Interleaved $\mathbb{Z}_4$-Linear Sequences With Low Correlation for Global Navigation Satellite Systems

P. Vijay Kumar[*], Dileep Dharmappa[†], Sugandh Mishra[‡]
[*] Department of Electrical Communication Engineering, IISc Bangalore,
[†] ISTRAC, Indian Space Research Organization, Bengaluru, India,
[‡] Space Applications Centre, Indian Space Research Organization, Ahmedabad, India

Abstract

Global Navigation Satellite Systems (GNSS) employ low-correlation sequences, termed as spreading codes, to distinguish between the signals transmitted by the different satellites. The spreading codes commonly employed have period that is a multiple of 1023, as the fundamental frequency associated with the navigation signals generated onboard all of these systems is 10.23 MHz, derived using highly-stable atomic clocks. The principal contribution of the paper is the construction of a family $\mathcal{J}_{\text{NAV}}$, of low-correlation, binary sequences having period 10230, derived by interleaving a selected set of 5 $\mathbb{Z}_4$-Linear sequences of period 2046 followed by flipping or complementing, a subset of the interleaved sequences. Sequence selection is based on the value of an exponential sum over a Galois ring and interleaving is carried out using the Chinese Remainder Theorem. The period 10230 is of particular interest, as it is the period of the spreading codes employed by major GNSS currently in operation. The $\mathcal{J}_{\text{NAV}}$ spreading code family turns in competitive performance when compared to existing designs including a 4.5 dB improvement in worst-case, even-correlation properties. Additional techniques are employed to ensure that Family $\mathcal{J}_{\text{NAV}}$ has other desirable attributes of a GNSS spreading code such as low values of odd-correlation, an orthogonality property and a simple, shift-register-based implementation.

The construction is shown to be a special instance of a general select, interleave and flip approach to construction that generates families of balanced, low-correlation interleaved $\mathbb{Z}_4$-linear sequences having period $10(2^m-1)$ for $m = 2 \pmod 4$ and $14(2^m-1)$ for $m = 2, 4 \pmod 6$. By replacing the constituent $\mathbb{Z}_4$-linear sequences with Family $\mathcal{A}$ quaternary sequences, the same approach can be used to construct low-correlation, interleaved quaternary sequence families $\mathcal{Q}_{5,\text{BAL}}$, $\mathcal{Q}_{7,\text{BAL}}$ having period $5(2^m-1)$ with $m = 2 \pmod 4$ and $7(2^m-1)$ with $m = 2, 4 \pmod 6$.

Index Terms: Low-correlation sequences, $\mathbb{Z}_4$-linear sequences, quaternary sequences, GNSS, CDMA sequences, interleaved sequences, global navigation satellite systems, spreading codes, NavIC.

I. Introduction

The principal sequence family $\mathcal{J}_{\text{NAV}}$ constructed in this paper is relevant to Global Navigation Satellite Systems (GNSS). Some background on such systems is provided below.

A. Satellite-Based Navigation Systems

Satellite-based navigation systems provide accurate positioning, time and velocity information of a user by determining the distance of the user from a collection of four or more satellites. This distance computation is carried out by determining the time lag between the signal transmitted by the satellite and the replica present in the user's receiver. This estimate of time lag in turn, relies upon the auto and cross-correlation properties of the family of pseudorandom sequences termed as spreading codes, transmitted by the satellites, and which enable satellite-signal acquisition and tracking.

A list of current satellite-based navigation systems appears in Table I. The fundamental frequency associated with the navigation signals generated onboard all of these systems is 10.23 MHz, and this is derived using highly-stable atomic clocks. As a result, for convenience in time measurement, the periods of the spreading codes employed

This paper was presented in part at the *IEEE International Symposium on Information Theory (ISIT)*, Melbourne, (online), July 12-20, 2021. The research of P. Vijay Kumar was supported by the J C Bose National Fellowship JCB/2017/000017.

are a multiple of 1023, as can be seen from Table II. Thus there is interest within the GNSS community, in the construction of spreading codes having period that is of this form. We shall interchangeably use the terms sequence length and sequence period throughout the paper. Table II also provides additional detail about the spreading codes employed, including their method of generation and frequency band of operation.

Table I: Principal Satellite-Based Navigation Systems†.

System	GPS	GLONASS	BDS	GALILEO	NavIC	QZSS
Nominal Constellation Size	24	24	35	30	7	4
Frequency Bands	L1, L2, L5	L1, L2, L3	B1, B2, B3	E1, E5a, E5b, E6	L1, L5, S	L1, L2, L5, E6

† GPS: Global Positioning System (US), GLONASS: Globalnaya Navigazionnaya Sputnikovaya Sistema (Russia), BDS: BeiDou Navigation Satellite System (China), GALILEO (EU), NavIC:Navigation with Indian Constellation (India), and QZSS: Quasi-Zenith Satellite System, (Japan).

Table II: Length and nature of spreading codes employed by different satellite-based navigation systems.

Sl. No.	Satellite-Based Navigation Signal	Code Length	Multiple of 1023	Code Generation Method	Frequency Band	Center Frequency (MHz)
1	GPS L1 C/A	1023	1	Gold code (10-bit SRs)	L1	1575.42
2	NavIC L5	1023	1	Gold codes (10-bit SRs)	L5	1176.45
3	NavIC S	1023	1	Gold codes (10-bit SRs)	S	2492.028
4	BDS B1I	2046	2	Truncated Gold codes (11-bit SRs)	B1	1561.098
5	BDS B2I	2046	2	Truncated Gold codes (11-bit SRs)	B2	1207.14
6	Galileo E1B	4092	4	Memory/Random code	E1	1575.42
7	Galileo E1C	4092	4	Memory/Random code	E1	1575.42
8	Galileo E6B	5115	5	pseudo-random memory code sequences	E6	1278.750
9	Galileo E6C	5115	5	pseudo-random memory code sequences	E6	1278.750
10	GPS L1C	10230	10	Weil sequences of period 10223 with 7-bit padding	L1	1575.42
11	GPS L2 CM	10230	10	Short-cycled output of a 27-bit SR m-sequence	L2	1227.60
12	GPS L5	10230	10	Modulo 2 sum of two 13-bit SRs	L5	1176.45
13	Galileo E5a (I and Q)	10230	10	Two truncated and combined m-sequences from 14-bit SR	E5a	1176.45
14	Galileo E5b (I and Q)	10230	10	Two truncated and combined m-sequences from 14-bit SR	E5b	1207.14
15	GLONASS L1OC	10230	10	Truncated Kasami codes (small set) $(12, 6$-bit SRs)	L1	1600.995
16	GLONASS L2OCp	10230	10	Truncated Kasami codes (small set) $(12, 6$-bit SRs)	L2	1248.06
17	BDS B1C	10230	10	Truncated Weil sequences of period 10243 with 13-bit deletion	B1	1575.42
18	BDS B2a	10230	10	Modulo 2 sum of two 13-bit SRs	B2a	1176.45
19	BDS B3I	10230	10	Modulo 2 sum of two 13-bit SRs	B3	1268.52
20	NavIC L1 (design presented here)	10230	10	Interleaved $\mathbb{Z}_4$-Linear (IZ4) Sequence Family $\mathcal{J}_{\text{NAV}}$	L1	1575.42
21	GPS L2 CL	767250	750	Short-cycled output of a 27-bit SR m-sequence	L2	1227.60

B. Performance Measures Relevant to GNSS

Performance measures that are relevant in the context of a GNSS setting, are even and odd-correlation properties, symbol balance, and pairing of the sequence set into pairs that are orthogonal when in-phase. These performance measures are described in more detail below.

Let $\mathcal{J} = \{ \ \{J^{(a)}(t)\}_{a \in [M]} \ \}$ be a family of M binary $\{0, 1\}$ sequences, each of period L, where for an integer $k \geq 1$, we use $[k]$ to denote the set $\{0, 1, 2, \cdots, k-1\}$.

a) Sequence Period: As noted in Table II above, GNSS currently call for families of sequences whose length or period L, is an integer multiple $L = \ell(1023)$ of 1023. On the other hand, most sequence designs rely upon the theory of finite fields. As a result, the period of the sequences so designed, is related to the size of the finite field. The families of Gold, Kasami, Bent and No sequences [1]–[4], [7], [8] all have period of the form $(2^k - 1)$ for some integer $k \geq 2$. $\mathbb{Z}_4$-linear sequences [9]–[15], which make use of the related theory of Galois rings, have period that is twice this number, i.e., of the form $2(2^k - 1)$. The sequence designs by Gong [16] have period of the form p^2 or $(p^k - 1)^2$ for p prime. The design by Paterson [17] has period that of the form p^2 for p prime. Thus the options for sequence length are somewhat limited, and constructing sequences having the desired period $L = \ell(1023)$ for $\ell > 2$ becomes a challenging problem. A principal focus of the present paper is on the case $\ell = 10$, corresponding to the period 10230 widely used in the satellite-based navigation setting (see Table II), and this is discussed in detail below.

