1 = k_2 \le p-1$, suppose that $\pi_{k_1}^{r_1}(t) = \pi_{k_2}^{r_2}(t)$, then we have $r_1t^2 + t + k_1 = r_2t^2 + t + k_2$, calculate that $t_1 = 0 \pmod p$, it indicates that there is only one solution t_1 satisfying $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t) = 0 \pmod p$, where $0 \le t \le p-1$. Therefore, the second property holds.

Case 3. When $1 \le r_1 = r_2 \le p-1$, $0 \le k_1, k_2 \le p-1$ and $\tau \neq 0$, suppose that $\pi_{k_1}^{r_1}(t) = \pi_{k_2}^{r_2}(t+\tau)$, then we have $r_1t^2 + t + k_1 = r_2(t+\tau)^2 + (t+\tau) + k_2$, calculate that $t = \frac{k_1-k_2}{2r_2\tau} - \frac{r_2\tau+1}{2r_2} \pmod p$, it indicates that there is at most one solution t_1 satisfying $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t+\tau) = 0$, where $0 \le t_1 \le p-1$. Hence, the third property holds.

Case 4. When $1 \le r_1 \neq r_2 \le p-1$, $0 \le k_1 = k_2 \le p-1$, $\tau \neq 0$, or $1 \le r_1 \neq r_2 \le p-1$, suppose that $\pi_{k_1}^{r_1}(t) = \pi_{k_2}^{r_2}(t+\tau)$, we have $r_1t^2 + t + k_1 = r_2(t+\tau)^2 + (t+\tau) + k_2$, then we have $(r_1 - r_2)t^2 - (2r_2\tau)t - (k_2 - k_1 + r_2\tau^2 + \tau) = 0$, it indicates that there are at most two solutions t_1, t_2 satisfying $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t) = 0 \pmod p$, where $0 \le t_1, t_2 \le p-1$. Hence the forth property holds.

This completes the proof of Lemma 2.

□

The main construction is given as follows.

Construction 1. *Let $p \ge 3$ be a prime, $\mathbb{Z}_p$ denote the ring of integers modulo p, and $\omega_p = e^{2\pi\sqrt{-1}/p}$ be a primitive p-th root of unity. Let*

$$\pi_k^r(t) = rt^2 + t + k \pmod p. \tag{6}$$

Define a function $f_n^{(r,k,m)} : \mathbb{Z}_p \to \mathbb{Z}_p$ *as follows.*

$$f_n^{(r,k,m)}(t) = n \cdot \pi_k^r(t) + mt \pmod p, \tag{7}$$

where $1 \le r \le p-1$, $0 \le k, m, n, t \le p-1$. *Define* $p-1$ *sequence sets* $\mathcal{S}^r = \left\{\mathbf{S}^{(r,k,m)} : 0 \le k, m \le p-1\right\}$, *where*

$$\mathbf{S}^{(r,k,m)} = \begin{bmatrix} s_{0,0}^{(r,k,m)}, & s_{0,1}^{(r,k,m)}, & \cdots & s_{0,p-1}^{(r,k,m)} \\ s_{1,0}^{(r,k,m)}, & s_{1,1}^{(r,k,m)}, & \cdots & s_{1,p-1}^{(r,k,m)} \\ \vdots & \vdots & \ddots & \vdots \\ s_{p-1,0}^{(r,k,m)}, & s_{p-1,1}^{(r,k,m)}, & \cdots & s_{p-1,p-1}^{(r,k,m)} \end{bmatrix}, \tag{8}$$

and

$$s_{n,t}^{(r,k,m)} = \omega_p^{f_n^{(r,k,m)}(t)}. \tag{9}$$

Theorem 1. *Sequence sets* $\mathcal{S}^r$ *for* $1 \le r \le p-1$ *obtained from Construction 1 have following properties,*

1. *Each sequence set* $\mathcal{S}^r$ *is an aperiodic* (p^2, p, p, p)*-LC-CSS.*
2. *The inter-set cross-correlation between any two different LC-CSSs* $\mathcal{S}^{r_1}$ *and* $\mathcal{S}^{r_2}$ *is upper bounded by* $2p$, *i.e.,*

$$\left| \sum_{n=0}^{p-1} \widetilde{R}_{\mathbf{s}_n^{(r_1,k_1,m_1)}, \mathbf{s}_n^{(r_2,k_2,m_2)}}(\tau) \right| \le 2p, \tag{10}$$

for all $1 \le r_1 \ne r_2 \le p-1$, $0 \le \tau \le p-1$ *and* $0 \le k_1, k_2, m_1, m_2 \le p-1$.

Proof. First, let us prove Part 1.

Let $\mathbf{S}^{(r,k_1,m_1)}, \mathbf{S}^{(r,k_2,m_2)} \in \mathcal{S}^r$, where $1 \le r \le p-1$ and $0 \le k_1, k_2, m_1, m_2 \le p-1$. Then calculate the aperiodic correlation of $\mathbf{S}^{(r,k_1,m_1)}$ and $\mathbf{S}^{(r,k_2,m_2)}$ as following:

$$\begin{aligned} &\widetilde{R}_{\mathbf{S}^{(r,k_1,m_1)}, \mathbf{S}^{(r,k_2,m_2)}}(\tau) \\ &= \sum_{n=0}^{p-1} \widetilde{R}_{\mathbf{s}_n^{(r,k_1,m_1)}, \mathbf{s}_n^{(r,k_2,m_2)}}(\tau) \\ &= \sum_{n=0}^{p-1} \sum_{t=0}^{p-1-\tau} s_{n,t}^{(r,k_1,m_1)} \cdot \left(s_{n,t+\tau}^{(r,k_2,m_2)}\right)^* \\ &= \omega_p^{-m_2\tau} \cdot \sum_{n=0}^{p-1} \sum_{t=0}^{p-1-\tau} \omega_p^{t(m_1-m_2)+n\left(\pi_{k_1}^r(t)-\pi_{k_2}^r(t+\tau)\right)}. \end{aligned} \tag{11}$$

Consider the following four cases.

Case 1. When $k_1 = k_2$, $m_1 = m_2$ and $\tau = 0$, it is evident that $\widetilde{R}_{\mathbf{S}^{(r,k_1,m_1)}, \mathbf{S}^{(r,k_2,m_2)}}(0) = p^2$.

Case 2. When $k_1 = k_2$, $m_1 \neq m_2$ and $\tau = 0$, then we have $\widetilde{R}_{\mathbf{S}^{(r,k_1,m_1)},\mathbf{S}^{(r,k_2,m_2)}}(\tau) = p \cdot \sum_{t=0}^{p-1} \omega_p^{t(m_1-m_2)} = 0$.

Case 3. When $k_1 \neq k_2$ and $\tau = 0$, from the property 1 in Lemma 2, there is no solution t' for $\pi_{k_1}^r(t') - \pi_{k_2}^r(t') = 0 \pmod p$, thus $\sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^r(t) - \pi_{k_2}^r(t+\tau)\right)} = 0$. Therefore, $\widetilde{R}_{\mathbf{S}^{(r,k_1,m_1)},\mathbf{S}^{(r,k_2,m_2)}}(\tau) = 0$ holds.

Case 4. When $\tau \neq 0$, according to the property 3 in Lemma 2, there is at most one solution t' satisfying $\pi_{k_1}^r(t') - \pi_{k_2}^r(t'+\tau) = 0 \pmod p$.

If $t' \in [0, p-1-\tau]$, we have

$$\begin{aligned}
&\widetilde{R}_{\mathbf{S}^{(r,k_1,m_1)},\mathbf{S}^{(r,k_2,m_2)}}(\tau) \\
&\quad = \omega_p^{-m_2\tau} \cdot \left[\omega_p^{t'(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^r(t') - \pi_{k_2}^r(t'+\tau)\right)} \right. \\
&\qquad \left. + \sum_{t=0, t\neq t'}^{p-1-\tau} \omega_p^{t(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^r(t) - \pi_{k_2}^r(t+\tau)\right)} \right] \\
&\quad = p \cdot \omega_p^{t'(m_1-m_2)-m_2\tau}.
\end{aligned} \tag{12}$$

If $t' \in (p-1-\tau, p-1]$, then $\sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^r(t) - \pi_{k_2}^r(t+\tau)\right)} = 0$, thus $\widetilde{R}_{\mathbf{S}^{(r,k_1,m_1)},\mathbf{S}^{(r,k_2,m_2)}}(\tau) = 0$. Otherwise, we have no solution t' satisfying $(\pi_{k_1}^r(t) - \pi_{k_2}^r(t+\tau) = 0 \pmod p)$, then $\widetilde{R}_{\mathbf{S}^{(r,k_1,m_1)},\mathbf{S}^{(r,k_2,m_2)}}(\tau) = 0$.

From the results of above four cases, we conclude that the maximum aperiodic correlation sidelobe amplitude value of $\mathcal{S}^r$ is $\delta_{\max} = p$.

Now we prove the Part 2.

Let $\mathbf{S}^{(r_1,k_1,m_1)} \in \mathcal{S}^{r_1}, \mathbf{S}^{(r_2,k_2,m_2)} \in \mathcal{S}^{r_2}$, where $1 \leq r_1 \neq r_2 \leq p-1$ and $0 \leq k_1, k_2, m_1, m_2 \leq p-1$. Similarly,

$$\begin{aligned}
&\widetilde{R}_{\mathbf{S}^{(r_1,k_1,m_1)},\mathbf{S}^{(r_2,k_2,m_2)}}(\tau) \\
&\quad = \omega_p^{-m_2\tau} \cdot \sum_{n=0}^{p-1} \sum_{t=0}^{p-1-\tau} \omega_p^{t(m_1-m_2)+n\left(\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t+\tau)\right)}.
\end{aligned} \tag{13}$$

Consider the following two cases.

Case 1. When $r_1 \neq r_2, k_1 = k_2$ and $\tau = 0$, based on the property 2 in Lemma 2, there is only one solution t' with $t' = 0$ such that $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t) = 0 \pmod p$, then it holds

$$\begin{aligned}
&\widetilde{R}_{\mathbf{S}^{(r_1,k_1,m_1)},\mathbf{S}^{(r_2,k_2,m_2)}}(\tau) \\
&\quad = \sum_{n=0}^{p-1} \sum_{t=0}^{p-1-\tau} \omega_p^{t(m_1-m_2)+n\left(\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t)\right)} \\
&\quad = \omega_p^{t'(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t') - \pi_{k_2}^{r_2}(t')\right)} + \sum_{t=0, t\neq t'}^{p-1-\tau} \omega_p^{t(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t)\right)} \\
&\quad = p \cdot \omega_p^{t'(m_1-m_2)}.
\end{aligned} \tag{14}$$

Case 2. When $r_1 \neq r_2, k_1 = k_2, \tau \neq 0$, or $r_1 \neq r_2, k_1 \neq k_2$, according to the property 4 in Lemma 2, there are at most two solutions t' and t'' meeting $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t+\tau) = 0 \pmod p$.

Suppose that $t', t'' \in [0, p-1-\tau]$, we have

$$\begin{aligned}
&\widetilde{R}_{\mathbf{S}^{(r_1,k_1,m_1)},\mathbf{S}^{(r_2,k_2,m_2)}}(\tau) \\
&= \omega_p^{-m_2\tau} \cdot \left[\omega_p^{t'(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t') - \pi_{k_2}^{r_2}(t'+\tau)\right)} \right. \\
&\quad + \omega_p^{t''(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t'') - \pi_{k_2}^{r_2}(t''+\tau)\right)} \\
&\quad \left. + \sum_{t=0, t\neq t', t''}^{p-1-\tau} \omega_p^{t(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t+\tau)\right)} \right] \\
&= p \cdot \omega_p^{-m_2\tau} \cdot \left(\omega_p^{t'(m_1-m_2)} + \omega_p^{t''(m_1-m_2)} \right). \qquad (15)
\end{aligned}$$

Suppose that $t' \in [0, p-1-\tau]$, $t'' \in (p-1-\tau, p-1]$ or $t' \in [0, p-1-\tau]$, t'' unsolved, we have

$$\begin{aligned}
&\widetilde{R}_{\mathbf{S}^{(r_1,k_1,m_1)},\mathbf{S}^{(r_2,k_2,m_2)}}(\tau) \\
&= \omega_p^{-m_2\tau} \cdot \left[\omega_p^{t'(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t') - \pi_{k_2}^{r_2}(t'+\tau)\right)} \right. \\
&\quad \left. + \sum_{t=0, t\neq t'}^{p-1-\tau} \omega_p^{t(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t+\tau)\right)} \right] \\
&= p \cdot \omega_p^{-m_2\tau + t'(m_1-m_2)}. \qquad (16)
\end{aligned}$$

Suppose that $t', t'' \in (p-1-\tau, p-1]$, or $t' \in (p-1-\tau, p-1]$, t'' unsolved, then $\sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}('+\tau)\right)} = 0$, thus $\widetilde{R}_{\mathbf{S}^{(r_1,k_1,m_1)},\mathbf{S}^{(r_2,k_2,m_2)}}(\tau) = 0$. Otherwise, we have no solution t' or t'' satisfying $\left(\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}('+\tau)\right) = 0 \pmod p$, hence $\widetilde{R}_{\mathbf{S}^{(r_1,k_1,m_1)},\mathbf{S}^{(r_2,k_2,m_2)}}(\tau) = 0$.