b) Even-Correlation: The even correlation of a pair of sequences $\{J^{(a)}(t)\}, \{J^{(b)}(t)\}$ at shift τ, is given by

$$\Omega(a, b, \tau) \ = \ \sum_{t=0}^{L-1} (-1)^{J^{(a)}(t+\tau) - J^{(b)}(t)}, \tag{1}$$

where the sum $(t + \tau)$ is computed modulo the period L. An even correlation is referred to as an even auto or an even cross-correlation depending upon whether $a = b$ or not respectively. The maximum out-of-phase even autocorrelation magnitude and the maximum even cross-correlation magnitude will be denoted by the symbols $\Omega_{a,\max}$ and $\Omega_{c,\max}$ respectively:

$$\Omega_{a,\max} \ := \ \max_{a \in [M]} \{ \ |\Omega(a, a, \tau)| \ \mid \tau \in [L], \tau \neq 0 \}, \tag{2}$$

$$\Omega_{c,\max} \ := \ \max_{\substack{a,b \in [M], \\ a \neq b}} \{ \ |\Omega(a, b, \tau)| \ \mid \tau \in [L] \}. \tag{3}$$

By maximum nontrivial (even) correlation magnitude, we will mean the quantity $\Omega_{\max}$ defined by

$$\Omega_{\max} \ = \ \max \{\Omega_{a,\max}, \ \ \Omega_{c,\max}\}. \tag{4}$$

c) Odd Correlation: The aperiodic correlation $\hat{\Omega}(a, b, \tau)$ of a pair of binary sequences $\{J^{(a)}(t)\}, \{J^{(b)}(t)\}$ at shift τ, is given by

$$\hat{\Omega}(a, b, \tau) \ = \ \begin{cases} \sum_{t=0}^{L-1-\tau} (-1)^{J^{(a)}(t+\tau) - J^{(b)}(t)}, & 0 \leq \tau \leq (L-1), \\ \sum_{t=-\tau}^{L-1} (-1)^{J^{(a)}(t+\tau) - J^{(b)}(t)}, & -(L-1) \leq \tau < 0. \end{cases} \tag{5}$$

An aperiodic correlation is referred to as an aperiodic autocorrelation or else an aperiodic cross-correlation depending upon whether $a = b$ or not respectively. The even and aperiodic correlation functions of a pair of sequences having period L, are related by

$$\Omega(a, b, \tau) \ = \ \hat{\Omega}(a, b, \tau) \ + \ \hat{\Omega}(a, b, \tau - L), \quad 0 \leq \tau \leq (L-1).$$

The odd-correlation function of a pair of periodic binary sequences $\{J^{(a)}(t)\}, \{J^{(b)}(t)\}$ having period L, at shift τ is defined by

$$\begin{aligned} \Omega^{(\text{odd})}(a, b, \tau) \ &= \ \hat{\Omega}(a, b, \tau) \ - \ \hat{\Omega}(a, b, \tau - L), \quad 0 \leq \tau \leq (L-1), \\ &= \ \sum_{t=0}^{L-1-\tau} (-1)^{J^{(a)}(t+\tau) - J^{(b)}(t)} \ - \ \sum_{t=L-\tau}^{L-1} (-1)^{J^{(a)}(t+\tau) - J^{(b)}(t)}, \quad 0 \leq \tau \leq (L-1). \end{aligned}$$

Odd correlations arise when the spreading code is modulated using Binary Phase-Shift-Keying (BPSK), by a data sequence whose bit duration is equal to an entire period or a multiple of an entire period, of the spreading code, and where the window of length L chips over which correlation takes place, corresponds to two adjacent data bits having opposing signs. We use the term chip to denote the time duration of a symbol in the transmitted spreading code.

An odd correlation is referred to as an odd autocorrelation or else an odd cross-correlation depending upon whether $a = b$ or not respectively. Lowering odd-correlation values is of importance since, when one is trying to align the spreading code in the receiver to the incoming spreading code, and the incoming spreading code while periodic, is modulated by data, the correlations that impact receiver performance are odd correlations rather than even correlations. The maximum auto and cross-correlation magnitudes in the case of odd correlation will be denoted by the symbols denoted by $\Omega^{(\text{odd})}_{a,\max}$ and $\Omega^{(\text{odd})}_{c,\max}$ respectively. Thus we have:

$$\Omega^{(\text{odd})}_{a,\max} := \max_{a\in[M]} \left\{ |\Omega^{(\text{odd})}(a,a,\tau)| \tau \in [L], \tau \neq 0 \right\}, \tag{6}$$

$$\Omega^{(\text{odd})}_{c,\max} := \max_{\substack{a,b\in[M],\\ a\neq b}} \left\{ |\Omega^{(\text{odd})}(a,b,\tau)| \ \mid \tau \in [L] \right\}. \tag{7}$$

In the GNSS literature, the quantities $\Omega_{a,\max}$, $\Omega_{c,\max}$, $\Omega^{(\text{odd})}_{a,\max}$, $\Omega^{(\text{odd})}_{c,\max}$ are respectively referred to as Even ACR (EACR), Even CCR (ECCR), Odd ACR (OACR), and odd CCR (OCCR). Thus, we have:

$$\text{EACR} := \Omega_{a,\max}, \qquad \text{ECCR} := \Omega_{c,\max}, \qquad \text{OACR} := \Omega^{(\text{odd})}_{a,\max}, \qquad \text{OCCR} := \Omega^{(\text{odd})}_{c,\max}. \tag{8}$$

d) Balance: It is also desirable that the sequences employed in a GNSS system be balanced as far as possible. The symbol balance of a binary sequence $\{J(t)\}$ of period L is defined to be the numerical value

$$|\sum_{t=0}^{L-1}(-1)^{J(t)}| \ = \ | \ L \ - \ 2\sum_{t=0}^{L-1} w_H(J(t)) \ |, \tag{9}$$

where the real-valued Hamming-weight function $w_H(\cdot)$ satisfies $w_H(J(t)) = 0$ if $J(t) = 0$, and $w_H(J(t)) = 1$ if $J(t) = 1$. It follows that if the value of the symbol balance equals b, the number of zeros and ones in each period of $\{J(t)\}$ differs by an amount b. In particular, if $b = 0$, this implies that L is even and that the number of zeros and ones is the same in each period, i.e., the sequence is perfectly balanced.

e) Orthogonal Pairs: Another property that is desired in a GNSS setting, is the orthogonal-pairs property. This property requires that the designed family should permit a pairing

$$\left\{ \{J^{(a)}(t)\} \mid a \in [M] \right\} \quad \Longrightarrow \quad \left\{ \left(\{J^{a_i}(t)\}, \{J^{b_i}(t)\}\right) \mid i \in [M/2] \right\},$$

such that the in-phase correlation,

$$\sum_{t=0}^{L-1} (-1)^{J^{(a_i)}(t)+J^{(b_i)}(t)}, \tag{10}$$

is for every pair, of very small magnitude. The need for this last property, which we will term as the orthogonal-pairs property, arises because each satellite is assigned a pair of sequences corresponding to data and pilot. Typically the pilot signal is used to aid synchronization, while the data signals is used to communicate information. Since these two signals are received in synchronization at the receiver, orthogonality of the data and pilot signals when in phase, is used to ensure that neither sequence poses an interference to the other. The pilot signal is modulated by a known secondary pseudorandom code called the overlay code, to assist in tracking after acquisition has taken place, while the data sequence is modulated by low-rate, navigational data.

C. Principal Contribution

The principal contribution of the paper is the construction of a family $\mathcal{J}_{\text{NAV}}$ of low-correlation binary sequences having period 10230. The family is constructed via a Select, Interleave and Flip (S-I-F) approach. The two-step S-I-F approach may be described as follows. In the first step, a set of 5 $\mathbb{Z}_4$-linear sequences of period 2046 are selected based on the value of an exponential sum over a Galois ring, and then interleaved using the Chinese Remainder Theorem. In the second step, a subset of the sequences selected for interleaving are then flipped or complemented. The selection prior to interleaving is carried out to ensure low correlation properties. The flipping operation is aimed at improving symbol balance and is defined below.

Definition 1. *By flipping or complementing a binary sequence $\{s(t)\}$ of period P, we mean replacing*

$$\{(-1)^{s(t)}\}_{t=0}^{P-1} \quad by \quad \{(-1) \times (-1)^{s(t)}\}_{t=0}^{P-1} \;=\; \{(-1)^{s(t)+1}\}_{t=0}^{P-1}.$$

By flipping or complementing a quaternary sequence $\{s(t)\}$ of period P, i.e., a sequence having symbol alphabet $\mathbb{Z}_4$ of period P, we mean replacing

$$\{\imath^{s(t)}\}_{t=0}^{P-1} \quad by \quad \{(-1) \times \imath^{s(t)}\}_{t=0}^{P-1} \;=\; \{\imath^{s(t)+2}\}_{t=0}^{P-1}.$$

A more detailed overview of the construction of Family $\mathcal{J}_{\text{NAV}}$ is presented in the next section, Section II. As can be seen from Table II, the period 10230 is of particular interest, as it is the period of the spreading codes employed by major satellite-based navigation systems currently in operation. Table III presents a tabular comparison of the properties of Family $\mathcal{J}_{\text{NAV}}$ in comparison with spreading-code designs employed by GPS and BDS. To our knowledge, the properties of the GPS and BDS families improve upon corresponding of other satellite-based navigation systems employing the same period 10230. The spreading codes employed by both GPS as well as BDS are based upon the family of Weil sequences [18]–[21], [24]. The maximum correlation magnitudes appearing in the table, are presented in 3 formats: as an integer, normalized to $\sqrt{L}$, where $L = 10230$ and in dB where the dB value is derived from

$$x \;\text{ in dB} \;=\; 20\log\big(\frac{x}{10230}\big).$$

The normalization with respect to $\sqrt{L}$ is carried out because for large family size M and block length L, the Welch lower bound [30]

$$\Omega_{\max} \;\geq\; L\sqrt{\frac{M-1}{ML-1}},$$

on maximum even-correlation magnitude, approaches the value $\sqrt{L}$. The lower the magnitudes of cross-correlation and out-of-phase auto correlation, the better is the performance in terms of signal acquisition and resistance to inter-channel interference. Equivalently, the more negative the value in dB, the better the performance. The numerical values appearing in Table III are based on our MATLAB simulations and agree with the results presented in [22] and [26].

As can be seen from the table, Family $\mathcal{J}_{\text{NAV}}$ turns in competitive performance when compared to existing designs. While the EACR, OACR, OCCR, sequence imbalance and orthogonality properties are comparable, Family $\mathcal{J}_{\text{NAV}}$ achieves a 4.5 dB improvement in ECCR. The low even-correlation values of Family $\mathcal{J}_{\text{NAV}}$ are obtained by exploiting a closed-form expression for an exponential sum over a Galois ring. Additional techniques are employed to ensure that the Family $\mathcal{J}_{\text{NAV}}$ has other desirable attributes such as symbol balance, low values of odd-correlation and a simple, shift-register-based implementation. Sequences within the family can also be paired such that sequences within a pair are orthogonal when in phase [1].

D. Additional Contributions

With respect to even-correlation and balance properties, it is shown that Family $\mathcal{J}_{\text{NAV}}$ is a special instance of a more general family, Family $\mathcal{J}_{5,\text{BAL}}$, of balanced, low-correlation binary sequences having period $L = 10(2^m - 1)$ for $m = 2 \pmod 4$, that is also constructed by following the S-I-F approach.

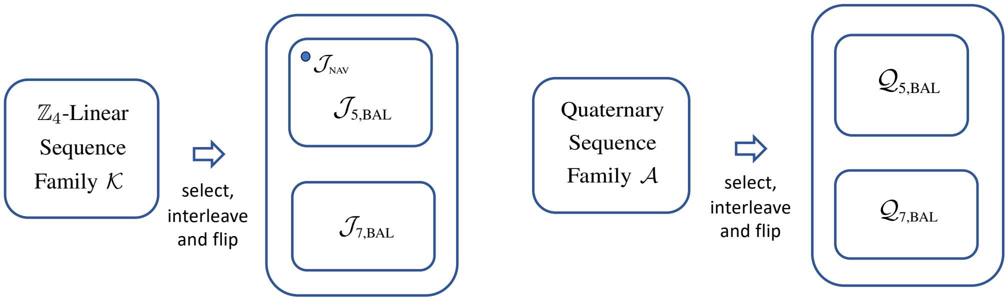
It is additionally shown that the same approach can be applied to construct families of

1) balanced, low-correlation, binary sequence families $\mathcal{J}_{7,\text{BAL}}$ having period of the form $L = 14(2^m - 1)$ for $m = 2, 4 \pmod 6$,
2) low-correlation, quaternary sequence families $\mathcal{Q}_{5,\text{BAL}}$ having period of the form $L = 5(2^m - 1)$ for $m = 2 \pmod 4$, and
3) low-correlation, quaternary sequence families $\mathcal{Q}_{7,\text{BAL}}$ having period of the form $L = 7(2^m - 1)$ for $m = 2, 4 \pmod 6$.

[1] The spreading code family $\mathcal{J}_{\text{NAV}}$ has been incorporated into the $L1$ band Standard Positioning Service signal of the Indian Space Research Organization's NavIC (Navigation with Indian Constellation) satellite system, see [25].

Table III: Comparing performance of the Interleaved $\mathbb{Z}_4$-linear (IZ4) Sequence Family $\mathcal{J}_{\text{NAV}}$ with that of the primary codes employed by GPS and BDS in the $L1$ band.

Performance Parameter	IZ4 Family $\mathcal{J}_{\text{NAV}}$	GPS L1C codes	BDS B1C codes
EACR	266 $= 2.63\sqrt{L}$ = -31.7 dB	282 $= 2.79\sqrt{L}$ = -31.19 dB	282 $= 2.79\sqrt{L}$ = -31.19 dB
ECCR	266 $= 2.63\sqrt{L}$ = -31.7 dB	446 $= 4.41\sqrt{L}$ = -27.21dB	442 $= 4.37\sqrt{L}$ = -27.29 dB
OACR	330 $= 3.26\sqrt{L}$ = -29.83 dB	406 $= 4.01\sqrt{L}$ = -28.03 dB	282 $= 2.79\sqrt{L}$ = -31.19 dB
OCCR	484 $= 4.79\sqrt{L}$ = -26.5 dB	500 $= 4.94\sqrt{L}$ = -26.22 dB	442 $= 4.37\sqrt{L}$ = -27.29 dB
Sequence Imbalance	0 or 2	0	0
Orthogonality	0	2	2


$\mathbb{Z}_4$-Linear Sequence Family $\mathcal{K}$
select, interleave and flip
$\mathcal{J}_{\text{NAV}}$
$\mathcal{J}_{5,\text{BAL}}$
$\mathcal{J}_{7,\text{BAL}}$
Quaternary Sequence Family $\mathcal{A}$
select, interleave and flip
$\mathcal{Q}_{5,\text{BAL}}$
$\mathcal{Q}_{7,\text{BAL}}$

Interleaved $\mathbb{Z}_4$-Linear Sequence Families (IZ4)

Interleaved Quaternary Sequence Families (IQS)

Figure 1: The four sequence families arising from the Select, Interleave and Flip (S-I-F) approach to sequence construction in this paper. Family $\mathcal{J}_{\text{NAV}}$ is an instance of Family $\mathcal{J}_{5,\text{BAL}}$ corresponding to $m = 10$, i.e., period 10230. The binary Interleaved $\mathbb{Z}_4$-linear sequence families, i.e., IZ4 sequence families, $\mathcal{J}_{5,\text{BAL}}$, $\mathcal{J}_{7,\text{BAL}}$ on the left, are obtained by applying the S-I-F approach to binary sequence Family $\mathcal{K}$. The Interleaved Quaternary Sequence families, i.e., IQS sequence families $\mathcal{Q}_{5,\text{BAL}}$, $\mathcal{Q}_{7,\text{BAL}}$ on the right, are obtained by applying the S-I-F approach to quaternary sequence Family $\mathcal{A}$.

In the case of the quaternary sequence families, when employing the S-I-F approach, we interleave sequences drawn from Family $\mathcal{A}$ quaternary sequences in place of the binary sequence family $\mathcal{K}$, see Fig. 1. Quaternary sequence families $\mathcal{Q}_{5,\text{BAL}}$ and $\mathcal{Q}_{7,\text{BAL}}$ are approximately balanced, and the symbol balance value is identical to that of Family $\mathcal{A}$ and is on the order of the square root of the period of the sequence family, see Table IV below.

Definition 2. *We will refer to any binary sequence family such as Families $\mathcal{J}_{\text{NAV}}$, $\mathcal{J}_{5,\text{BAL}}$, $\mathcal{J}_{7,\text{BAL}}$ obtained by interleaving a collection of $\mathbb{Z}_4$-linear sequences as an Interleaved $\mathbb{Z}_4$-linear sequence family, or in abbreviated form, as an IZ4 family.*

Definition 3. *We will refer to any quaternary sequence family such as Families $\mathcal{Q}_{5,\text{BAL}}$, $\mathcal{Q}_{7,\text{BAL}}$obtained by interleaving a collection of quaternary sequences, i.e., sequences having $\mathbb{Z}_4$ as their symbol alphabet, as an Interleaved Quaternary Sequence family, or in abbreviated form, as an IQS family.*

Parameters of the four sequence families constructed here are listed in Table IV.

Table IV: The select-and-interleave approach presented here can be used to generate the sequences having periods and correlation performance as shown in the table. The quantities ρ_5, ρ_7 appearing in the table, are given by, $\rho_5 = \sqrt{(5 + (4 \times 2^{m/2}))^2 + 2^m}$ and $\rho_7 = \sqrt{(7 + (5 \times 2^{m/2}))^2 + (2 \times 2^{m/2})^2}$.