By summarizing the above discussion, we conclude that $\left| \sum_{n=0}^{p-1} \widetilde{R}_{\mathbf{S}^{(r_1,k_1,m_1)},\mathbf{S}^{(r_2,k_2,m_2)}}(\tau) \right| \leq 2p$ for $1 \leq r_1 \neq r_2 \leq p-1$, $0 \leq \tau \leq p-1$ and $0 \leq k_1, k_2, m_1, m_2 \leq p-1$.

Consequently, the proof of Theorem 1 is completed.

□

Remark 1. According to Lemma 1, we get the limit of the optimality factor of $\mathcal{S}^r$ is

$$\lim_{p\to+\infty} \rho = \lim_{p\to+\infty} \frac{p}{\sqrt{p^2\left(1 - 2\sqrt{\frac{p}{3p^2}}\right)}} = 1. \qquad (17)$$

It implies that the aperiodic LC-CSS $\mathcal{S}^r$ generated from Construction 1 is asymptotically optimal.

3.2 Large-capacity aperiodic LC-CSS

We can use $p-1$ LC-CSSs with low inter-set aperiodic cross-correlation amplitude to generate a large-capacity aperiodic LC-CSS, as illustrated in the following.

Corollary 1. *Let $\mathcal{S} = \mathcal{S}^1 \cup \mathcal{S}^2 \cup \cdots \cup \mathcal{S}^{p-1}$, obtained $\mathcal{S}$ is a large-capacity aperiodic $(p^2(p-1), p, p, 2p)$-LC-CSS.*

Proof. Each sequence set $\mathcal{S}^r$ in Theorem 1 is a (p^2, p, p, p)-LC-CSS, where $1 \le r \le p-1$, and the intra-set maximum aperiodic cross-correlation amplitudes are p. According to Theorem 1, the inter-set aperiodic cross-correlation amplitudes are $2p$. Consequently, the set $\mathcal{S}$ is a large-capacity aperiodic $(p^2(p-1), p, p, 2p)$-LC-CSS. □

Now calculate the optimality factor of $\mathcal{S}$. $\lim_{p\to+\infty} \rho = 2$. It indicates that aperiodic cross-correlation amplitudes of $\mathcal{S}$ asymptotically reaches twice concerning the correlation bound in Lemma 1.

In the following, we give an example to increase the readability of the construction in this paper.

Example 1. Let $p = 5$, we can generate four $(25, 5, 5, 5)$-LC-CSSs, $\mathcal{S}^1, \mathcal{S}^2, \mathcal{S}^3, \mathcal{S}^4$ from Theorem 1. The two LC-CSSs $\mathcal{S}^1$ and $\mathcal{S}^2$ are presented in Table 1, where each element denotes a power of ω_5. The optimality factor of $\mathcal{S}^r (1 \le r \le 4)$ is $\rho = 1.4380$, which means that $\mathcal{S}^r$ is near-optimal. Moreover, we can combine these four LC-CSSs to obtain a large-capacity aperiodic $(100, 5, 5, 10)$-LC-CSS $\mathcal{S} = \mathcal{S}^1 \cup \mathcal{S}^2 \cup \mathcal{S}^3 \cup \mathcal{S}^4$ by Corollary 1. A brief overview of the correlation among the LC-CSSs is provided in Figure 1.

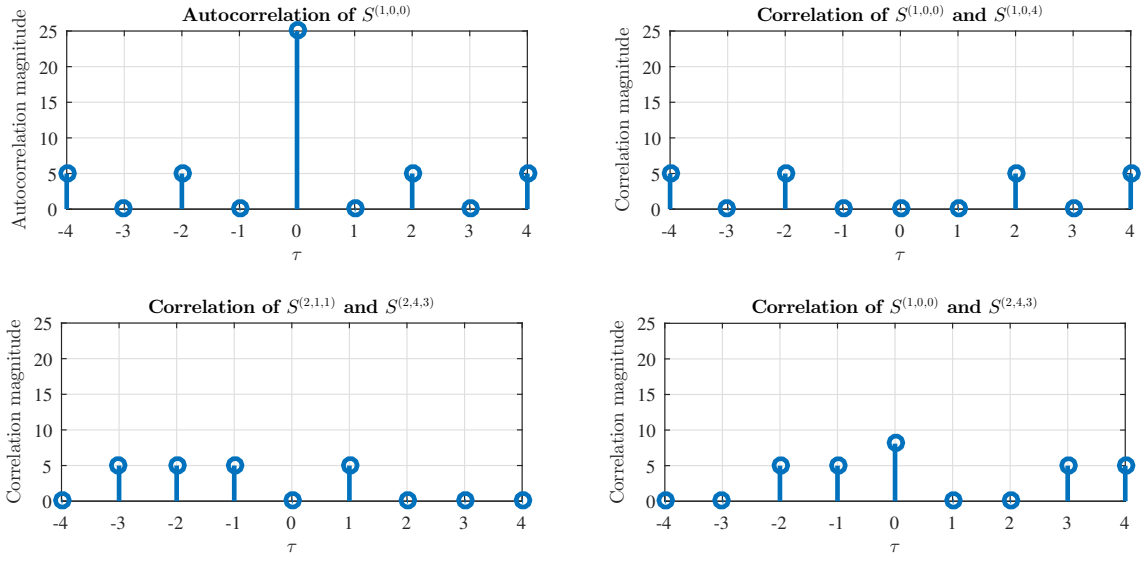


Figure 1: The correlation magnitudes of the LC-CSSs are illustrated in Example 1

Table 1: The two (25,5,5,5)-LC-CSSs $\mathcal{S}^1$ and $\mathcal{S}^2$ of Example 1

	$S^{(1,0,0)}$	$S^{(1,0,1)}$	$S^{(1,0,2)}$	$S^{(1,0,3)}$	$S^{(1,0,4)}$	$S^{(1,1,0)}$	$S^{(1,1,1)}$	$S^{(1,1,2)}$	$S^{(1,1,3)}$	$S^{(1,1,4)}$	$S^{(1,2,0)}$	$S^{(1,2,1)}$
	00000	01234	02413	03142	04321	00000	01234	02413	03142	04321	00000	01234
	02120	03304	04033	00212	01441	13231	14410	10144	11323	12002	24342	20021
$\mathcal{S}^1$	04240	00424	01103	02332	03011	21412	22141	23320	24004	20233	43134	44313
	01310	02044	03223	04402	00131	34143	30322	31001	32230	33414	12421	13100
	03430	04114	00343	01022	02201	42324	43003	44232	40411	41140	31213	32442
$S^{(1,2,2)}$	$S^{(1,2,3)}$	$S^{(1,2,4)}$	$S^{(1,3,0)}$	$S^{(1,3,1)}$	$S^{(1,3,2)}$	$S^{(1,3,3)}$	$S^{(1,3,4)}$	$S^{(1,4,0)}$	$S^{(1,4,1)}$	$S^{(1,4,2)}$	$S^{(1,4,3)}$	$S^{(1,4,4)}$
02413	03142	04321	00000	01234	02413	03142	04321	00000	01234	02413	03142	04321
21200	22434	23113	30403	31132	32311	33040	34224	41014	42243	43422	44101	40330
40042	41221	42400	10301	11030	12214	13443	14122	32023	33202	34431	30110	31344
14334	10013	11242	40204	41433	42112	43341	44020	23032	24211	20440	21124	22303
33121	34300	30034	20102	21331	22010	23244	24423	14041	10220	11404	12133	13312
	$S^{(2,0,0)}$	$S^{(2,0,1)}$	$S^{(2,0,2)}$	$S^{(2,0,3)}$	$S^{(2,0,4)}$	$S^{(2,1,0)}$	$S^{(2,1,1)}$	$S^{(2,1,2)}$	$S^{(2,1,3)}$	$S^{(2,1,4)}$	$S^{(2,2,0)}$	$S^{(2,2,1)}$
	00000	01234	02413	03142	04321	00000	01234	02413	03142	04321	00000	01234
	03011	04240	00424	01103	02332	14122	10301	11030	12214	13443	20233	21412
$\mathcal{S}^2$	01022	02201	03430	04114	00343	23244	24423	20102	21331	22010	40411	41140
	04033	00212	01441	02120	03304	32311	33040	34224	30403	31132	10144	11323
	02044	03223	04402	00131	01310	41433	42112	43341	44020	40204	30322	31001
$S^{(2,2,2)}$	$S^{(2,2,3)}$	$S^{(2,2,4)}$	$S^{(2,3,0)}$	$S^{(2,3,1)}$	$S^{(2,3,2)}$	$S^{(2,3,3)}$	$S^{(2,3,4)}$	$S^{(2,4,0)}$	$S^{(2,4,1)}$	$S^{(2,4,2)}$	$S^{(2,4,3)}$	$S^{(2,4,4)}$
02413	03142	04321	00000	01234	02413	03142	04321	00000	01234	02413	03142	04321
22141	23320	24004	31344	32023	33202	34431	30110	42400	43134	44313	40042	41221
42324	43003	44232	12133	13312	14041	10220	11404	34300	30034	31213	32442	33121
12002	13231	14410	43422	44101	40330	41014	42243	21200	22434	23113	24342	20021
32230	33414	34143	24211	20440	21124	22303	23032	13100	14334	10013	11242	12421

3.3 Comparison with previous works

The most of existing parameters of aperiodic QCCSs are listed in Table 2. The QCSSs reported in [15, 10, 11] are constructed by combining multiple sets of CCCs, whereas our construction is based on combining multiple sets of LC-CSSs. When M and N is prime, this paper can obtain multiple subsets LC-CSSs and form a large set LC-CSS, which results in a larger set size than the literature [15, 9, 10, 11]. For example, when $M = N = 5$, one $(20, 5, 5, 5)$-LC-CSS can be provided from [15, 10, 11], one $(30, 5, 5, 5)$-LC-CSS can be generated from [9], four $(25, 5, 5, 5)$-LC-CSSs and one $(100, 5, 5, 10)$-LC-CSS can be obtained in this paper from Th.1 and Co.1.

Table 2: The parameters of aperiodic QCSSs

Ref.	Set size	Flock size	Sequence length	$\delta_{\max}$	Parameter condition(s)
Th.2 [15]	$p(p-1)$	p	p	p	$p \geq 3$ is a prime.
Th.1 [9]	$q(q+1)$	q	q	q	q is the power of a prime.
Th.3 [9]	q^2	q	$q-1$	q	$q \geq 5$ is the power of a prime.
Th.2 [10]	$N(p_0-1)$	N	N	N	$N \geq 5$ is an odd, and the minimum prime factor of N is p_0.
Th.4 [11]	$N \times F(N)$	N	N	N	$N \geq 2$ is an integer, $F(N)$ represents the largest number of rows that a Florentine rectangle of size $F(N) \times N$ can have.
Th.1 Proposed	p^2	p	p	p	$p \geq 3$ is a prime.
Co.1 Proposed	$p^2(p-1)$	p	p	$2p$	$p \geq 3$ is a prime.

4 Conclusion

This paper presents a method to construct multiple aperiodic LC-CSSs with low inter-set cross-correlation properties. Each aperiodic quasi-complementary sequence set is (p^2, p, p, p)-LC-CSS, and the parameters are asymptotically optimal. Moreover, a large-capacity aperiodic $(p^2(p-1), p, p, 2p)$-LC-CSS can be obtained by combining $p-1$ sequence sets. As communication technology improves, it is promising for researchers to create more various quasi-complementary sequences to meet communication system needs.

References

[1] A. Rathinakumar, A. K. Chaturvedi. Complete mutually orthogonal Golay complementary sets from Reed–Muller codes. *IEEE Trans. Inf. Theory*, 54(3):1339–1346, 2008.

[2] J. Tang, N. Zhang, Z. Ma, B. Tang. Construction of Doppler resilient complete complementary code in MIMO radar. *IEEE Trans. Signal Process.*, 62(18):4704–4712, 2014.

[3] S. Wang, A. Abdi. MIMO ISI channel estimation using uncorrelated Golay complementary sets of polyphase sequences. *IEEE Trans. Veh. Technol.*, 56(5):3024–3039, 2007.

[4] H. H. Chen, S. W. Chu, M. Guizani. On next generation CDMA technologies: The REAL approach for perfect orthogonal code generation. *IEEE Trans. Veh. Technol.*, 57(5):2822–2833, 2008.

[5] Z. Liu, U. Parampalli, Y. L. Guan, S. Boztas. Constructions of optimal and near-optimal quasi-complementary sequence sets from singer difference sets. *IEEE Wireless Commun. Lett.*, 2(5):487–490, 2013.

[6] A. Samad, S. Majhi. A near-optimal and low-complex joint multiuser detection for QCSS-MC-CDMA system. *IEEE Syst.*, 15(2):1594–1603, 2021.

[7] Y. Li, L. Tian, T. Liu, C. Xu. Constructions of quasi-complementary sequence sets associated with characters. *IEEE Trans. Inf. Theory*, 65(7):4597–4608, 2019.

[8] G. Luo, X. Cao, M. Shi, T. Helleseth. Three new constructions of asymptotically optimal periodic quasi-complementary sequence sets with small alphabet sizes. *IEEE Trans. Inf. Theory*, 67(8):5168–5177, 2021.