Sequence Family	Symbol Alphabet	Code Length L	Parameter Constraint	Family Size	Maximum Correlation Magnitude $\Omega_{\max}$	Asymptotic Value of $\Omega_{\max}$	Symbol Balance
$\mathcal{J}_{5,\text{BAL}}$	Binary	$10 \times (2^m - 1)$	$m = 2 \pmod 4$ $m \geq 6$	$2\lfloor \frac{2^{m-2}}{3} \rfloor$	$(8 \times 2^{m/2}) + 10$	$2.53\sqrt{L}$	2
$\mathcal{J}_{7,\text{BAL}}$	Binary	$14 \times (2^m - 1)$	$m = 6k + \ell$ $\ell \in \{2, 4\}$ $m \geq 4$	2^{m-3}	$(10 \times 2^{m/2}) + 14$	$2.67\sqrt{L}$	2
$\mathcal{Q}_{5,\text{BAL}}$	Quaternary	$5 \times (2^m - 1)$	$m = 2 \pmod 4$ $m \geq 6$	$\lfloor \frac{2^m}{5} \rfloor$	ρ_5	$1.84\sqrt{L}$	$(1 + 2^{m/2})$
$\mathcal{Q}_{7,\text{BAL}}$	Quaternary	$7 \times (2^m - 1)$	$m = 6k + \ell$ $\ell \in \{2, 4\}$ $m \geq 4$	2^{m-3}	ρ_7	$2.04\sqrt{L}$	$(1 + 2^{m/2})$

E. Outline of the Paper

An overview of the select, interleave and flip (s-i-f) approach to constructing sequence families $\mathcal{J}_{5,\text{BAL}}$, $\mathcal{J}_{7,\text{BAL}}$, $\mathcal{Q}_{5,\text{BAL}}$ and $\mathcal{Q}_{7,\text{BAL}}$ is provided in Section II. The $\mathbb{Z}_4$-linear Family $\mathcal{K}$ from which the sequences being interleaved are drawn, is introduced in Section III. The correlation properties of $\mathcal{K}$ are studied in Section IV, and a closed-form expression for correlation values is provided. The construction of binary sequence family $\mathcal{J}_{5,\text{LEC}}$ is presented in Section V. A closed-form expression for the correlation values of Family $\mathcal{J}_{5,\text{LEC}}$ is provided in Section VI. A significantly improved upper bound on even-correlation values appears in the subsequent section, Section VII. Family $\mathcal{J}_{5,\text{BAL}}$ that has symbol balance to within 2 and the same correlation properties as Family $\mathcal{J}_{5,\text{LEC}}$ is presented in Section VIII. The next two sections, Section IX and Section X deal with an instance of Family $\mathcal{J}_{5,\text{BAL}}$, namely Family $\mathcal{J}_{\text{NAV}}$, having period 10230, that is well-suited to GNSS applications in terms of having low values of odd-correlation and satisfying the orthogonal-pairs property. The approach adopted to construct $\mathcal{J}_{\text{NAV}}$ is presented in Section IX. It is shown in Section X, that Family $\mathcal{J}_{\text{NAV}}$ admits a simple, shift-register-based implementation. The next section, Section XI, shows how the same S-I-F approach can be used to generate the low-correlation sequence families $\mathcal{J}_{7,\text{BAL}}$, $\mathcal{Q}_{5,\text{BAL}}$ and $\mathcal{Q}_{7,\text{BAL}}$. Background on Galois rings and on a relevant exponential sum is provided in the Appendix.

II. Overview of the Sequence-Family Constructions

As noted in the prior section,

- the principal contribution here, is the construction of a binary sequence family, Family $\mathcal{J}_{\text{NAV}}$ having period $L = 10230$, obtained by interleaving a collection of 5 $\mathbb{Z}_4$-linear sequences, each of period 10230, and that
- this construction is shown to be a specific instance of a general S-I-F approach that generates the four sequence families $\mathcal{J}_{5,\text{BAL}}$, $\mathcal{J}_{7,\text{BAL}}$, $\mathcal{Q}_{5,\text{BAL}}$ and $\mathcal{Q}_{7,\text{BAL}}$ that are listed in Table IV.

Before providing additional detail, we present some background.

A. $\mathbb{Z}_4$-linear sequences and the MSB-Gray Map

Given an element $s \in \mathbb{Z}_4$, of the form $s = u + 2v,\ u, v \in \{0, 1\}$, we will refer to binary values u, v as the least significant bit (LSB) and most significant bit (MSB) respectively, of s. Note that the MSB map defined by $\text{MSB}(s) = v$, is a nonlinear map. We define a $\mathbb{Z}_4$-linear sequence to be any binary $\{0, 1\}$ sequence $\{K_j(t)\}$ that can be expressed in the form

$$K(t) \quad = \quad \text{MSB}\left\{3^t Q(t)\right\}, \quad \text{all } t, \tag{11}$$

where $\{Q(t)\}$ is a quaternary sequence that has odd period n and that satisfies a recursion over $\mathbb{Z}_4$ of the form

$$Q(t) \;=\; \sum_{i=1}^{d} c_i \; Q(t-i), \;\; d \geq 1, \quad c_i \in \mathbb{Z}_4. \tag{12}$$

We shall refer to a recursion of the form in (12) as a linear recursion. We will refer to the map

$$\mathcal{G}_{\text{MSB}} : \{Q(t)\} \;\; \rightarrow \;\; \{K(t)\}, \tag{13}$$

mapping a quaternary sequence $\{Q(t)\}$ having odd period n to a binary sequence $\{K_j(t)\}$ via equation (11) as the MSB-Gray map for reasons that will become clear in Section III. Clearly, $\{K(t)\}$ is periodic with period dividing $2n$. Low-correlation families of $\mathbb{Z}_4$-linear sequences can be found discussed in [9]–[14]. The specific family $\mathcal{K}$ of low-correlation $\mathbb{Z}_4$-linear sequences that we make use of in this paper have period $2(2^m-1)$ with m even, and are referred to in [14] as Generalized Udaya-Siddiqi Sequences. This sequence family may be regarded as an extension to the case of even exponent m, of sequence families described in [9], [11], [12]. Relevant parameters of Family $\mathcal{K}$ appear below.

Sequence Family	Symbol Alphabet	Code Length R	Relevant Parameter Constraint	Family Size	Maximum Correlation Magnitude $\Omega_{\max}$	Asymptotic Value of $\Omega_{\max}$
$\mathcal{K}$	Binary $\{0,1\}$	$R = 2(2^m-1)$	m even	2^m	$1 + 2^{m/2+1}$	$\sqrt{2}\sqrt{R}$

B. Quaternary Sequence Family $\mathcal{A}$

By a quaternary sequence family, we will mean a sequence family having symbol alphabet $\mathbb{Z}_4$. Quaternary sequences are associated to Quaternary Phase-Shift Keying (QPSK) modulation in the same way:

$$a \in \mathbb{Z}_4 \;\; \rightarrow \;\; \cos\big(2\pi f_0 t \; + \; a\frac{\pi}{2}\big),$$

as binary sequences are associated to BPSK modulation. Here, f_0 denotes the carrier frequency. As an example of their application in practice, quaternary sequence family, Family $S(2)$ constructed in [23] was part of the 3G WCDMA cellular communication standard.

If $\mathcal{Q} = \big\{ \; \{Q^{(a)}(t)\}_{a\in[M]} \; \big\}$ is a family of M quaternary sequences over $\mathbb{Z}_4$, each of period n, then the even correlation of a sequence pair $\{Q^{(a)}(t)\}, \{Q^{(b)}(t)\}$ at shift τ, is given by

$$\Omega(a,b,\tau) \;\;=\;\; \sum_{t=0}^{n-1} (\imath)^{Q^{(a)}(t+\tau) - Q^{(b)}(t)}, \tag{14}$$

where the sum $(t+\tau)$ is computed modulo the period n. Quaternary sequence Family $\mathcal{A}$ [33], [34] is an efficient family of low-correlation sequences having the parameters listed below:

Sequence Family	Symbol Alphabet	Code Length n	Relevant Parameter Constraint	Family Size	Maximum Correlation Magnitude $\Omega_{\max}$	Asymptotic Value of $\Omega_{\max}$
$\mathcal{A}$	Quaternary $\mathbb{Z}_4$	$n = (2^m-1)$	m odd or even	2^m+1	$1 + 2^{m/2}$	$\sqrt{n}$

C. Rectangular Interleaving

Let $\{\{U_i(t)\}_{t=0}^{p-1} \mid 0 \leq i \leq q-1\}\}$ be a set of q sequences, each having common period p that are being interleaved, then the sequence $\{J(t)\}$ obtained via rectangular interleaving is defined to be given by

$$J(t) \;\; := \;\; U_j(\ell),$$

where the pair (j,ℓ) are uniquely recovered from t using the q-ary decomposition

$$t \;\; = \;\; q\ell + j, \;\; 0 \leq j \leq (q-1), \; 0 \leq \ell \leq (p-1).$$

This is illustrated below for the case $q = 3, p = 7$.

$\{U_0(t)\}$	$\{U_1(t)\}$	$\{U_2(t)\}$
$U_0(0)$	$U_1(0)$	$U_2(0)$
$U_0(1)$	$U_1(1)$	$U_2(1)$
$U_0(2)$	$U_1(2)$	$U_2(2)$
$U_0(3)$	$U_1(3)$	$U_2(3)$
$U_0(4)$	$U_1(4)$	$U_2(4)$
$U_0(5)$	$U_1(5)$	$U_2(5)$
$U_0(6)$	$U_1(6)$	$U_2(6)$

rectangular $\Longrightarrow$ interleaving

$\{J(t)\}$		
$J(0)$	$J(1)$	$J(2)$
$J(3)$	$J(4)$	$J(5)$
$J(6)$	$J(7)$	$J(8)$
$J(9)$	$J(10)$	$J(11)$
$J(12)$	$J(13)$	$J(14)$
$J(15)$	$J(16)$	$J(17)$
$J(18)$	$J(19)$	$J(20)$

D. *CRT-Based Interleaving*

The form of interleaving employed in our IZ4 construction is based on the Chinese Remainder Theorem (CRT). The reason for employing CRT-based interleaving is because such an interleaving makes the problem of constructing an interleaved sequence set with reduced correlation values more tractable, as will shortly be explained (see Remark 4 in Section VI). Once again, let (p, q) be a pair of integers ≥ 2, where we require this time, that (p, q) are relatively prime. Let $r = pq$. Since (p, q) are relatively prime, it follows that the map from $\mathbb{Z}_r \to \mathbb{Z}_p \times \mathbb{Z}_q$ given by

$$t \quad \Rightarrow \quad (\ell, j)$$

with

$$\ell \;=\; t \pmod{p}, \qquad j \;=\; t \pmod{q},$$

provides a 1-1 correspondence between integers $t \in \mathbb{Z}_r$ and pairs $(\ell, j) \in \mathbb{Z}_p \times \mathbb{Z}_q$. Let $\{\{U_i(t)\}_{t=0}^{p-1} \mid 0 \leq i \leq q-1\}\}$ be as before, a set of q sequences, each having common period p that are being interleaved, then the sequence $\{J(t)\}$ obtained via CRT-based interleaving is defined to be given by

$$J(t) \;:=\; U_j(\ell), \quad \text{where } \ell = t \pmod{p}, \;\; j = t \pmod{q}.$$

Since $(p, q) = 1$, it follows that $\{J(t)\}$ has period $r = pq$. An analogous example showing the CRT-based interleaving of $q = 3$ sequences, each of period $p = 7$, to yield a single interleaved sequence of period $r = 21$ is shown below. As can be seen, CRT-based interleaving can also be regarded as a form of diagonal interleaving with wrap around.

$\{U_0(t)\}$	$\{U_1(t)\}$	$\{U_2(t)\}$
$U_0(0)$	$U_1(0)$	$U_2(0)$
$U_0(1)$	$U_1(1)$	$U_2(1)$
$U_0(2)$	$U_1(2)$	$U_2(2)$
$U_0(3)$	$U_1(3)$	$U_2(3)$
$U_0(4)$	$U_1(4)$	$U_2(4)$
$U_0(5)$	$U_1(5)$	$U_2(5)$
$U_0(6)$	$U_1(6)$	$U_2(6)$

CRT-based $\Longrightarrow$ interleaving

$\{J(t)\}$		
$J(0)$	$J(7)$	$J(14)$
$J(15)$	$J(1)$	$J(8)$
$J(9)$	$J(16)$	$J(2)$
$J(3)$	$J(10)$	$J(17)$
$J(18)$	$J(4)$	$J(11)$
$J(12)$	$J(19)$	$J(5)$
$J(6)$	$J(13)$	$J(20)$

E. *Achieving Desired Period* 10230 *in the GNSS Context*

As noted in Section I-B, existing sequence designs in the literature are limited in terms of the length or periods for which a low-correlation sequence family can be generated. Faced with the task of designing a signal set for GPS of period 10230, and noting the limited sequence-length options available, Rushanan [18]–[20] came up with a design of a family $\mathcal{W}$ of sequences termed as Weil sequences having odd-prime length p, and given by

$$\mathcal{W} \;=\; \left\{ \{s_i(t)\}_{t=0}^{p-1} \mid 1 \leq i \leq \frac{p-1}{2} \right\},$$

where $s_i(t) = z_{t+i} z_t$, with $(t + i)$ computed modulo p and with z_t, for $t \neq 0$ being the Legendre symbol:

$$z_0 \;=\; -1, \qquad z_t \;=\; \left(\frac{t}{p}\right), \quad 1 \leq t \leq (p-1).$$

The Weil sequence family for primes $p = 3 \pmod 4$ was previously studied by Guohua and Quanin in [21]. The idea in [18]–[20] was that it is easier to find primes that are closer in length to the desired period of 10230 than the other possibilities for sequence length presented by prior sequence designs. The closest primes to 10230 are 10223 and 10243. As an illustration, the GPS Weil-sequence-based spreading-code design by Rushanan [20], begins from a family of Weil sequences of length 10223 and adds 7 padding bits to obtain the desired length of 10230. The BDS design [24], also based on Weil sequences, begins with a family of Weil sequences having period 10243 and truncates 13 bits to arrive at the period 10230. However, both padding and truncation can cause a degradation in correlation properties. Our approach described below, achieves the desired period 10230 without need for either padding or truncation.

F. Our Approach

Our approach to constructing the desired sequence family $\mathcal{J}_{\text{NAV}}$ involves three steps. We will focus in the beginning on the first two steps as these steps are more general and yield the low-correlation sequence families $\mathcal{J}_{5,\text{BAL}}$, $\mathcal{J}_{7,\text{BAL}}$, $\mathcal{Q}_{5,\text{BAL}}$ and $\mathcal{Q}_{7,\text{BAL}}$. We begin with the generation of Family $\mathcal{J}_{5,\text{BAL}}$.

1) Family $\mathcal{J}_{5,BAL}$: Our approach is the two-step S-I-F approach mentioned in Section I-C. The two steps involved in the generation of Family $\mathcal{J}_{5,\text{BAL}}$ are illustrated in Fig. 2.

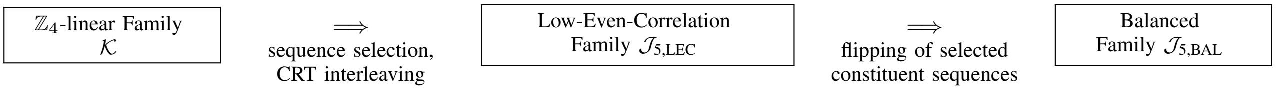


Figure 2: The two-step construction of the binary sequence Family $\mathcal{J}_{5,\text{BAL}}$. Each sequence in Family $\mathcal{J}_{5,\text{LEC}}$ is obtained by carrying out CRT-based interleaving of a carefully selected subset of 5 sequences from Family $\mathcal{K}$ with $m = 2 \pmod 4$. Family $\mathcal{J}_{5,\text{BAL}}$ is derived by selectively complementing or flipping the interleaved sequences so as to achieve symbol balance within 2 without impacting the low, even-correlation properties.

1) The first step is to interleave 5 sequences from Family $\mathcal{K}$ of period $2(2^m - 1)$ with $m = 2 \pmod 4$, to obtain a single sequence of period

$$5 \times 2(2^m - 1) \quad = \quad 10(2^m - 1).$$

The restriction to $m = 2 \pmod 4$ is in part because of our interest in the specific case $m = 10$ corresponding to period 10230 and in part, because it is only in this case that our approach can be used to improve upon the naive (i.e., rectangular) interleaving approach explained in Section II-C. Such interleaving would in general, result in a family having maximum correlation magnitude $5(2 + 2^{m/2+1})$. Our approach involves interleaving based on the CRT coupled with careful selection of the set of 5 sequences that are being interleaved. It turns out that this approach allows us to lower the value of $\Omega_{\max}$ to $4(2^{m/2+1}) + 2$.

Remark 1. *The quantity $2(5 + 4(2^k))$ with $m = 2k = 10$, evaluates to 266 and as can be seen from the entries in Table III, it is this reduction from $5(2^6 + 2) = 330$ to $4(2^6) + 2 = 266$ that causes the value of $\Omega_{\max}$ to be lower than that of the other designs by 4.5 dB.*

A key ingredient in the selection process is the availability of a closed-form expression for an exponential sum over a Galois ring. This also allows us to provide closed-form expressions for both auto and cross-correlation in the new family $\mathcal{J}_{5,\text{BAL}}$. However, at the end of this step, the sequences will in general have significant symbol imbalance.

2) The second step is to selectively complement or flip the 5 constituent sequences being interleaved by making use of the flipping operation defined in Definition 1. It turns out that this flipping can be done in such a way that the symbol balance is reduced to 2 while preserving the maximum correlation value $\Omega_{\max}$.

The conceptual generation of sequence Family $\mathcal{J}_{5,\text{BAL}}$ appears in Fig. 3.

2) Family $\mathcal{J}_{7,BAL}$: An analogous two-step approach can be used to construct Family $\mathcal{J}_{7,\text{BAL}}$ with the difference that here we require $m = 2, 4, \pmod 6$ and we interleave 7 sequences from Family $\mathcal{K}$.

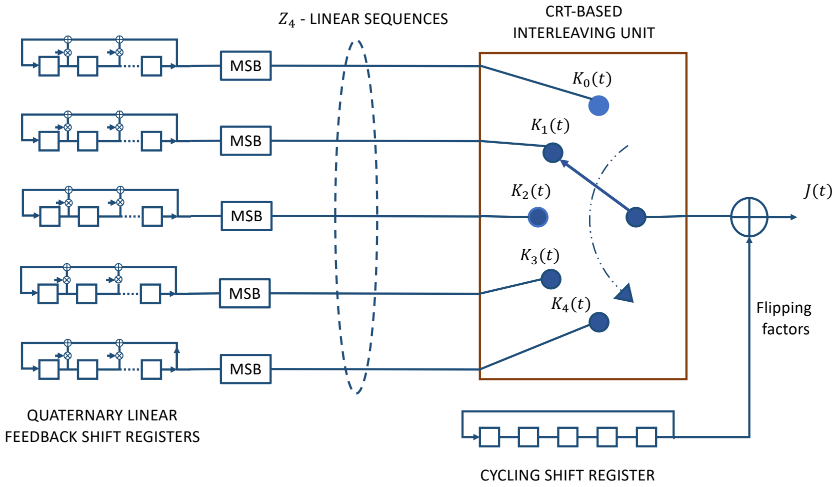


Figure 3: Illustrating the generation of sequences within the Family $\mathcal{J}_{5,\text{BAL}}$. The five binary $\mathbb{Z}_4$-linear sequences from Family $\mathcal{K}$ that are being interleaved appear at the output of the five MSB maps. The rotary switch represents a conceptually-simple means of carrying out CRT-based interleaving of the 5 sequences. The five-stage binary cycling shift-register shown in the lower-right, implements flipping of the constituent sequences. All shift registers and the rotary switch are synchronously advanced. The output sequence $\{J(t)\}$ is a sequence belonging to Family $\mathcal{J}_{5,\text{BAL}}$.