[9] Y. Li, L. Tian, C. Xu. Constructions of asymptotically optimal aperiodic quasi-complementary sequence sets. *IEEE Trans. Commun.*, 67(11):7499–7511, 2019.

[10] Z. Zhou, F. Liu, A. R. Adhikary, P. Fan. A generalized construction of multiple complete complementary codes and asymptotically optimal aperiodic quasi-complementary sequence sets. *IEEE Trans. Commun.*, 68(6):3564–3571, 2020.

[11] A. R. Adhikary, Y. Feng, Z. Zhou, P. Fan. Asymptotically optimal and near-optimal aperiodic quasi-complementary sequence sets based on Florentine rectangles. *IEEE Trans. Commun.*, 70(3):1475–1485, 2022.

[12] D. Li, C. Li, P. Sarkar. Asymptotically optimal quasi-complementary code sets of length $p_1^{m_1}p_2^{m_2}$. *Proc. 10th IEEE Int. Workshop Signal Des. Appl. Commun.*, 1–5, Colchester, United Kingdom, 2022.

[13] A. Roy, S. Majhi. Lower bounds on the maximum cross-correlations of 2-D quasi-complementary array sets. *Cryptogr. Commun.*, 1–19, 2023.

[14] Z. Zhou, D. Zhang, T. Helleseth, J. Wen. A construction of multiple optimal ZCZ sequence sets with good cross correlation. *IEEE Trans. Inf. Theory*, 64(2):1340–1346, 2018.

[15] T. Liu, C. Xu, Y. Li. Multiple complementary sequence sets with low inter-set cross-correlation property. *IEEE Signal Process. Lett.*, 26(6):913–917, 2019.

[16] P. Sarkar, C. Li, S. Majhi, Z. Liu. New correlation bound and construction of quasi-complementary sequence sets. *IEEE Trans. Inf. Theory*, 2024.

[17] Z. Liu, Y. L. Guan, W. H. Mow. A tighter correlation lower bound for quasi-complementary sequence sets. *IEEE Trans. Inf. Theory*, 60(1):388–396, 2014.

[18] P. Fan, M. H. Lee, D. Peng. New family of hopping sequences for time/frequency-hopping CDMA systems. *IEEE Wireless Commun. Lett.*, 4(6):2836–2842, 2005.

Hierarchical Frequency Hopping Technique for Heterogeneous Multi-Tier Networks

Qi Zeng*
School of Electrical Engineering
Sichuan University
Chengdu, China
qzeng1@hotmail.com

Peiyi Zhao
Sichuan University -Pittsburgh Institute
Sichuan University
Chengdu, China
1434162157pennyz@gmail.com

Xing Liu
School of Electrical Engineering
Sichuan University
Chengdu, China
liuxing4@126.com

Changyuan Wang
Faculty of Artificial Intelligence and Big Data
Yibin University
Sichuan, China
184780948@qq.com

Abstract

Future wireless communication networks are characterized by the heterogeneous multi-tier infrastructure, which require the various levels of quality-of-services (QoSs) for different tiers. In this paper, we propose a novel type of frequency hopping (FH) with hierarchical level of Hamming correlations values (i.e., hierarchical FH for short). A construction algorithm of hierarchical FH sequence set (FHS) is proposed and its hierarchical Hamming property is demonstrated by an example. As a study case, the developed FHS set is imposed in asynchronous and heterogeneous multi-tier uplinks networks. The simulated results reveal that the proposed hierarchical FHS can provide multi-level bit-error-rate (BER) for various tiers networks; meanwhile, guarantee the superior transmission quality by significantly suppressing the inter- and intra- tier interferences.

1 Introduction

In the fifth cellular network and beyond (5G/B5G), a heterogeneous multi-tier architecture which consists of macro-cells (MC) and small cells (SC, including micro-cells, pico-cells

*Qi Zeng is supported by Sichuan Science and Technology Program under Grant 2023NSFSC0480 and in part by Open Fund for Key Laboratory of Internet of Things Standards and Applications in Ministry of Industry and Information Technology under Grant 202303.

and femto-cells) is the fundamental network infrastructure [1]. In the multi-tier networks, hierarchical quality-of-services (QoSs) which refer to the error-rate, spectral efficiency, latency and so forth, are required for various tiers, as illustrated in Fig. 1. For example, the network tier serving for the connected autonomous vehicles should require much higher QoS than the network tier serving for the wireless personal applications of pedestrians. Actually, in the PHY the multi-QoSs always refers to multi-level BERs. Besides, due to the natures of heterogeneous architecture, multi-tier interferences including the inter-tier and intra-tier interferences, are the critical challenges that degrade the performance.

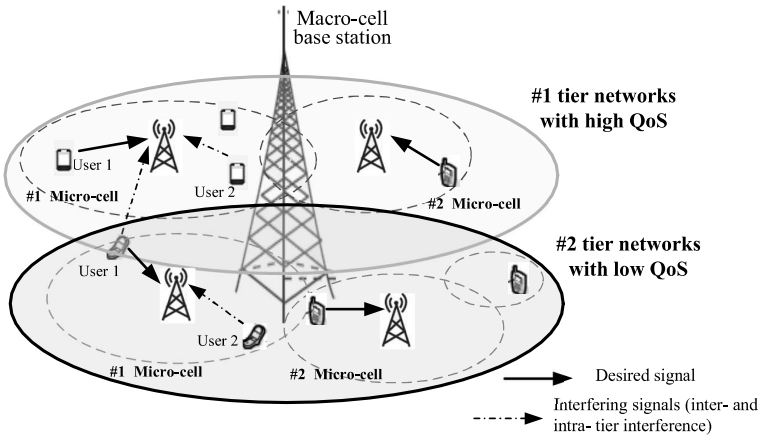


Figure 1: The infrastructure of heterogeneous multi-tier networks with hierarchical QoSs requirements. The desired signal may be impaired by the inter- and intra- tiers interferences.

The traditional pseudo-random FH technique and its FH sequence set (FHS) [2, 3, 4, 5, 6, 7] can efficiently combat various interference, channel fading and jamming attacks; however, it is unable to provide hierarchical QoSs, due to the fact that each available frequency-slot in these pseudo-random FHS sets just follows a near unform-distribution. The uniform-distribution property determines that FHS has only single-level values of Hamming cross-/auto-correlations (i.e., frequency-hits). Thus the traditional FH is not suitable to the heterogeneous multi-tier networks. It is well known that the BER performance of FH multi-access (FHMA) system is closely related to the Hamming cross-correlation value. By our previous study [8], the multi-QoSs goal for heterogeneous multi-tier can be achieved by delicately controlling the values of Hamming cross-correlations (e.g., frequency-hit rate). Taking the case of two-level hierarchical FHS set as the instance, the tier with high-QoS FHS (i.e., HQoS-FHS or HQoS-tier) should have the lower value of Hamming correlation, while the tier with low-QoS FHS (i.e., LQoS-FHS or LQoS-tier) is opposite. In addition, both high-QoS and low-QoS tiers should efficiently reduce the inter- and intra- tier interferences.

The prototype of two-level hierarchical FHS is firstly developed for smart grid communication networks[8]. The smart grid communications require the various QoSs of the data transmission for diversified power services. Based on this inspiration, recently a

new FH technique with two-level hierarchy was proposed and adopted by users located in cell edge to attain the prioritized radio-access [9]. However, these hierarchical FHSs have the drawback: they may experience all frequency-hits in the entire FHS period at some large access delays (i.e., asynchronous access), thus leading to the worst error-rate. Since the heterogeneous multi-tier networks always follows the asynchronous access, the aforementioned FHSs are not suitable to the heterogeneous multi-tier scenarios.

In this paper, we will propose a *strong* two-level hierarchical FH technique, which can provide optimal two-level Hamming correlations in the asynchronous access, also offer the low intra- and inter- tier interferences to heterogeneous multi-tier networks. The construction algorithm of such a hierarchical FH pattern is proposed via the series of mathematical transformations based on a given optimal pseudo-random FHS set. As a study case, the developed FHS set is imposed into the FH-based OFDM in asynchronous heterogeneous multi-tier networks, and the multi-level BERs are investigated and verified by extensive simulations.

2 Requirement of Hierarchical FHS Set

First, we introduce the definition of Hamming correlation with regard to FHS set.

Definition 1. Let $\mathbb{S} = \{\mathbf{s}^{(k)} | k = 1, 2, \cdots, K\}$ denote an FHS set with K sequences over a given frequency set $\mathbb{F} = \{f_1, f_2, \cdots, f_q\}$ with size q, where $\mathbf{s}^{(k)} = \left(s_0^{(k)}, s_1^{(k)}, \cdots, s_{L-1}^{(k)}\right)$, is the k-th sequence with length L. The Hamming correlation function of $\mathbf{s}^{(u)}$ and $\mathbf{s}^{(v)}$ at the integer delay τ is defined as

$$H_{uv}(\tau|\mathbf{s}^{(u)}, \mathbf{s}^{(v)}) = \sum_{i=0}^{L-1} h\left[s_i^{(u)}, s_{i+\tau}^{(v)}\right], \mathbf{s}^{(u,v)} \in \mathbb{S} \tag{1}$$

where $h[x, y] = 1$ for $x = y$ denotes the frequency-slot x colliding with another one y, whilst $h[x, y] = 0$ for $x \neq y$ denotes hit-free. The subscript addition $(\cdot)_{i+\tau}$ is performed modulo L. Further, for $u = v$, $H_{uu}(\cdot)$ denotes Hamming auto-correlation, and $H_{uv}(\cdot)$ denotes Hamming cross-correlation for $u \neq v$.

From this definition, the Hamming correlation function denotes the total number of the frequency hits over a whole length of sequence L at the relative delay τ. The Hamming correlation function determines the capability of anti-interference, anti-jamming and so forth, which is the most critical properties for FH multi-access (FHMA) systems.

Next, we define the maximum Hamming (out-of-phase) auto-correlation and cross-correlation of $\mathbb{S}$ as follows, respectively.

$$\begin{aligned} H_a(\mathbb{S}) &= \max\left\{H_{uu}(\tau)|\mathbf{s}^{(u)} \in \mathbb{S}, 0 < |\tau| \leq L-1\right\}, \\ H_c(\mathbb{S}) &= \max\left\{H_{uv}(\tau)|\mathbf{s}^{(u)}, \mathbf{s}^{(v)} \in \mathbb{S}, u \neq v, |\tau| \leq L-1\right\}. \end{aligned} \tag{2}$$

For ease understanding, an two-level hierarchical FHS set $\mathbb{S}$ is briefly introduced in this section, which can be easily extend to the generalized case of multi-level case. According

to the various levels of Hamming correlation values, the FHS set $\mathbb{S}$ can be separated into two disjoint subsets

$$\mathbb{S} = \{\mathbb{S}_1; \mathbb{S}_2\}, \mathbb{S}_1 \cap \mathbb{S}_2 = \varnothing, \tag{3}$$

where $\mathbb{S}_1$ with low Hamming cross-correlation value applied to the high QoS (HQoS) tier and $\mathbb{S}_2$ with high Hamming cross-correlation value applied to the low QoS (LQoS) tier, that is, $H_c(\mathbb{S}_1) < H_c(\mathbb{S}_2)$.

To realize the optimal performance in FHMA systems, it is generally desired that $\mathbb{S}_1$ and $\mathbb{S}_2$ have the following requirements under the given number of frequency slot q.

- The size of single FHS set $\mathbb{S}_1$ (and $\mathbb{S}_2$) should be as large as possible.
- The length of sequence in $\mathbb{S}_1$ (and $\mathbb{S}_2$) should be as long as possible.
- The Hamming cross- and (out-of-phase) auto- correlation values within $\mathbb{S}_1$ (and $\mathbb{S}_2$) should be as small as possible.
- The Hamming cross-correlation value of $\mathbb{S}_1$ is lower than that of $\mathbb{S}_2$.
- The Hamming cross-correlation between $\mathbb{S}_1$ and $\mathbb{S}_2$ should be as small as possible.

The first three properties are the required ones for traditional pseudo-random FHS, while the remaining ones are the additional properties for the proposed FHS set. Based on the theory of the code design, meeting all above requirements will significantly increase the design difficulty.

3 Design and Analysis of Two-Level Hierarchy FH Pattern

In this section, we firstly propose a construction algorithm of FHS set with two-level hierarchy, i.e., $\mathbb{S} = \{\mathbb{S}_1; \mathbb{S}_2\}$, where $\mathbb{S}_1$ denotes the HQoS FHS set and $\mathbb{S}_2$ denotes the LQoS one. Then, an example is presented to verify its hierarchical Hamming correlation properties.

Before demonstrating the construction algorithm, we define the two-level hierarchical FHS sets $\mathbb{S}_1$ and $\mathbb{S}_2$ as follows respectively,

$$\mathbb{S}_1 = \left\{\mathbf{s}_1^{(k)} | k = 1, 2, \cdots, K_{S1}\right\}, \mathbb{S}_2 = \left\{\mathbf{s}_2^{(k)} | k = 1, 2, \cdots, K_{S2}\right\}, \tag{4}$$

where K_{S1} and K_{S2} denote the sizes of $\mathbb{S}_1$ and $\mathbb{S}_2$, respectively. The sequences in $\mathbb{S}_1$ and $\mathbb{S}_2$ are denoted as

$$\mathbf{s}_1^{(k)} = \left(u_0^{(k)}, u_1^{(k)}, \cdots, u_{L-1}^{(k)}\right), \quad \mathbf{s}_2^{(k)} = \left(w_0^{(k)}, w_1^{(k)}, \cdots, w_{L-1}^{(k)}\right), \tag{5}$$

where L is the length of these sequences.

Next, we define a cyclic v-digit(s) shift operation, where v is a non-negative integer. Given a row (or column) vector $\mathbf{g} = (g_0, g_1, \cdots, g_{L-1})$ with length L, the cyclic v-digit(s) shift operation on $\mathbf{g}$ is defined as

$$\mathbf{g}^{\langle v \rangle} := (g_v, g_{v+1}, \cdots, g_{L-1}, g_0, \cdots, g_{v-1}), \tag{6}$$

where the subscript addition $(\cdot)_{a+b}$ is performed modulo L.

3.1 Construction Algorithm

The two-level hierarchical FHS set $\mathbb{S} = \{\mathbb{S}_1; \mathbb{S}_2\}$ can be constructed via the following steps.
Step 1: Given a *prime FHS set* $\mathbb{C}$ with size K_c as following

$$\begin{aligned}\mathbb{C} &= \left\{\mathbf{c}^{(k)} | k = 1, 2, \cdots, K_c\right\}, \\ \mathbf{c}^{(k)} &= \left(c_0^{(k)}, c_1^{(k)}, \cdots, c_{L_c-1}^{(k)}\right), c_l^{(k)} \in \mathrm{GF}(p),\end{aligned} \tag{7}$$

where p is a prime and L_c is the length of prime FHS. Based on the properties of prime sequence, we have $L_c = p$ and $K_c = p - 1$.

In addition, we define a new subset $\overline{\mathbb{C}}$ which is obtained from $\mathbb{C}$ excluding $\mathbf{c}^{(k_1)}$, that is,

$$\overline{\mathbb{C}} = \mathbb{C} \backslash \mathbf{c}^{(k_1)}, \forall\ k_1 = 1, 2, \cdots, K_c, \tag{8}$$

where $\overline{\mathbb{C}}$ has length p and size $p - 2$. The sequence set $\overline{\mathbb{C}}$ will be utilized to construct the LQoS FHS set $\mathbb{S}_2$.
Step 2: Based on the selected sequence $\mathbf{c}^{(k_1)}$ from the *prime FHS set* $\mathbb{C}$, a new sequence set $\mathbb{G}$ is obtained as follows via performing the cyclic v-digit(s) shift operation on $\mathbf{c}^{(k_1)}$.

$$\mathbb{G} = \left\{ \left(\mathbf{c}^{(k_1)}\right)^{<v>} | v = 0, 1, 2, \cdots, p-1 \right\}. \tag{9}$$

The set $\mathbb{G}$ can be written as the matrix with the column-wise manner, that is,

$$\mathbb{G} = [\mathbf{g}_0, \mathbf{g}_1, \cdots, \mathbf{g}_{p-1}]_{p \times p}, \tag{10}$$

where the i-th column vector in $\mathbb{G}$ $\mathbf{g}_i = [g_0^{(i)}, g_1^{(i)}, g_2^{(i)}, \cdots, g_{p-1}^{(i)}]^{\mathrm{T}}, g_l^{(i)} \in GF(p)$.
Step 3: Given a small positive integer $Z, 0 < Z < p$, we define Z non-negative integers $\{a_1, a_2, \cdots, a_Z | a_i > 1\}$, where $a_i \neq a_j$ if $i \neq j$. In addition, we select Z column-vectors as follows.

$$\begin{aligned}\mathbf{u}_1 &= [p, p+1, \cdots, 2p-1]^{\mathrm{T}}, \\ \mathbf{u}_2 &= [2p, 2p+1, \cdots, 3p-1]^{\mathrm{T}}, \\ &\vdots \\ \mathbf{u}_Z &= [Zp, Zp+1, \cdots, (Z+1)p-1]^{\mathrm{T}}.\end{aligned} \tag{11}$$

Based on (10) and (11), multiple matrices can be obtained as follows.

$$\begin{aligned}\mathbf{G}_0 &= [\mathbf{g}_0, \mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_Z], \\ \mathbf{G}_1 &= [\mathbf{g}_1, \mathbf{u}_1^{\langle a_1 \rangle}, \mathbf{u}_2^{\langle a_2 \rangle}, \cdots, \mathbf{u}_Z^{\langle a_Z \rangle}], \\ &\vdots \\ \mathbf{G}_{p-1} &= \left[\mathbf{g}_{p-1}, \mathbf{u}_1^{\langle (p-1)a_1 \rangle}, \mathbf{u}_2^{\langle (p-1)a_2 \rangle}, \cdots, \mathbf{u}_Z^{\langle (p-1)a_Z \rangle}\right],\end{aligned} \tag{12}$$

where $\mathbf{u}_i^{\langle v\rangle}$ denotes the cyclic v-digit(s) shifting operator on the column vector $\mathbf{u}_i$. Then a new matrix $\mathbb{S}_1$ can be obtained as follows via the cascading all matrices shown in (12).

$$\mathbb{S}_1 = [\mathbf{G}_0, \mathbf{G}_1, \mathbf{G}_2, \cdots, \mathbf{G}_{p-1}]_{p\times p(Z+1)}\,. \tag{13}$$

The matrix $\mathbb{S}_1$ by reforming it as a row-wise manner is namely the HQoS FHS set. The k-th row vector in $\mathbb{S}_1$ is the k-th HQoS FHS $\mathbf{s}_1^{(k)} = \left(u_0^{(k)}, u_1^{(k)}, \cdots, u_{L-1}^{(k)}\right)$.

Step 4: We select the first row vector of $\mathbb{S}_1$ (i.e., $\mathbf{s}_1^{(1)}$) as the base FHS to further generate the LQoS FHS set[1]. Based on the construction steps shown in (12) and (13), $\mathbf{s}_1^{(1)}$ can be also denoted as

$$\mathbf{s}_1^{(1)} = \left(g_0^{(0)}, u_0^{(1:Z)},\ g_0^{(1)}, u_0^{\langle a(1:Z)\rangle}, \cdots, g_0^{(p-1)}, u_0^{\langle (p-1)a(1:Z)\rangle}\right) \tag{14}$$

where $u_0^{(1:Z)}$ and $u_0^{\langle ia(1:Z)\rangle}$ denote these Z elements which are the first elements of column vectors in $[\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_Z]$, and in $[\mathbf{u}_1^{\langle ia_1\rangle}, \mathbf{u}_2^{\langle ia_2\rangle}, \cdots, \mathbf{u}_Z^{\langle ia_Z\rangle}]$ as shown in (11), respectively.

Based on (14), we design a mapping operator $\mathcal{M}(g_0^{(i)})$ which maps the element $g_0^{(i)} \in GP(p)$ to a specific vector, that is,

$$\begin{aligned} \mathcal{M}(g_0^{(0)}):&\quad g_0^{(0)} \mapsto \left[g_0^{(0)}, u_0^{(1:Z)}\right], \\ \mathcal{M}(g_0^{(i)}):&\quad g_0^{(i)} \mapsto \left[g_0^{(i)}, u_0^{\langle ia(Z:1)\rangle}\right],\ i \neq 0, \end{aligned} \tag{15}$$

where the operator '$A \mapsto B$' denotes the entry A is replaced by B. $u^{\langle ia(Z:1)\rangle}$ denotes Z elements with the inverse order of $u_0^{\langle ia(1:Z)\rangle}$, that is, the first elements of column vectors in $[\mathbf{u}_Z^{\langle ia_Z\rangle}, \mathbf{u}_{Z-1}^{\langle ia_{Z-1}\rangle}, \cdots, \mathbf{u}_2^{\langle ia_2\rangle}, \mathbf{u}_1^{\langle ia_1\rangle}]$.

According to the above mapping operation, the element $c_i^{(k)}, k \neq k_1$ in the set $\overline{\mathbb{C}}$ as shown in (8) can be extended, that is, different values of $c_i^{(k)}$ are mapped to different sub-vectors as shown in (15). Then the LQoS FHS set $\mathbb{S}_2$ is obtained as following,

$$\begin{aligned} \mathbb{S}_2 =& \left\{ \left(w_0^{(k)}, w_1^{(k)}, \cdots, w_L^{(k)}\right) \right\} \\ :=& \left\{ \left(\mathcal{M}(c_0^{(k)}), \mathcal{M}(c_1^{(k)}), \cdots, \mathcal{M}(c_{p-1}^{(k)})\right) \right\}, k \neq k_1, \end{aligned} \tag{16}$$

where $\left(c_0^{(k)}, c_1^{(k)}, \cdots, c_{p-1}^{(k)}\right) \in \overline{\mathbb{C}}$. According to above construction, it is easy to obtain that the length of $\mathbb{S}_2$ is $L = p(Z+1)$ and the size of $\mathbb{S}_2$ is $K_{S2} = K_c - 2 = p - 2$.

3.2 An Example of Two-Level hierarchical FH Pattern

In this subsection, an example of two-level hierarchical FH pattern and its Hamming correlation properties are presented.

[1]Other row vector of $\mathbb{S}_1$ is applicable as well.

Table 1: The comparisons of Hamming correlations among the proposed FHS set and other FHS sets with Z=2.

	τ	**-7**	**-6**	**-5**	**-4**	**-3**	**-2**	**-1**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Proposed	$H_{uv}(\tau\|\mathbb{S}_1)$	0	**5**	0	0	**5**	0	0	0	0	0	**5**	0	0	**5**	0
FHS	$H_{uv}(\tau\|\mathbb{S}_2)$	0	3	0	0	3	0	0	3	0	0	3	0	0	3	0
	$H_{uv}(\tau\|\mathbb{S}_1,\mathbb{S}_2)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	$H_{uu}(\tau)$	0	0	0	0	0	0	0	15	0	0	0	0	0	0	0
Multi-QoS	$H_{uv}(\tau\|\mathbb{S}_1)$	0	**15**	0	0	**15**	0	0	0	0	0	**15**	0	0	**15**	0
FHS in [8]	$H_{uv}(\tau\|\mathbb{S}_2)$	0	3	0	0	3	0	0	3	0	0	3	0	0	3	0
	$H_{uv}(\tau\|\mathbb{S}_1,\mathbb{S}_2)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	$H_{uu}(\tau)$	0	0	0	0	0	0	0	15	0	0	0	0	0	0	0
Trad.	$H_{uv}(\tau)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
FHS in [5]	$H_{uu}(\tau)$	0	0	0	0	0	0	0	15	0	0	0	0	0	0	0

$\cdot\ u \neq v$.

Example 1: Let $Z = 2, p = 5$ and $[a_1, a_2] = [2, 3]$, the HQoS FHS set $\mathbb{S}_1$ and the LQoS FHS set $\mathbb{S}_2$ can be generated as shown below.

$$\mathbf{s}_1^{(1)} = \{0, 5, 10, 1, 7, 13, 2, 9, 11, 3, 6, 14, 4, 8, 12\};$$
$$\mathbf{s}_1^{(2)} = \{1, 6, 11, 2, 8, 14, 3, 5, 12, 4, 7, 10, 0, 9, 13\};$$
$$\mathbf{s}_1^{(3)} = \{2, 7, 12, 3, 9, 10, 4, 6, 13, 0, 8, 11, 1, 5, 14\};$$
$$\mathbf{s}_1^{(4)} = \{3, 8, 13, 4, 5, 11, 0, 7, 14, 1, 9, 12, 2, 6, 10\};$$
$$\mathbf{s}_1^{(5)} = \{4, 9, 14, 0, 6, 12, 1, 8, 10, 2, 5, 13, 3, 7, 11\}.$$

$$\mathbf{s}_2^{(1)} = \{0, 10, 5, 2, 11, 9, 4, 12, 8, 1, 13, 7, 3, 14, 6\};$$
$$\mathbf{s}_2^{(2)} = \{0, 10, 5, 3, 14, 6, 1, 13, 7, 4, 12, 8, 2, 11, 9\};$$
$$\mathbf{s}_2^{(3)} = \{0, 10, 5, 4, 12, 8, 3, 14, 6, 2, 11, 9, 1, 13, 7\}.$$

From the example, we obtain the following parameters: $K_{S1} = 5, K_{S2} = 3, L = 15$ and the size of available frequency-slots set $q = 15$. In addition, the obtained FHSs have a good randomness since frequency-slot elements ($q = 15$ frequency-slots) in each FHS evenly spread over the entire FHS set.

The typical Hamming correlations of the proposed $\{\mathbb{S}_1; \mathbb{S}_2\}$ and the comparisons among other FHS sets are shown in Table 1 in details. For fair comparisons, the FHS sets in Tab. 1 have the same parameters, i.e., q, and L. The construction algorithms of the previous two-level hierarchical FHS set and the traditional pseudo-random FHS set are referred to [8] and [5], respectively.