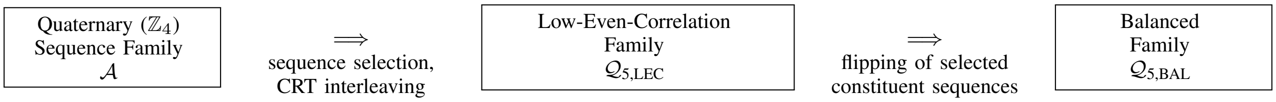

Quaternary ($\mathbb{Z}_4$) Sequence Family $\mathcal{A}$
$\Longrightarrow$
sequence selection, CRT interleaving
Low-Even-Correlation Family $\mathcal{Q}_{5,\text{LEC}}$
$\Longrightarrow$
flipping of selected constituent sequences
Balanced Family $\mathcal{Q}_{5,\text{BAL}}$

Figure 4: The two-step construction of the quaternary sequence Family $\mathcal{Q}_{5,\text{BAL}}$. Each sequence in Family $\mathcal{J}_{5,\text{LEC}}$ is obtained by carrying out CRT-based interleaving of a carefully selected subset of 5 sequences from Family $\mathcal{A}$ with $m = 2 \pmod 4$. Family $\mathcal{J}_{5,\text{BAL}}$ is derived by selectively complementing the interleaved sequences so as to achieve the same symbol balance as Family $\mathcal{A}$ without impacting the low even-correlation values.

3) Family $\mathcal{Q}_{5,BAL}$: The select-interleave-flip approach can also be used to construct the low-correlation the quaternary sequence Family $\mathcal{Q}_{5,\text{BAL}}$(see Fig. 4). The principal difference is that here we interleave 5 sequences from quaternary sequence Family $\mathcal{A}$ in place of $\mathbb{Z}_4$-linear sequence family $\mathcal{K}$. Sequence selection prior to interleaving and flipping to improve symbol balance are carried out as before.

4) Family $\mathcal{Q}_{7,BAL}$: An analogous two-step approach can be used to construct quaternary sequence Family $\mathcal{Q}_{7,\text{BAL}}$ with the difference that here we require $m = 2, 4, \pmod 6$ and we interleave 7 sequences from Family $\mathcal{A}$.

Remark 2. *The construction of all four sequence families $\mathcal{J}_{5,BAL}$, $\mathcal{J}_{7,BAL}$, $\mathcal{Q}_{5,BAL}$, $\mathcal{Q}_{7,BAL}$ share the following two features in common: the select-interleave-flip approach with balance and correlation properties that are established using the closed-form expression for an exponential sum over a Galois ring given in Theorem 2 of the appendix.*

G. The Additional Step Used to Construct Family $\mathcal{J}_{NAV}$

To generate the family $\mathcal{J}_{\text{NAV}}$ having specific period 10230, corresponding to value $m = 10$ and having the properties listed in Table III, an additional step is needed. This step is used to improve upon odd-correlation values as well as ensure the orthogonal-pairs property without impacting either the upper bound on $\Omega_{\max}$ or the symbol balance. The operations that are used in this step include refined sequence selection and flipping along with cyclically shifting constituent sequences. This is illustrated in Fig. 5.

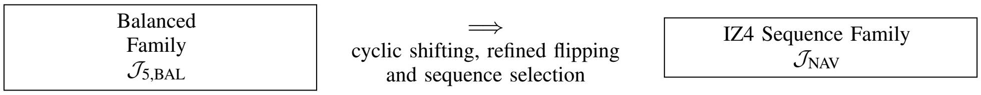

Balanced
Family
$\mathcal{J}_{5,\text{BAL}}$
$\Longrightarrow$
cyclic shifting, refined flipping
and sequence selection
IZ4 Sequence Family
$\mathcal{J}_{\text{NAV}}$

Figure 5: The additional step used to derive Family $\mathcal{J}_{\text{NAV}}$ having specific period 10230, from sequence Family $\mathcal{J}_{5,\text{BAL}}$. This family is derived using a combination of cyclic shifts, refined sequence selection and flipping so as to lower odd-correlation values and permit the creation of orthogonal pairs, while preserving the even-correlation and symbol-balance properties of Family $\mathcal{J}_{5,\text{BAL}}$.

H. *Family Size*

Since the $\mathbb{Z}_4$-linear family $\mathcal{K}$ contains 2^m sequences, and each sequence in each of the Families $\mathcal{J}_{5,\text{LEC}}$, $\mathcal{J}_{5,\text{BAL}}$and $\mathcal{J}_{\text{NAV}}$ is obtained by interleaving a set of 5 $\mathbb{Z}_4$-linear sequences, one might imagine that each of these families would have size $\lfloor \frac{2^m}{5} \rfloor$. However it turns out that the requirement of symbol balance to within 2 reduces this to $2\lfloor \frac{2^{m-1}}{6} \rfloor$. For the case $m = 10$ this gives us a family size of 170. As noted in [31] (see column 3, lines 37-57), the GNSS scenario differs from that of cellular Code-Division Multiple Access (CDMA). While cellular CDMA calls for a large number of spreading sequences to cater to a large number of potential users, in contrast, in a GNSS, the spreading codes need only support the number of envisaged satellites, pseudolites and satellite-based augmentation systems. For this reason, while there are potentially 5111 distinct Weil sequences of period 10223 that can be used to generate spreading codes having period 10230 through padding, only a subset of size 420 were reserved for operation by GPS in their Interface Control Document [32]. Similarly, while there are potentially 5121 distinct Weil sequences of period 10243 that can be used to generate spreading codes having period 10230 through truncation, only a subset of size 126 were reserved for operation by BDS in their Interface Control Document [24].

III. The Family $\mathcal{K}$ of $\mathbb{Z}_4$-Linear Sequences

We briefly review properties of the $\mathbb{Z}_4$-Linear sequence family $\mathcal{K}$ and present them in a form that will be helpful in our derivation of the properties of the sequence families $\mathcal{J}_{5,\text{LEC}}$, $\mathcal{J}_{5,\text{BAL}}$ and $\mathcal{J}_{\text{NAV}}$. We adopt the notation contained in the Appendix A on Galois rings. Specifically, $f(x)$ will denote a primitive polynomial over $\mathbb{F}_2$ of degree $m \geq 1$ and $F(x)$ will denote the basic irreducible polynomial over $\mathbb{Z}_4$ given by $F(x^2) = (-1)^m f(x)\, f(-x)$. The Galois Ring (GR) $\mathbb{R}_{4^m}$ is given by $\mathbb{R}_{4^m} = \mathbb{Z}_4[x]/(F(x)) \cong \mathbb{Z}_4[\beta]$, where β is a zero of $F(x)$, i.e., satisfies $F(\beta) = 0$. The map $\mu(\cdot)$ is the modulo-2 reduction map that maps $\mathbb{R}_{4^m}$ to the finite field $\mathbb{F}_{2^m}$, $F(x)$ to $f(x)$ and β to the primitive element α of the finite field $\mathbb{F}_{2^m}$. Thus

$$\mu(F(x)) \;=\; f(x), \qquad \mu(\beta) \;=\; \alpha.$$

We restrict our attention throughout this paper to the case m even, $m \geq 2$, and set $m = 2k$. Consider the binary $\mathbb{Z}_4$-linear sequence $\{K(x, y, t)\}$ defined by

$$K(x, y, t) \quad := \quad \text{MSB}\left\{3^t \left[x + T([1 + 2y]\beta^t)\right]\right\}, \; t \in [2n], \tag{15}$$

where $x \in \mathbb{Z}_4$, $y \in \mathcal{T}_m \subseteq \mathbb{R}_{4^m}$, where $\mathcal{T}_m$ is the set of Teichmuller representatives

$$\mathcal{T}_m = \{0\} \cup \{1, \beta, \beta^2, \cdots, \beta^{n-1}\}.$$

It can be verified that $K(x, y, t)$ has period $2n = 2(2^m - 1)$. There is a natural isomorphism between the subset $2\mathcal{T}_m \subseteq \mathbb{R}_{4^m}$ and the finite field $\mathbb{F}_{2^m}$. By identifying elements of the subset $2\mathcal{T}_m \subseteq \mathbb{R}_{4^m}$ with elements in $\mathbb{F}_{2^m}$, we will regard y as an element of $\mathbb{F}_{2^m}$. In all of our discussion, β will remain a fixed element of order n in $\mathbb{R}_{4^m}$. Thus each sequence $K(x, y, t)$ is indexed by the pair (x, y) of parameters with $x \in \mathbb{Z}_4$ and $y \in \mathbb{F}_{2^m}$.