Observed from the Tab. 1, the Hamming correlation of $\mathbb{S}_1$ is equal to zero, and outperforms $\mathbb{S}_2$ for the time-shift $|\tau| \leq Z$ (i.e.,the quasi-synchronous multi-tier networks).For the asynchronous case ($Z < |\tau| < L$), the proposed FHS set gets the best performance due to lowest Hamming correlations. However, the previous two-level hierarchical FHS

set in [8] attains the whole hits (i.e., $H_{uv} = 15$) thus leading to the disastrous BER degradation, which is wholly unacceptable for the asynchronous two-tier networks. Besides, the Hamming cross-correlation of traditional pseudo-random FHS has the single value for any two FHSs (i.e., $H_{uv} \equiv 1$), which cannot provide various QoSs for two-tier networks.

Overall, via this example, the properties of the proposed FHS set meet the technique requirements of hierarchical FHS set mentioned in Section 2. The similar conclusions can be drawn for the general cases with other Zs, ps and $\{a_i\}_i$.

4 BERs of the proposed Hierarchical FHS set applied in heterogenous networks

4.1 Transceiver of hierarchical FH based OFDM System

In heterogeneous multi-tier networks, the FH based OFDM transmitter (i.e., FH/OFDM) with N_b branches is introduced, as shown in [10], except that the proposed hierarchical FHSs are integrated into OFDM sub-branches. In this transmitter, the entire bandwidth is evenly divided into N_b non-overlapped sub-bands $\{\mathbb{F}_l, l = 0, 1, \cdots, N_b - 1\}$, and each sub-band contains q frequency slots, i.e., $||\mathbb{F}_l|| = q$. The active sub-carriers of the l-th sub-branch are hopped within $\mathbb{F}_l$ according to the proposed hierarchical FHS set $\mathbb{S} = \{\mathbb{S}_1, \mathbb{S}_2\}$, which is as shown in Section 3. For simplicity, it is assumed that one OFDM symbol is transmitted during one hop interval T. Then, the transmitted signal of the k-th user during the n-th hopping interval can be written as

$$S^{(k)}(t) = \sum_{l=0}^{N_b-1} \sqrt{2P^{(k)}} d_l^{(k)}(n) \cos\left[j2\pi \left(f_l + \frac{s_n^{(k)}}{T} \right) t \right], \quad nT \le t < (n+1)T, \tag{17}$$

where $d_l^{(k)}(n)$ denotes the baseband symbol on the l-th branch. In the following analysis, the binary PSK (BPSK) mapping scheme is employed, thus $d_l^{(k)}(n)$ is randomly generated the symbol from the alphabet set $\{-1, 1\}$. f_l is the first frequency slot in the l-th branch, which can be set as ql/T guaranteeing that the N_b sub-bands are not overlapped. $s_n^{(k)}$ denotes the instantaneous hopped-frequency slot of the k-th user, where $\{s_n^{(k)} | n = 0, 1, 2, \cdots\} \subset \mathbb{S}_1$ is adapted by users in the HQoS tier, and $\{s_n^{(k)} | n = 0, 1, 2, \cdots\} \subset \mathbb{S}_2$ is utilized by users in the LQoS tier. $P^{(k)}$ denotes the transmitting power of the k-th user.

In this paper, we assume that the received envelop of signal in base-station (BS) $\Gamma^{(k)} = \sqrt{2P^{(k)}}$ follows an i.i.d. Rayleigh distribution. In addition, a practical case of heterogeneous multi-tier networks with arbitrary access delays (i.e., asynchronous access mechanism) is considered in this paper, then the received signal at the BS is shown as

$$r(t) = \sum_{k=1}^{K} S^{(k)}(t - \tau_k) + \eta(t), \tag{18}$$

where K denotes the number of users in the entire multi-tier networks, including the high-QoS users and the low-QoS users). τ_k is the arbitrary access delay of the k-th user, which

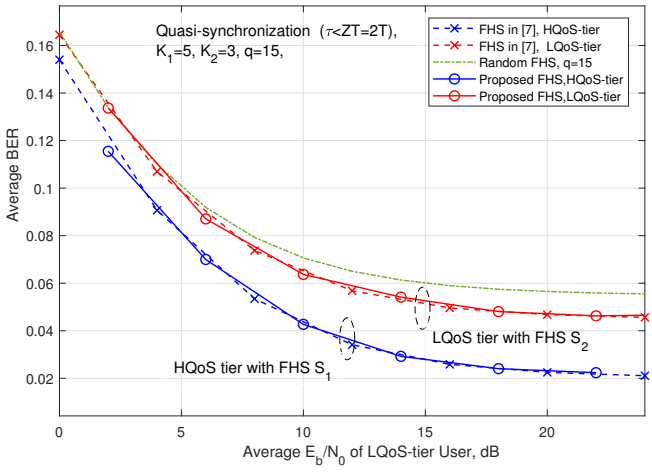


Figure 2: The BER comparisons between HQoS- and LQoS- tiers users in quasi-synchronous multi-tier networks by employing various FHSs.

uniformly distributed over duration of the entire sequence length. $\eta(t)$ represents the complex additional white Gaussian noise (AWGN) with two-sided power spectral density of $N_0/2$.

At the BS, the receiver structure of FH/OFDM system is shown in Fig. 2, which consists of N_b receiver branches. In each branch, the received signals $r(t)$ are first put into dehoppers, of which local frequencies are controlled by the given FHS. Then the low-pass-filter (LPF) with bandwith $2/T$ following the dehopper. Subsequently, the signal in each branch is processed by the correlator. The output of correlator is put into the demodulator.

4.2 BER analysis via simulations

In this section, the performance of the FH/OFDM system employing the developed hierarchical FHS set will be evaluated. To demonstrate the merits of our developed FHS set, the quasi-synchronous access mechanism (i.e., $D \leq ZT$) and the a-synchronous access mechanism (i.e., $D > ZT$) are adopted in multi-tier networks respectively in the following simulations. The employed two-level hierarchical FHS sets $\{\mathbb{S}_1; \mathbb{S}_2\}$ in the following simulations are as shown in *Example 1* in Section 3.2, where the parameters are $(q, K_1, K_2, L, Z) = (15, 5, 3, 15, 2)$.

The BER comparisons of the proposed FH/OFDM multi-tier networks employing the various FHS sets are plotted in Fig. 2 under quasi-synchronous mechanism and in Fig. 3 under asynchronous mechanism, respectively. For comparison, two types of classic FHS sets (i.e., the completely random FHS and the previous hierarchical FHS in [8]) are investigated as well under the same conditions, e.g., the number of frequency slots q, the length of FHS L. The system parameters are set as: $K_1 = 5, K_2 = 3$.

In Figs. 2-3, we find that our proposed hierarchical FHS and the previous FHS in [8] can attain two-level BERs for two-tiers networks but the random FHS set fails. In the

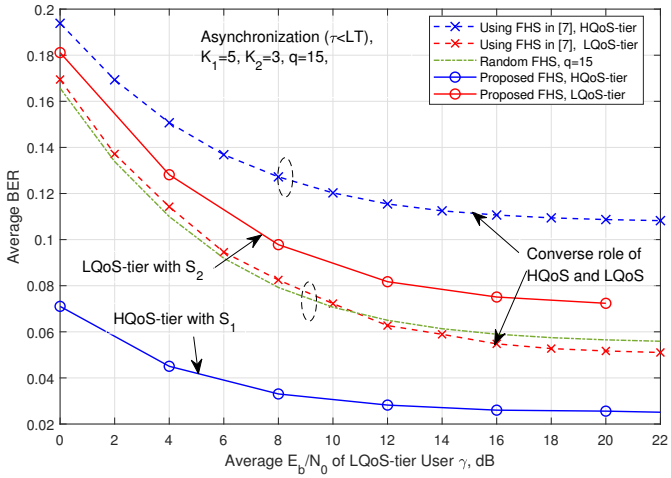


Figure 3: The BER comparisons between HQoS- and LQoS- tiers users in asynchronous multi-tier networks by employing various FHSs.

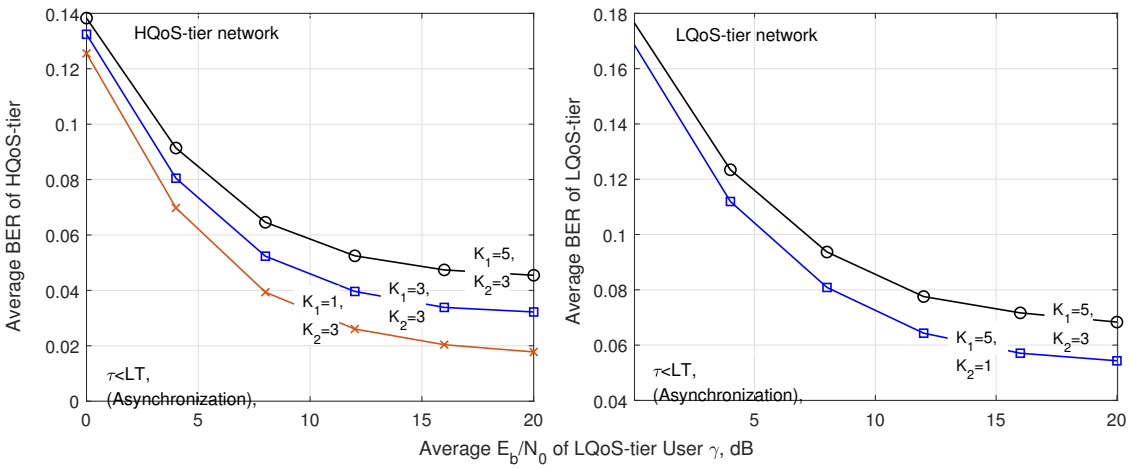


Figure 4: The average BERs of the proposed hierarchical FHSs with various number of users K_1 and K_2.

quasi-synchronization, the performance of our proposed FHS set coincides with that of FHS in [8], since these two types of FHS sets have the same Hamming correlation value when $D < 2T$ which is as shown in Tab. 1. However as for the a-synchronization scenario shown in Fig. 3, the previous FHS in [8] can not provide two-level QoSs, the FHS set $\mathbb{S}_1$ even is inferior to $\mathbb{S}_2$ due to the whole-hits occurrence of $\mathbb{S}_1$ at some large access delays, e.g., $H_{uv}(\mathbb{S}_1||\tau| = 3, 6) = L = 15$. By employing the FHS set proposed in this paper, the two-level QoSs target can readily restore, as illustrated in Fig. 3.

The average BERs of the HQoS- and LQoS- tiers with various number of users K_1 and K_2 are plotted in Fig. 4. The left sub-figure is for the HQoS-tier BERs, and the right one is for the LQoS-tier BERs. The results in these figure can also quantify the impacts

of intra- and inter- tiers interferences on the BERs of HQoS- and LQoS- tiers due to the frequency-hits of FHS set. Here, we will take the figure of HQoS-tier case as example to explain the BER behavior. Obtained from this sub-figure, the BER follows descent as the K_1 decreases due to the reductions of the multi-user interference contributed from intra-tier. The BER behavior of LQoS-tier follows the same trend as that of HQoS-tier, of which explanation is omitted due to the limited space.

5 Conclusions

This paper is dedicated to the design and analysis of a hierarchical FHS set and its application to heterogeneous multi-tier FH/OFDM networks. As an improvement of the traditional FHS set with single-level Hamming correlation, the hierarchical FHS set attains two-level Hamming correlations to match the two-level QoSs requirement. The newly developed FHS set $\mathbb{S} = \{\mathbb{S}_1; \mathbb{S}_2\}$ enjoys the following properties: the FHS subset $\mathbb{S}_1$ with lower frequency-hit rate is applicable to HQoS-tier networks, while the FHS set with higher frequency-hit rate $\mathbb{S}_2$ is applicable to LQoS-tier networks. The more attractive merits are that the FH subsets $\mathbb{S}_1$ and $\mathbb{S}_2$ possess the minimum Hamming correlation for the large access delay, which is very helpful to the asynchronous multi-tier networks.

To evaluate the enabling of two-level QoSs via the proposed FHS set, we investigated the FH/OFDM system employed with such an FHS set in multi-tier uplinks. The simulation results have shown that, in aid of the hierarchical FHS set, the FH/OFDM system conveniently implements the multi-level BERs target, meanwhile, eliminating the intra- and inter-tier interference efficiently. In our future work, some interesting topics following this paper will be studied, such as, the bounds on the Hammming correlation of the multi-level hierarchy FHS, the construction algorithm of generalized multi-level hierarchy FHS and so forth.

References

[1] E. Hossain, M. Rasti, H. Tabassum, and A. Abdelnasser, "Evolution toward 5G multi-tier cellular wireless networks: an interference management perspective," *IEEE Wireless Commun.*, vol. 21, no. 3, pp. 118-127, June 2014.

[2] C. Ding, R. Fuji-Hara, Y. Fujiwara and *et al.*, "Sets of frequency hopping sequences: bounds and optimal constructions," *IEEE Trans Inf. Theory*, vol. 55, no. 7, pp. 3297-3304, July 2019.

[3] Q. Zeng, Z. Z. Zhou, X. Liu, and Z. L. Liu, "Strong no-hit-zone sequences for improved quasi-orthogonal FHMA systems: sequence design and performance analysis," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5336-5345, Aug. 2019.

[4] S. Xu, J. Mi, "New Constructions for Near-Optimal Sets of Frequency-Hopping Sequences via the Gaussian Periods in Finite Fields," *IEEE Access*, vol. 10, pp. 18463 - 18469, Feb. 2022.

[5] X. Niu, C. Xing, Y. Liu, and L. Zhou, "A construction of optimal frequency hopping sequence set via combination of multiplicative and additive groups of finite fields," *IEEE Trans Inf. Theory*, vol. 66, no. 8, pp. 5310-5315, Aug. 2020.

[6] L. Zhou and X. Liu, "Families of optimal low-hit-zone frequency-hopping sequence sets under the periodic partial Hamming correlation properties," *IEEE Access*, vol. 8, pp. 14991-14998, Jan. 2020.

[7] Q. Zeng, Z. Liu and G. Gradoni, "Optimal quasi-orthogonal FH sequences with adaptive array receiver for massive connectivity in asynchronous multi-cluster networks," *IEEE Trans. Wireless Commun.*, vol.21, no. 8, pp. 5730-5743, Aug. 2022.

[8] Q. Zeng, H. Li, and D. Peng, "Frequency-hopping based communication network with multi-level QoS's in smart grid: code design and performance analysis," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1841-1852, Dec. 2012.

[9] Q. Zeng and Xing Liu, "Multi-priority based interference mitigation scheme for HetNets uplinks: a frequency hopping method," in Proc. IEEE ISNCC, Istanbul, Turkey, June. 23-25, 2019.

[10] M. Ebrahimi and M. Nasiri-Kenari, "Performance analysis of multicarrier frequency-hopping (MC-FH) code-division multiple-access systems: uncoded and coded schemes," *IEEE Trans. Veh. Technol.*, vol. 53, no. 4, pp. 968-981, Jul. 2004.

Circular quasi-Florentine rectangles and its application in designing optimal polyphase sequence sets

Avik Ranjan Adhikary
Department of Mathematics
Southwest Jiaotong University
Chengdu, China
avik.adhikary@ieee.org

Zhengchun Zhou
School of Information Science and Technology
Southwest Jiaotong University
Chengdu, China
zzc@swjtu.edu.cn

Yang Yang
Department of Mathematics
Southwest Jiaotong University
Chengdu, China
yang_data@swjtu.edu.cn

Abstract

In this paper, first we introduce the concept of circular quasi-Florentine rectangles and propose circular quasi-Florentine rectangles when N is of the form p^n, where p is any prime number. Next, we design polyphase sequence sets with new parameters using the proposed circular quasi-Florentine rectangles. The proposed polyphase sequence sets are optimal with respect to the Welch bound.

1 Introduction

Circular Florentine rectangles first appeared around mid 1980's in the remarkable works of T. Etzion, S. Golomb and H. Taylor [1, 2]. Circular Florentine rectangles are matrices of size $F_c(N) \times N$, where each of the N symbols $0,\ 1,\ 2, \cdots,\ N-1$ appears exactly once in each of the $F_c(N)$ rows. Additionally, for any two symbols a and b, and for each m from 1 to n, there is at most one row in which b is the m-th symbol to the right of a when the rows are considered to be circular. Several conjectures were proposed in [2] about the availability of circular Florentine rectangles for different values of N. Working towards this direction Song [3] constructed several circular Florentine rectangles through computer search. However, systematic construction of circular Florentine rectangle still remains open other than the cases when $N = p$ is a prime number [2].

Recently, circular Florentine rectangles emerge as an efficient combinatorial tool to design several sequence sets with various desired correlation properties. In two separate

works, based on circular Florentine rectangles, Zhang *et al.* [4] and Song *et al.* [5] proposed polyphase sequence sets, which are asymptotically optimal with respect to the Welch bound [6]. The set size of all these sequence sets highly depends on the number of rows $F_c(N)$ of the corresponding circular Florentine rectangle. Since 1991 till date, very few research work has been reported towards the construction of circular Florentine rectangles for various values of N. Moreover, almost all the existing works are computer search results.

Recent applications of circular Florentine rectangles in desiging sequences with desired correlation properties motivates us to design circular Florentine rectangles with large number of rows for a given N. In [2] it is proved that $F_c(N) = N - 1$, when N is prime, and provided a systematic construction. It is also conjectured in [2] that when N is not prime, $F_c(N)$ cannot achieve the value $N-1$. In his work in [3], Song compiled all possible values of $F_c(N)$, when N is odd. It is also proved in [3] that for even N, $F_c(N) = 1$. In view of these facts, it is a challenging task to construct circular Florentine rectangles with large number of rows, when N is not prime. Working towards this direction, we introduce a new concept of "circular quasi-Florentine rectangles". In circular quasi-Florentine rectangles we preserve all the properies of circular Florentine rectangles other than the fact that every row contains $N - 1$ elements instead of N elements. In other words, one of the element is missing in each of the rows. We also propose a construction of circular quasi-Florentine rectangle for the cases when $N = p^n$. We show that for these cases we can obtain a maximum of $F_c^Q(N) = p^n$ rows. Also, when N is even and is of the form p^n, then also we can achieve p^n number of rows, earlier which was only one.

Next, to demonstrate the applications of the proposed circular quasi-Florentine rectangles in designing sequence sets, we propose a class of periodic polyphase sequence sets using the proposed circular quasi-Florentine rectangles. Polyphase sequence sets achieving Welch bound [6] has a rich literature. Interested readers can go through [4,7] and the references therein. In summary, polyphase sequences which achieves the Welch bound, have important applications in communication systems [8]. Recent works of Zhang *et al.* [4], Song *et al.* [5] motivates us to check the applications of the proposed circular quasi-Florentine rectangles in designing polyphase sequence sets. Interestingly, the proposed polyphase sequence sets are asymptotically optimal with respect to the Welch bound. The parameters of the asymptotically optimal periodic polyphase sequence sets proposed till date are listed in Table 1.

The rest of the paper is organised as follows. In Section 2, we fix some notations and revisit some basic definitions and Welch bound. In Section 3, we introduce the concept of "circular quasi-Florentine rectangles" and propose a construction when N is of the form of p^n, where p is any prime number. In Section 4, we propose a construction of periodic polyphase sequence set using the circular quasi-Florentine rectangles and discussed its optimality with respect to the Welch bound. Finally, we conclude the paper in Section 5.

2 Preliminaries

Let us fix the following notations before we begin:

Table 1: Polyphase sequences asymptotically achieving the Welch bound.

References	Period	$\theta_{\max}$	θ_a	Family Size	Alphabet Size	Constraint(s)
Sidelnikov [9]	p^n-1	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	p^n	p	p is an odd prime
Welch and Scholtz [10, 11]	p	$2+\sqrt{p}$	3	$p-2$	$p-1$	p is an odd prime
Cubic family by Alltop [12]	p	$\sqrt{p}$	$\sqrt{p}$	p	p	$p \geq 5$ is prime
Frank-Zadoff-Heimiller [13]	p^2	p	0	$p-1$	p	p is an odd prime
Popovic [14]	N	$\sqrt{N}$	0	$\nu(N)^\dagger$	N	$N=sl^2$ is odd
Kasami [15]	p^n-1	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	p	$p=2$
Kumar and Moreno [16]	p^n-1	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	$p^{\frac{n}{2}}$	p	p is an odd prime
Liu and Komo [17]	p^n-1	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	$p^{\frac{n}{2}}$	p	p is an odd prime
Moriuchi and Imamura [18]	p^n-1	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	$p^{\frac{n}{2}}$	p	p is an odd prime
Jang *et al.* [19]	p^n-1	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	$p^{\frac{n}{2}}$	p	p is an odd prime
Family $\mathcal{A}$ [20, 22]	p^n-1	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	$1+p^n$	4	$p=2$
Family $\mathcal{U}$ [21, 22]	$p(p^n-1)$	$p+p^{\frac{n+1}{2}}$	$p+p^{\frac{n+1}{2}}$	p^n	4	$p=2$
Chung *et al.* [23]	p^2-p	p	p	p	p	p is an odd prime
Zhou *et al.* [7]	p^n-1	$p^{\frac{n}{2}}$	1	p^n-1	$p(p^n-1)$	p is any prime
Zhou *et al.* [7]	p^n-1	$p^{\frac{n}{2}}$	1	K	pK	p is any prime and $K \mid (p^n-1)$
Gu *et al.* [24]	p^m-1	$p^{k-1}p^{\frac{m}{2}}$	$p^{k-1}p^{\frac{m}{2}}$	$p^{km}-1$	$p^k(p^m-1)$	p is any prime, k is any integer
Zhang *et al.* [4]	N^2	N	0	$F_c(N)$	N	$F_c(N)$ is the number of rows of a circular Florentine rectangle
Proposed	$N(N-1)$	N	N	$F_c^Q(N)$	N	$F_c^Q(N)$ is the number of rows of a circular quasi-Florentine rectangle

- x^* denotes the conjugate of x.
- $\langle x \rangle_N$ denotes $x \pmod N$.

Let $\mathcal{C} = \{\mathbf{c}_i = \{c_{i,t}\}_{t=0}^{N-1} : 0 \leq i \leq M-1\}$ be a family of M unimodular polyphase sequences each of length N. The periodic correlation function between two sequences $\mathbf{c}_i$ and $\mathbf{c}_j$ in $\mathcal{C}$ is defined as follows:

$$\theta_{\mathbf{c}_i,\mathbf{c}_j}(\tau) = \sum_{t=0}^{N-1} c_{i,t} c^*_{j,\langle t+\tau \rangle_N}, \ 0 \leq \tau \leq N-1. \tag{1}$$

when $i=j$, it is called autocorrelation, otherwise it is cross-correlation. Let us define the maximum magnitudes of the autocorrelation and cross-correlation of the sequences in $\mathcal{C}$ as follows:

$$\begin{aligned} \theta_a(\mathcal{C}) &= \{\mid \theta_{\mathbf{c}_i}(\tau) \mid : 0 \leq i < M, 0 < \tau < N\}, \\ \theta_c(\mathcal{C}) &= \{\mid \theta_{\mathbf{c}_i,\mathbf{c}_j}(\tau) \mid : 0 \leq i \neq j < M, 0 \leq \tau < N\}. \end{aligned} \tag{2}$$

Let $\theta_{\max}(\mathcal{C}) = \max\{\theta_a(\mathcal{C}), \theta_c(\mathcal{C})\}$. Accordingly, a sequence set $\mathcal{C}$ is said to be an (M, N, θ_{max}) sequence set.

Lemma 1. *[6] Considering periodic correlation, for a sequence set $\mathcal{C}$ with M sequences, each of length N and periodic correlation tolerance $\theta_{\max}$, we have the Welch bound, as follows*

$$\theta_{\max} \geq N\sqrt{\frac{M-1}{NM-1}}. \tag{3}$$

An $(M, N, \theta_{\max})$- sequence set $\mathcal{C}$ is said to be optimal, if it satisfies the Welch bound, with equality. Therefore, we define the optimality factor ρ as follows:

$$\rho = \frac{\text{achieved } \theta_{max}}{\text{theoretical } \theta_{\max}}, \tag{4}$$

where "achieved $\theta_{\max}$" is the correlation bound achieved through the proposed constructions and "theoretical $\theta_{\max}$" is the Welch bound in Lemma 1. In general $\rho \geq 1$. When $\rho = 1$, we call the sequence set optimal.

3 Circular Quasi-Florentine Rectangles

In this section, first we propose the definition of circular quasi-Florentine rectangles, then we propose a construction of circular quasi-Florentine rectangles for the cases when N can be written in the form of p^n, where p is any prime number.

Definition 1. A matrix $\mathcal{A}$ over $\mathbb{Z}_N$ is said to be a circular quasi Florentine rectangle, if it satisfies the following two conditions:

C1: Each row contains $N-1$ symbols, where each symbol, except one, occours exactly once in each row.

C2: For any ordered pair (a, b) of two distinct symbols, and for any integer m from 1 to $N-2$, there is atmost one row in which b is m steps right of a, when steps are considered circularly.

Remark 1. The only difference of circular quasi Florentine rectangle from the circular Florentine rectangle is that, in circular Florentine rectangle, each row must contains all the elements of $\mathbb{Z}_N$, whereas in circular quasi Florentine rectangle, one element is missing in each of the rows. Please note that the missing element may be different for each of the rows.

3.1 Construction of circular quasi-Florentine rectangles

Construction 1. *Let p be prime and n be a positive integer. $\mathbb{F}_p$ denotes a finite field with p elements and $\mathbb{F}_q$ be the extension field of $\mathbb{F}_p$, where $q = p^n$. Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{F}_p$. Let α be a primitive element of $\mathbb{F}_q$. The non-zero elements of $\mathbb{F}_q$ can be written in the power of α as $\{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{q-2}\}$. Let us define a one-to-one mapping ψ from $\mathbb{F}_q$ to $\mathbb{Z}_q$ which takes the n-tuple to decimal version of the elements in $\mathbb{Z}_q$.*

Example 1. When $p = 3$, $n = 2$, and primitive polynomial $f(x) = \alpha^2 + 2\alpha + 2$, the elements of $\mathbb{F}_9$ are

$$S = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}. \tag{5}$$

Then,

$$\psi(S) = \{0, 1, 3, 4, 7, 2, 6, 8, 5\}. \tag{6}$$

Theorem 1. *Let $\mathcal{A}$ be a matrix of order $q \times (q-1)$, defined as follows:*

$$\mathcal{A} = \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,p^n-2} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,p^n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{p^n-1,0} & a_{p^n-1,1} & \cdots & a_{p^n-1,p^n-2} \end{bmatrix}_{q\times(q-1)} \tag{7}$$

where,

$$A_{i,j} = \begin{cases} \psi(\alpha^j) & \text{for } i = 0; \\ \psi(\alpha^j + \alpha^{i-1}) & \text{for } 0 < i \leq q-1, \end{cases} \tag{8}$$

and ψ is a one-to-one mapping as defined in Construction 1. Then, $\mathcal{A}$ is a quasi Florentine rectangle of size $q \times (q-1)$, with $F_c^Q(q) = q$.