A. *Related Sequences*

Let

$$Q(x, y, t) \quad := \quad x + T([1 + 2y]\beta^t), \; x \in \mathbb{Z}_4, \; y \in \mathcal{T}_m \subseteq \mathbb{R}_{4^m}, \quad t \in [n]. \tag{16}$$

Then we can write

$$K(x, y, t) \quad = \quad \text{MSB}\left\{3^t Q(x, y, t)\right\}, \; t \in [2n]. \tag{17}$$

Thus the binary sequence $\{K(x,y,t)\}$ is obtained by applying the MSB-Gray map (see (13)) to the quaternary sequence $\{Q(x,y,t)\}$. Let $u(x,y,t)$ and $v(x,y,t)$ denote the LSB and MSB components in the binary expansion of $Q(x,y,t)$, i.e.,

$$Q(x,y,t) \;=\; u(x,y,t)+2v(x,y,t), \;\text{ where } u(x,y,t),v(x,y,t)\in\{0,1\}, \tag{18}$$

and let $w(x,y,t)$ denote the sum component:

$$w(x,y,t) \;:=\; u(x,y,t)+v(x,y,t) \pmod 2. \tag{19}$$

We then have the following alternate description of the sequence $\{K(x,y,t)\}$:

$$K(x,y,t) \;=\; \text{MSB}\left(3^t[u(x,y,t)+2v(x,y,t)]\right) \;=\; \begin{cases} v(x,y,t), & t \text{ even}, \; t\in[2n], \\ w(x,y,t), & t \text{ odd}, \; t\in[2n]. \end{cases} \tag{20}$$

The Gray map $\mathbb{Z}_4 \to \big(\mathbb{Z}_2\times\mathbb{Z}_2\big)$ is given by

$$\mathcal{G}(s) \;:=\; (s_1,s_2),$$

where $s_0,s_1\in\{0,1\}$ are the LSB and MSB components respectively, of the quaternary symbol $s=s_0+2s_1\in\mathbb{Z}_4$, and where $s_2=s_0+s_1 \pmod 2$. From this, the reason for the MSB-Gray map terminology becomes clear since the map

$$Q(x,y,t) \;=\; u(x,y,t)+2v(x,y,t) \;\to\; (v(x,y,t),w(x,y,t)), \tag{21}$$

is precisely the Gray map. Thus we have that for t even, the pair,

$$\big(K(x,y,t),\; K(x,y,t+n)\big) \;=\; (v(x,y,t),w(x,y,t)),$$

is the image under the Gray map of the quaternary symbol $Q(x,y,t)$.

B. $\mathbb{Z}_4$-Linear Family $\mathcal{K}$

In this section, we introduce a sequence family $\mathcal{K}$, derived by collecting together sequences $\{K(x,y,t)\}$ having parameters (x,y) that belong to a parameter set P that will shortly be specified. Let H be an $(m-1)$-dimensional subspace (or hyperplane) of $\mathbb{F}_{2^m}$ over $\mathbb{Z}_2$ satisfying the property that $1\notin H$. It follows that $y\in H \Rightarrow (y+1)\notin H$. Let P denote the parameter set

$$P \;=\; \{(x,y) \mid x\in\{0,1\}\subseteq\mathbb{Z}_4,\; y\in H\}.$$

Clearly P is of size 2^m. We then define the $\mathbb{Z}_4$-linear family $\mathcal{K}$ as the collection of 2^m sequences given by:

$$\mathcal{K} \;=\; \{\{K(x,y,t)\} \mid (x,y)\in P\}.$$

This sequence family is referred to in [14] as the family of Generalized Udaya-Siddiqi sequences. We also introduce the quaternary sequence family $\mathcal{Q}$, indexed by the same parameter set and given by

$$\mathcal{Q} \;=\; \left\{\{Q(x,y,t)\}_{t=0}^{n-1} \;\mid\; (x,y)\in P\right\}. \tag{22}$$

C. Hamming and Lee Weights and Distances

The Hamming weight $w_H(\underline{u})$ of a binary vector $\underline{u}\in\mathbb{Z}_2^k$ for some integer $k\geq 1$, is the number of non-zero symbols in $\underline{u}$. The Hamming distance $d_H(\underline{u}_1,\underline{u}_2)$ between a pair of vectors in $\mathbb{Z}_2^k$ is the number of symbols in which they differ. Clearly

$$d_H(\underline{u}_1,\underline{u}_2) \;=\; w_H(\underline{u}_1+\underline{u}_2).$$

The Lee weight $w_{\text{Lee}}(s)$ of a quaternary symbol $s\in\mathbb{Z}_4$, $s=s_0+2s_1$, $s_0,s_1\in\{0,1\}$, is defined by:

$$w_{\text{Lee}}(s) \;:=\; \begin{cases} 0, & s=0, \\ 1, & s=1,3, \\ 2, & s=2. \end{cases}$$

It can be verified that the following identity holds:

$$w_{\text{Lee}}(s) \;\; := \;\; 1 - \Re(\imath^s), \tag{23}$$

where $\Re(u)$ denotes the real part of a complex number u. It can be verified that

$$w_{\text{Lee}}(s) \;\; = \;\; w_H\big(\mathcal{G}(s)\big) \;\; := \;\; w_H\big(s_1\big) + w_H\big(s_2\big),$$

where $s_2 = s_0 + s_1 \pmod 2$. The Lee distance $d_{\text{Lee}}(x, y)$ of $x, y \in \mathbb{Z}_4$ is defined to be the Lee weight of $(x - y)$ computed $(\bmod\ 4)$. It can be verified that

$$d_{\text{Lee}}(x, y) \;\; := \;\; w_{\text{Lee}}(x - y) \;\; = \;\; d_H\big(\mathcal{G}(x), \mathcal{G}(y)\big). \tag{24}$$

In other words, the Gray map from $\mathbb{Z}_4$ to $(\mathbb{Z}_2 \times \mathbb{Z}_2)$, is an isometry that preserves weights and distances with the understanding that in the $\mathbb{Z}_4$ domain, the computed weights and distances are Lee weights and Lee distances while in the $(\mathbb{Z}_2 \times \mathbb{Z}_2)$ domain, the computed weights and distances correspond to Hamming weights and Hamming distances.

D. Symbol Balance and Notation

As noted earlier, the symbol balance of a periodic binary sequence $\{J(t)\}$ having period L, is the non-negative value

$$\mid \sum_{t=0}^{L-1} (-1)^{J(t)} \mid .$$

If this value is $\leq b$ for some integer b, we will then say that $\{J(t)\}$ has (symbol) balance within b. For simplicity, in the sequel, when the underlying parameter set (x, y) is either understood, or else remains fixed throughout a series of expressions, we will drop mention of the parameter set, and adopt the abbreviations appearing in Table V.

Table V: Some convenient abbreviations

Symbol	Abbreviation	Symbol	Abbreviation
$K(x, y, t)$	$K(t)$	$K(x_i, y_i, t)$	$K_i(t)$
$Q(x, y, t)$	$Q(t)$	$Q(x_i, y_i, t)$	$Q_i(t)$
$u(x, y, t)$	$u(t)$	$u(x_i, y_i, t)$	$u_i(t)$
$v(x, y, t)$	$v(t)$	$v(x_i, y_i, t)$	$v_i(t)$
$w(x, y, t)$	$w(t)$	$w(x_i, y_i, t)$	$w_i(t)$

E. Balance Properties of Sequences in $\mathcal{K}$

For $\{K(x, y, t)\} \in \mathcal{K}$ it can be verified that

$$\sum_{t=0}^{2n-1} (-1)^{K(t)} \;\; = \;\; 2n - 2 \sum_{t=0}^{2n-1} w_H\big(K(t)\big) \tag{25}$$

$$= \;\; 2 \sum_{t=0}^{n-1} \Re\{\imath^{x + T([1+2y]\beta^t)}\}, \tag{26}$$

$$= \;\; (-2)\Re\{\imath^x\} + 2\Re\left\{ \imath^x \sum_{z \in \mathcal{T}_m} \imath^{T([1+2y]z)} \right\}. \tag{27}$$

From the closed-form expression

$$\Gamma\big(\omega_1 + 2\omega_2\big) \;\; = \;\; -(2\imath)^k \imath^{-T(\omega_2/\omega_1)},$$

for the exponential sum

$$\Gamma\big(\omega_1 + 2\omega_2\big) \quad = \quad \sum_{z\in\mathcal{T}_m} \imath^{T([\omega_1+2\omega_2]z)}, \;\; \omega_i \in \mathcal{T}_m, \; i = 1,2, \; \omega_1 \neq 0,$$

appearing in Theorem 2 of the appendix, we obtain the following closed-form expression for the balance of a sequence $\{K(x,y,t)\} \in \mathcal{K}$:

$$\begin{aligned}\sum_{t=0}^{2n-1} (-1)^{K(t)} \quad &= \quad (-2)\Re\{\imath^x\} - 2\Re\{(2\imath)^k \imath^{x-T(y)}\}, && (28)\\ &= \quad (-2)\Re\{\imath^x\} - 2^{k+1}\Re\{\imath^{k+x-T(y)}\}. && (29)\end{aligned}$$

It follows that the Z_4-linear sequence $\{K(x,y,t)\}$ is balanced to within 2 symbols iff

$$k + x - T(y) \quad = \quad 1 \pmod 2.$$

IV. Closed-Form Correlation Expression for Family $\mathcal{K}$

We will continue to use the abbreviated notation $K_i(t)$ in place of $K(x_i, y_i, t)$ etc, introduced in Table V of the prior section, Section III. In this section, we will use the closed-form expression for the Galois ring exponential sum given in Theorem 2 of the appendix, to present a closed-form expression for the cross-correlation function $\phi\big(x_i, y_i, x_j, y_j, \cdot\big)$ of two sequences $\{K_i(t)\}, \; \{K_j(t)\}$, not necessarily distinct, belonging to the binary sequence Family $\mathcal{K}$ introduced in the Section III, and defined by

$$\phi\big(x_i, y_i, x_j, y_j, \tau\big) \quad := \quad \sum_{t\in[2n]} (-1)^{K_i(t+\tau)-K_j(t)}, \quad t,\tau \in [2n], \quad (x_i,y_i),(x_j,y_j) \in P, \qquad (30)$$

where the sum $(t+\tau)$ is computed modulo $2n$.