Proof. To show that $\mathcal{A}$ is a circular quasi Florentine rectangle, we need to prove the two conditions given in Definition 1.

α^j and α^{i-1} are both elements of $\mathbb{F}_q$ for $0 \leq i \leq (q-1)$ and $0 \leq j \leq (q-2)$, therefore $(\alpha^j + \alpha^{i-1}) \in \mathbb{F}_q$. Since, ψ is a one-to-one mapping, and $0 \leq j \leq (q-2)$, each element of $\mathbb{Z}_q$ will appear only once, and it will miss one element. Hence condition C1 of Definition 1 is satisfied.

Next, we prove C2. Let us assume that there are two elements x and y, where y is m (> 0) steps right of x, circularly, in two rows of $\mathcal{A}$, say r_1 and r_2, . In r_1-th row, let the position of x be at the $c_x^{r_1}$-th column, and y be at the $c_y^{r_1}$-th column. Similarly, in r_2-th row, let the position of x be at the $c_x^{r_2}$-th column, and y be at the $c_y^{r_2}$-th column. Let us assume $0 < r_1, r_2 \leq q-1$. The calculation will be similar if one of them is zero. So, we have

$$a_{r_1,c_x^{r_1}} = x = a_{r_2,c_x^{r_2}}, \tag{9}$$

and

$$a_{r_1,c_y^{r_1}} = y = a_{r_2,c_y^{r_2}}. \tag{10}$$

From (9), we have

$$\psi(\alpha^{c_x^{r_1}} + \alpha^{r_1-1}) = \psi(\alpha^{c_x^{r_2}} + \alpha^{r_2-1}), \tag{11}$$

since ψ is a bijection, we have

$$\alpha^{c_x^{r_1}} + \alpha^{r_1-1} = \alpha^{c_x^{r_2}} + \alpha^{r_2-1}. \tag{12}$$

Similarly, from (10), we have

$$\alpha^{c_y^{r_1}} + \alpha^{r_1-1} = \alpha^{c_y^{r_2}} + \alpha^{r_2-1}. \tag{13}$$

Therefore, from (12) and (13), we have

$$\begin{aligned}\alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}} &= \alpha^{c_y^{r_1}} - \alpha^{c_y^{r_2}} \\ &= \alpha^{\langle c_x^{r_1}+m\rangle_{q-1}} - \alpha^{\langle c_x^{r_2}+m\rangle_{q-1}}.\end{aligned} \tag{14}$$

So, we have four cases:

Case 1: When $c_x^{r_1}+m < q-1$ and $c_x^{r_2}+m < q-1$. In this case, $\langle c_x^{r_1}+m\rangle_{q-1} = c_x^{r_1}+m$ and $\langle c_x^{r_2}+m\rangle_{q-1} = c_x^{r_2}+m$. Hence, from (14), we have

$$\begin{aligned}\alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}} &= \alpha^{c_x^{r_1}+m} - \alpha^{c_x^{r_2}+m} \\ &= \alpha^m(\alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}})\end{aligned} \tag{15}$$

Since $0 < r_1, r_2 \leq p^n - 1$ and $r_1 \neq r_2$, therefore, $\alpha^{r_1-1} \neq \alpha^{r_2-1}$. Note that $\alpha^{c_x^{r_1}} + \alpha^{r_1-1} = \alpha^{c_x^{r_2}} + \alpha^{r_2-1}$. Therefore, $\alpha^{c_x^{r_1}} \neq \alpha^{c_x^{r_2}}$. Hence, from (15), we have

$$\alpha^m = 1, \tag{16}$$

which implies $m = 0$ or $m = q-1$. If $m = 0$, then it is a contradiction, since we had assumed m is non-zero. If $m = q-1$, then $x = y$, which is also a contradiction, since $x \neq y$. Hence, C2 of Defintion 1 is satisfied.

Case 2: When $c_x^{r_1} + m > q-1$ and $c_x^{r_2} + m < q-1$. In this case $\langle c_x^{r_1} + m\rangle_{q-1} = [(c_x^{r_1} + m) - (q-1)]$ and $\langle c_x^{r_2} + m\rangle_{q-1} = c_x^{r_2} + m$. Hence, from (14), we have

$$\begin{aligned}\alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}} &= \alpha^{\left[(c_x^{r_1}+m)-(q-1)\right]} - \alpha^{c_x^{r_2}+m} \\ &= \alpha^m(\alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}}),\end{aligned} \tag{17}$$

since, $\alpha^{(q-1)} = 1$. Hence, similar to Case 1 above, we can show the contradiction.

Case 3: When $c_x^{r_1} + m < q-1$ and $c_x^{r_2} + m > q-1$. In this case, we have from (14),

$$\begin{aligned}\alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}} &= \alpha^{(c_x^{r_1}+m)} - \alpha^{\left[c_x^{r_2}+m-(q-1)\right]} \\ &= \alpha^m(\alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}}).\end{aligned} \tag{18}$$

Case 4: When $c_x^{r_1} + m > q-1$ and $c_x^{r_2} + m > q-1$. In this case, we have from (14),

$$\begin{aligned}\alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}} &= \alpha^{\left[(c_x^{r_1}+m)-(q-1)\right]} - \alpha^{\left[c_x^{r_2}+m-(q-1)\right]} \\ &= \alpha^m(\alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}}).\end{aligned} \tag{19}$$

For Case 3 and Case 4 the contradiction can be shown similar to Case 2.

This completes the proof. □

Example 2. When $p = 2$, $n = 3$, and primitive polynomial $f(x) = x^3 + x + 1$, using Theorem 1, we have

$$\mathcal{A} = \begin{bmatrix} 1 & 2 & 4 & 3 & 6 & 7 & 5 \\ 0 & 3 & 5 & 2 & 7 & 6 & 4 \\ 3 & 0 & 6 & 1 & 4 & 5 & 7 \\ 5 & 6 & 0 & 7 & 2 & 3 & 1 \\ 2 & 1 & 7 & 0 & 5 & 4 & 6 \\ 7 & 4 & 2 & 5 & 0 & 1 & 3 \\ 6 & 5 & 3 & 4 & 1 & 0 & 2 \\ 4 & 7 & 1 & 6 & 3 & 2 & 0 \end{bmatrix}_{8\times 7}, \tag{20}$$

which is a circular quasi-Florentine rectangle, with $F_c^Q(8) = 8$.

Property 1. *Let $N = p^n$, where p is prime and $n \geq 1$ is an integer. Let $\mathcal{A}$ be a circular quasi Florentine rectangle of size $F_c^Q(N) \times (N-1)$ over $\mathbb{Z}_N$, given as follows:*

$$\mathcal{A} = \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,N-2} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,N-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{F_c^Q(N)-1,0} & a_{F_c^Q(N)-1,1} & \cdots & a_{F_c^Q(N)-1,N-2} \end{bmatrix}_{F_c^Q(N)\times(N-1)} \tag{21}$$

where $a_{i,j}$ denotes the j-th element of the i-th row. According to Definition 1, each row of $\mathcal{A}$, i.e., $\mathbf{a}_i$ for $0 \leq i < F_c^Q(N)$, is a permutation on $\mathbb{Z}_N$, missing one element. For each $0 < m < N-1$, $(a_{i,\langle j\rangle_{(N-1)}}, a_{i,\langle j+m\rangle_{(N-1)}}) \neq (a_{p,\langle q\rangle_{(N-1)}}, a_{p,\langle q+m\rangle_{(N-1)}})$ unless $i = p$ and $j = q$, where $0 \leq i, p \leq F_c^Q(N) - 1$, $0 \leq j, q \leq N-2$, $0 < \langle j+m\rangle_{(N-1)} < N-1$ and $0 < \langle q+m\rangle_{(N-1)} < N-1$. In other words, if $\pi_i^{cQ} : \mathbb{Z}_N \to \mathbb{Z}_N$ be a permutation on $\mathbb{Z}_N$, i.e., if π_i^{cQ} denotes the i-th row of $\mathcal{A}$, then for each $0 < m < N-1$, $(\pi_i^{cQ}(j), \pi_i^{cQ}(\langle j+m\rangle_{(N-1)})) = (\pi_p^{cQ}(q), \pi_p^{cQ}(\langle q+m\rangle_{(N-1)}))$ if and only if $i = p$ and $j = q$, where $0 \leq j, q < N-1$.

Lemma 2. *Let $\mathcal{A}$ be a quasi-Florentine rectangle of size $F_c^Q(N)\times(N-1)$. Let π_i^{cQ} denotes the i-th row of a quasi Florentine rectangle $\mathcal{A}$. For $0 \leq i \neq j < F_c^Q(N)$, $\pi_i^{cQ}(\langle k\rangle_{(N-1)}) = \pi_j^{cQ}(\langle k+\tau\rangle_{(N-1)})$, has atmost one solution.*

Proof. Assume that for $0 \leq i \neq j < F_c^Q(N)$, $\pi_i^{cQ}(\langle k\rangle_{(N-1)}) = \pi_j^{cQ}(\langle k+\tau\rangle_{(N-1)})$, has more than one solution for $0 \leq \tau < N-1$. Let k_1 and k_2 be the two solutions. Then, we have $\pi_i^{cQ}(\langle k_1\rangle_{(N-1)}) = \pi_j^{cQ}(\langle k_1+\tau\rangle_{(N-1)})$ and $\pi_i^{cQ}(\langle k_2\rangle_{(N-1)}) = \pi_j^{cQ}(\langle k_2+\tau\rangle_{(N-1)})$. Therefore, we have $(\pi_i^{cQ}(\langle k_1\rangle_{(N-1)}), \pi_i^{cQ}(\langle k_2\rangle_{(N-1)})) = (\pi_j^{cQ}(\langle k_1+\tau\rangle_{(N-1)}), \pi_j^{cQ}(\langle k_2+\tau\rangle_{(N-1)}))$. This contradicts the definition of circular quasi Florentine rectangles. Hence, $\pi_i^{cQ}(\langle k\rangle_{(N-1)}) = \pi_j^{cQ}(\langle k+\tau\rangle_{(N-1)})$, has at most one solution for each $0 < \tau < N-1$ for $0 \leq i \neq j < F_c^Q(N)$. □

4 Construction of asymptotically optimal polyphase sequence sets from circular quasi-Florentine rectangles

Let $\mathcal{A}$ be a circular quasi-Florentine rectangle. Then each row of a $\mathcal{A}$ is a permutation over $\mathbb{Z}_N$, missing one element, according to C1 of Defintion 1. Let the i-th row of $\mathcal{A}$ be

denoted by π_i^{cQ}, then π_i^{cQ} is a permutation over $\mathbb{Z}_N$, which misses one element.

Construction 2. *Consider any positive integer $N \geq 2$, for which an $F_c^Q(N) \times (N-1)$ circular quasi-Florentine rectangle $\mathcal{A}$ exists over $\mathbb{Z}_N$. Also let π_i^{cQ} be the permutation over $\mathbb{Z}_N$ for $0 \leq i < F_c^Q(N)$, defined as above, which satisfies Lemma 2. Then for $0 \leq t < N(N-1)$, define $h_i(t)$ as follows:*

$$h_i(t) = t\pi_i^{cQ}(\langle t \rangle_{(N-1)}), \tag{22}$$

Construct a sequence set $\mathcal{C}$ of order $F_c^Q(N) \times N(N-1)$, as follows:

$$\mathcal{C} = \begin{bmatrix} \mathbf{c}_0 \\ \mathbf{c}_1 \\ \vdots \\ \mathbf{c}_{F_c^Q(N)-1} \end{bmatrix} = \begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,N(N-1)-1} \\ c_{1,0} & c_{1,1} & \cdots & c_{1,N(N-1)-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{F_c^Q(N)-1,0} & c_{F_c^Q(N)-1,1} & \cdots & c_{F_c^Q(N)-1,N(N-1)-1} \end{bmatrix}_{F_c^Q(N) \times N(N-1)}, \tag{23}$$

where

$$c_{i,j} = \omega_N^{h_i(j)}. \tag{24}$$

Theorem 2. *The sequence set $\mathcal{C}$, derived in Construction 2, is an $(F_c^Q(N), N(N-1), \theta_{\max})$ polyphase sequence set over $\mathbb{Z}_N$, with $\theta_{\max} = N$.*

Proof. The size of $\mathcal{C}$ is $F_c^Q(N) \times (N-1)$. For $0 \leq i, j < F_c^Q(N)$, and $0 \leq \tau < L$, where $L = N(N-1)$, we have

$$\begin{aligned} \theta_{\mathbf{c}_i,\mathbf{c}_j}(\tau) &= \sum_{k=0}^{L-1} c_{i,k} \left(c_{j,\langle k+\tau \rangle_L}\right)^* \\ &= \sum_{k=0}^{L-1} \omega_N^{h_i(k)} \left(\omega_N^{h_j(k+\tau)}\right)^* \\ &= \sum_{k=0}^{L-1} \omega_N^{k\pi_i^{cQ}(\langle k \rangle_{(N-1)}) - (k+\tau)\pi_j^{cQ}(\langle k+\tau \rangle_{(N-1)})} \\ &= \sum_{k_0=0}^{N-2} \omega_N^{-\tau_1 \pi_j^{cQ}(\langle k_0+\tau_0 \rangle_{(N-1)})} \cdot \sum_{k_1=0}^{N-1} \omega_N^{k_1(\pi_i^{cQ}(\langle k_0 \rangle_{(N-1)}) - \pi_j^{cQ}(\langle k_0+\tau_0 \rangle_{(N-1)}))} \end{aligned} \tag{25}$$

where $k_0 = \langle k \rangle_{N-1}$, $k_1 = \langle k \rangle_N$, $\tau_0 = \langle \tau \rangle_{N-1}$, and $\tau_1 = \langle \tau \rangle_N$. We have the following cases:

- Case I: when $i = j$, $\tau_0 = 0$ and $\tau_1 = 0$. In this case, from (25), we have

$$\theta_{\mathbf{c}_i}(0) = N(N-1). \tag{26}$$

- Case II: when $i = j$, $\tau_0 = 0$ and $\tau_1 \neq 0$, we have from (25)

$$\theta_{\mathbf{c}_i}(\tau) = N \sum_{k_0=0}^{N-2} \omega_N^{-\tau_1 \pi_i^{cQ}(\langle k_0 \rangle_{(N-1)})} \tag{27}$$

$\pi_i^{cQ}(k_0)$ is a permutation on $\mathbb{Z}_N$, missing one element, according to the construction. Let that missing element be t, then (27) becomes

$$\theta_{\mathbf{c}_i}(\tau) = N\omega_N^{-\tau_1 \cdot t}. \tag{28}$$

Therefore, in this case $\mid \theta_{\mathbf{c}_i}(\tau) \mid = N$.

- Case III: when $i = j$, $\tau_0 \neq 0$, we have from (25),

$$\theta_{\mathbf{c}_i}(\tau) = \sum_{k_0=0}^{N-2} \omega_N^{-\tau_1 \pi_i^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)})} \cdot \sum_{k_1=0}^{N-1} \omega_N^{k_1(\pi_i^{cQ}(\langle k_0\rangle_{(N-1)}) - \pi_i^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)}))}. \tag{29}$$

Since $\pi_i^{cQ}(k_0)$ is a permutation missing one element, so $\pi_i^{cQ}(\langle k_0\rangle_{(N-1)}) \neq \pi_i^{cQ}(\langle k_0 + \tau_0\rangle_{(N-1)}$. Hence,

$$\sum_{k_1=0}^{N-1} \omega_N^{k_1(\pi_i^{cQ}(\langle k_0\rangle_{(N-1)}) - \pi_i^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)}))} = 0. \tag{30}$$

Therefore, in this case $\mid \theta_{\mathbf{c}_i}(\tau) \mid = 0$.

- Case IV: when $i \neq j$, we have from (25),

$$\theta_{\mathbf{c}_i,\mathbf{c}_j}(\tau) = \sum_{k_0=0}^{N-2} \omega_N^{-\tau_1 \pi_j^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)})} \cdot \sum_{k_1=0}^{N-1} \omega_N^{k_1(\pi_i^{cQ}(\langle k_0\rangle_{(N-1)}) - \pi_j^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)}))} \tag{31}$$

Note that $\pi_i^{cQ}(\langle k_0\rangle_{(N-1)}) - \pi_j^{cQ}(\langle k_0 + \tau_0\rangle_{(N-1)}) = 0$ has atmost one solution as per Lemma 2. Therefore, if there is no solution then

$$\sum_{k_1=0}^{N-1} \omega_N^{k_1(\pi_i^{cQ}(\langle k_0\rangle_{(N-1)}) - \pi_j^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)}))} = 0, \tag{32}$$

hence, $\mid \theta_{\mathbf{c}_i,\mathbf{c}_j}(\tau) \mid = 0$. However, if there is a solution, let k_0' be the solution. Then we have from (31),

$$\begin{aligned}\theta_{\mathbf{c}_i,\mathbf{c}_j}(\tau) &= N \cdot \omega_N^{-\tau_1 \pi_j^{cQ}(\langle k_0'+\tau_0\rangle_{(N-1)})} \\ &\quad + \sum_{\substack{k_0=0 \\ k_0 \neq k_0'}}^{N-2} \omega_N^{-\tau_1 \pi_j^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)})} \cdot \sum_{k_1=0}^{N-1} \omega_N^{k_1(\pi_i^{cQ}(\langle k_0\rangle_{(N-1)}) - \pi_j^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)}))} \\ &= N \cdot \omega_N^{-\tau_1 \pi_j^{cQ}(\langle k_0'+\tau_0\rangle_{(N-1)})}.\end{aligned} \tag{33}$$

Hence, in this case $\mid \theta_{\mathbf{c}_i,\mathbf{c}_j}(\tau) \mid = N$.

Therefore, combining all the cases, we have $\theta_{\max}(\mathcal{C}) = N$. This proves the theorem.

□

4.1 Discussion on optimality

Theorem 3. *Let $\mathcal{C}$ be the sequence sets with parameters $(F_c^Q(N), N(N-1), N)$, as proposed in Theorem 2. Then $\mathcal{C}$ is an asymptotically optimal polyphase sequence set with respect to the Welch bound.*

Proof. From (4), we have

$$\rho = \frac{N}{N(N-1)\sqrt{\frac{F_c^Q(N)-1}{N(N-1)F_c^Q(N)-1}}}. \tag{34}$$

After some routine calculation we get

$$\rho = \frac{1}{\sqrt{1-\frac{1}{N}}} \frac{\sqrt{1-\frac{1}{F_c^Q(N)N(N-1)}}}{\sqrt{1-\frac{1}{F_c^Q(N)}}} \tag{35}$$

Hence, for the cases when $N \to \infty$, $F_c^Q(N) \to \infty$, we have $\lim_{N\to\infty} \rho = 1$.

Since in our case for $N = p^n$, $F_c^Q(N) = p^n$, we have $\lim_{N\to\infty} \rho = 1$. Hence, the proposed sequence sets are asymptotically optimal. □

Next we give an example of the proposed polyphase sequence sets.

Example 3. Let $p = 2$, $n = 3$, then $N = 2^3 = 8$. Using the circular quasi-Florentine rectangle constructed in *Example* 2, following **Construction** 2, we obtain asymptotically optimal polyphase sequence set $\mathcal{C}$ over $\mathbb{Z}_8$ with parameters $(8, 56, 8)$. A glimpse of the periodic autocorrelation and cross-correlation among the sequences are shown in Fig. 1.

5 Conclusion

In this paper, we have introduced a new concept of circular quasi-Florentine rectangle and proposed a construction of circular quasi-Florentine rectangle of size $F_c^Q(N) \times N$ when N is of the form p^n, where p is any prime number. We have also proposed a class of polyphase sequences using the circular quasi-Florentine rectangles which are asymptotically optimal with respect to the Welch bound.

References

[1] S. Golomb, and H. Taylor. Tuscan squares-a new family of combinatorial designs. *Ars Combinatoria* 20, 115–132, 1985.

[2] T. Etzion, S. Golomb, and H. Taylor. Tuscan-k squares. *Adv. Appl. Maths* 10(2), 164–174, 1989.

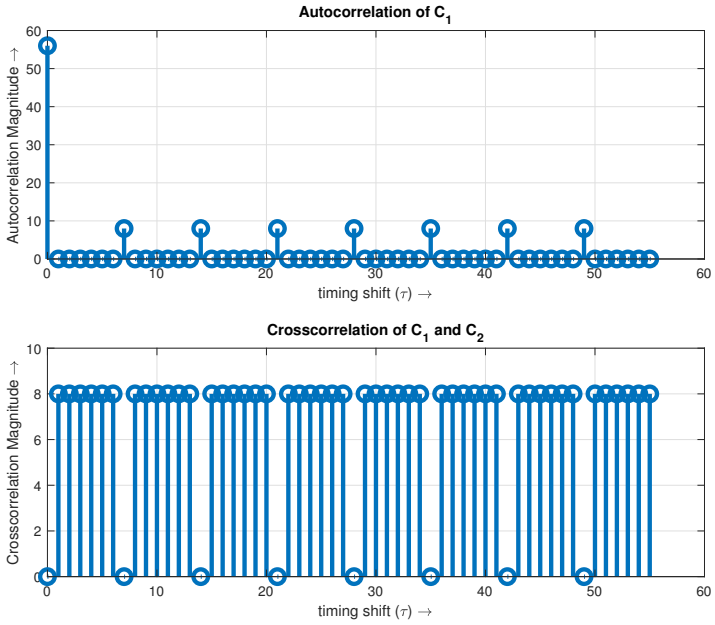


Figure 1: Glimpse of correlation magnitudes of the sequences $\mathbf{c}_1$, $\mathbf{c}_2$ of $\mathcal{C}$ in *Example 3*.

[3] H.-Y. Song. On aspects of Tuscan squares. M.S. thesis, Dept. Elect. Eng., Univ. Southern California, Los Angeles, CA, USA, 1991.

[4] D. Zhang and T. Helleseth. Sequences With Good Correlations Based on Circular Florentine Arrays. *IEEE Trans. Inf. Theory*, 68(5), 3381–3388, 2022.

[5] M. K. Song and H. -Y. Song. New Framework for Sequences With Perfect Autocorrelation and Optimal Crosscorrelation. *IEEE Trans. Inf. Theory*, 67(11), 7490–7500, 2021.

[6] L. R. Welch. Lower bounds on the maximum cross correlation of signals (Corresp.). *IEEE Trans. Inf. Theory*, IT-20(3), 397–399, 1974.

[7] Z. Zhou, T. Helleseth and U. Parampalli. A Family of Polyphase Sequences With Asymptotically Optimal Correlation. *IEEE Trans. Inf. Theory*, 64(4), 2896–2900, 2018.

[8] S. W. Golomb and G. Gong. *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[9] V. M. Sidelnikov. On mutual correlation of sequences. *Soviet Math. Dokl.*, 12, 197–201, 1971.

[10] R. A. Scholtz and L. R. Welch. Group characters: Sequences with good correlation properties. *IEEE Trans. Inf. Theory*, IT-24(5), 537–545, 1978.

[11] K.-U. Schmidt. Sequence families with low correlation derived from multiplicative and additive characters. *IEEE Trans. Inf. Theory*, 57(4), 2291–2294, 2011.

[12] W. O. Alltop. Complex sequences with low periodic correlations (Corresp.). *IEEE Trans. Inf. Theory*, IT-26(3), 350–354, 1980.

[13] R. L. Frank, S. A. Zadoff, and R. Heimiller. Phase shift pulse codes with good periodic correlation properties (Corresp.). *IRE Trans. Inf. Theory*, IT-8(6), 381–382, 1962.

[14] B. M. Popovic. Generalized chirp-like polyphase sequences with optimum correlation properties. *IEEE Trans. Inf. Theory*, 38(4), 1406–1409, 1992.

[15] T. Kasami. Weight distribution formula for some class of cyclic codes. Coordinated Sci. Lab., Univ. Illinois Urbana–Champaign, Urbana, IL, USA, Tech. Rep. R-285 (AD632574), 1966.

[16] P. V. Kumar and O. Moreno. Prime-phase sequences with periodic correlation properties better than binary sequences. *IEEE Trans. Inf. Theory*, 37(3), 603–616, 1991.

[17] S.-C. Liu and J. J. Komo. Nonbinary Kasami sequences over GF(p). *IEEE Trans. Inf. Theory*, 38(4), 1409–1412, 1992.

[18] T. Moriuchi and K. Imamura. Balanced nonbinary sequences with good periodic correlation properties obtained from modified Kumar–Moreno sequences. *IEEE Trans. Inf. Theory*, 41(2), 572–576, 1995.

[19] J.-W. Jang, Y.-S. Kim, J.-S. No, and T. Helleseth. New family of p-ary sequences with optimal correlation property and large linear span. *IEEE Trans. Inf. Theory*, 50(8), 1839–1843, 2004.

[20] S. Boztas, R. Hammons, and P. Y. Kumar. 4-phase sequences with near-optimum correlation properties. *IEEE Trans. Inf. Theory*, 38(3), 1101–1113, 1992.

[21] X. H. Tang and P. Udaya. A note on the optimal quadriphase sequences families. *IEEE Trans. Inf. Theory*, 53(1), 433–436, 2007.

[22] P. Udaya and M. U. Siddiqi. Optimal and suboptimal quadriphase sequences derived from maximal length sequences over Z4. *Appl. Algebra Eng., Commun. Comput.*, 9(2), 161–191, 1998.

[23] J.-H. Chung and K. Yang. A new class of balanced near-perfect nonlinear mappings and its application to sequence design. *IEEE Trans. Inf. Theory*, 59(2), 1090–1097, 2013.

[24] Z. Gu, Z. Zhou, S. Mesnager, P. Udaya. A new family of polyphase sequences with low correlation. *Cryptogr. Commun.* 14, 135–144, 2022.