This binary correlation function will be related to a correlation involving quaternary sequences $\{Q(x,y,t)\}$ belonging to quaternary sequence family $\mathcal{Q}$ introduced in (22). The closed-formed expression itself, will be presented later in the section. We will abbreviate and write $\phi_{ij}(\tau)$ in place of $\phi\big(x_i, y_i, x_j, y_j, \tau\big)$.

A. From Binary Correlation to Hamming Distance

We begin by noting that the binary correlation can be expressed in terms of Hamming distance:

$$\begin{aligned}\phi_{ij}(\tau) \quad &:= \quad \sum_{t\in[2n]} (-1)^{K_i(t+\tau)-K_j(t)}\\ &= \quad 2n - 2d_H\Big(\{K_i(t+\tau)\}, \{K_j(t)\}\Big), && (31)\end{aligned}$$

where

$$d_H\Big(\{K_i(t+\tau)\}, \{K_j(t)\}\Big) \quad := \quad \sum_{t=0}^{2n-1} d_H\big(K_i(t+\tau), K_j(t)\big),$$

denotes the Hamming distance between the sequences $\{K_i(t+\tau)\}, \{K_j(t)\}$. Next, we note from (20) that we have the following alternate description of the $\mathbb{Z}_4$-linear sequence $\{K(t)\}$:

$$K(t) \quad \triangleq \quad \begin{cases} v(t), & t \text{ even},\\ w(t), & t \text{ odd}.\end{cases}$$

Given a time-shift parameter τ, $\tau \in [2n]$, we analogously obtain

$$K(t+\tau) \quad = \quad \begin{cases} v(t+\tau), & \text{for } (t+\tau) \;\; \text{even},\\ w(t+\tau), & \text{for } (t+\tau) \;\; \text{odd}.\end{cases}$$

As a result, we arrive at the expressions for the pair $\big(K_i(t+\tau), K_j(t)\big)$ appearing in Table VI.

Table VI: Values of the pair $\{K_i(t+\tau)\}, \{K_j(t)\}$.

	t even	t odd
τ even	$\Big(v_i(t+\tau), v_j(t)\Big)$	$\Big(w_i(t+\tau), w_j(t)\Big)$
τ odd	$\Big(w_i(t+\tau), v_j(t)\Big)$	$\Big(v_i(t+\tau), w_j(t)\Big).$

B. Relating Hamming Distance to Quaternary Correlation

Next, we express the Hamming distance between $\{K_i(t+\tau)\}$ and $\{K_j(t)\}$ in terms of an exponential sum representing the pairwise correlation function of the collection $\mathcal{Q}$ of quaternary sequences defined in (22). We separately consider the cases τ even, τ odd.

1) Case of τ even: It follows from the relations observed above between Hamming and Lee weights and distances, that when τ is even:

$$\begin{aligned}
\sum_{t=0}^{2n-1} d_H\Big(K_i(t+\tau), K_j(t)\Big) \ &= \\
\sum_{\substack{t \text{ even} \\ 0\le t\le 2n-1}} d_H\Big(v_i(t+\tau), v_j(t)\Big) \ &+ \sum_{\substack{t \text{ odd} \\ 0\le t\le 2n-1}} d_H\Big(w_i(t+\tau), w_j(t)\Big), \\
\overset{\text{(a)}}{=} \sum_{0\le t\le n-1} d_H\Big(v_i(t+\tau), v_j(t)\Big) \ &+ \sum_{0\le t\le n-1} d_H\Big(w_i(t+\tau), w_j(t)\Big), \\
&= \sum_{0\le t\le n-1} d_H\Big(\big(v_i(t+\tau), w_i(t+\tau)\big), \big(v_j(t), w_j(t)\big)\Big) \\
&= \sum_{0\le t\le n-1} d_H\Big(\mathcal{G}\big(Q_i(t+\tau)\big),\ \mathcal{G}\big(Q_j(t)\big)\Big), \\
&\overset{\text{(b)}}{=} \sum_{0\le t\le n-1} d_{\text{Lee}}\Big(Q_i(t+\tau), Q_j(t)\Big), \\
&= \sum_{0\le t\le n-1} w_{\text{Lee}}\Big(Q_i(t+\tau) - Q_j(t)\Big), \\
&\overset{(c)}{=} n - \Re\Big(\rho(x_i, y_i, x_j, y_j, \tau)\Big),
\end{aligned} \tag{32}$$

where $\rho(x_i, y_i, x_j, y_j, \tau)$ is the quaternary correlation given by

$$\rho(x_i, y_i, x_j, y_j, \tau) \ := \ \sum_{t=0}^{n-1} \imath^{Q_i(t+\tau)-Q_j(t)}, \ \tau \in [2n], \ \tau \text{ even}. \tag{33}$$

In the above, equality (a) follows because the binary sequences $\{v_i(t)\}$, $\{w_i(t)\}$ have period n, and (b) follows from the isometry of the Gray map. The last equality (c), follows from the relationship between Lee weight and real part of a quaternary exponential sum given in (23). We will abbreviate and write $\rho_{ij}(\tau)$ in place of $\rho(x_i, y_i, x_j, y_j, \tau)$ for all $(x_i, y_i), (x_j, y_j) \in P$ and $\tau \in [2n]$. Note that the RHS in (33) is only a function of $\tau \pmod n$.

2) Case of τ odd: It follows analogously, that when τ is odd:

$$\begin{aligned}
\sum_{t=0}^{2n-1} d_H\Big(K_i(t+\tau), K_j(t)\Big) \; &= \\
\sum_{\substack{t \text{ even} \\ 0\leq t\leq 2n-1}} d_H\Big(w_i(t+\tau), v_j(t)\Big) \; &+ \; \sum_{\substack{t \text{ odd} \\ 0\leq t\leq 2n-1}} d_H\Big(v_i(t+\tau), w_j(t)\Big), \\
= \sum_{0\leq t\leq n-1} d_H\Big(w_i(t+\tau), v_j(t)\Big) \; &+ \; \sum_{0\leq t\leq n-1} d_H\Big(v_i(t+\tau), w_j(t)\Big), \\
&= \sum_{0\leq t\leq n-1} d_H\Big(\big(w_i(t+\tau), v_i(t+\tau)\big), \big(v_j(t), w_j(t)\big)\Big) \\
&= \sum_{0\leq t\leq n-1} d_H\Big(\mathcal{G}\big(3Q_i(t+\tau)\big), \; \mathcal{G}\big(Q_j(t)\big)\Big), \\
&\overset{(a)}{=} \sum_{0\leq t\leq n-1} d_{\text{Lee}}\Big(3Q_i(t+\tau), Q_j(t)\Big), \\
&= \sum_{0\leq t\leq n-1} w_{\text{Lee}}\Big(3Q_i(t+\tau) - Q_j(t)\Big), \\
&\overset{(b)}{=} n - \Re\Big(\rho^{(*)}(x_i, y_i, x_j, y_j, \tau)\Big), \qquad (34)
\end{aligned}$$

where, $\rho^{(*)}(x_i, y_i, x_j, y_j, \tau)$ is the quaternary-correlation function defined by

$$\rho^{(*)}(x_i, y_i, x_j, y_j, \tau) \;\; := \;\; \sum_{t=0}^{n-1} \imath^{3Q_i(t+\tau)-Q_j(t)}, \;\; \tau \in [2n], \;\; \tau \text{ odd}. \qquad (35)$$

analogous to $\rho(x_i, y_i, x_j, y_j, \tau)$ with $\{Q_i(t+\tau)\}$ replaced by $\{3Q_i(t+\tau)\}$. In the above, equality labelled (a) follows because if

$$Q_i(t+\tau) \;\; = \;\; u_i(t+\tau) + 2v_i(t+\tau),$$

then

$$\begin{aligned}
3Q_i(t+\tau) \;\; &= \;\; u_i(t+\tau) + 2\Big(u_i(t+\tau) + v_i(t+\tau)\Big), \\
&= \;\; u_i(t+\tau) + 2w_i(t+\tau),
\end{aligned}$$

and thus replacing $Q_i(t+\tau)$ by $3Q_i(t+\tau)$, is equivalent to interchanging the MSB component, $v_i(t+\tau)$ and the sum component, $w_i(t+\tau) \; = \; \big(v_i(t+\tau) + u_i(t+\tau)\big) \pmod 2$. The equality labelled (b) follows once again, from the relationship between Lee weight and real part of a quaternary exponential sum given in (23). We will abbreviate and write $\rho_{ij}^{(*)}(\tau)$ in place of $\rho^{(*)}(x_i, y_i, x_j, y_j, \tau)$ for all $(x_i, y_i), (x_j, y_j) \in P$ and $\tau \in [2n]$.

From equations (32) and (34) above and the relation between binary correlation and Hamming distance given in (31), we obtain:

$$\phi_{ij}(\tau) \;\; = \;\; \begin{cases} 2n - 2\left(n - \Re(\rho_{ij}(\tau))\right), & \tau \text{ even}, \\ 2n - 2\left(n - \Re(\rho_{ij}^{(*)}(\tau))\right), & \tau \text{ odd}, \end{cases}$$

which simplifies to

$$\phi_{ij}(\tau) \;\; = \;\; \begin{cases} 2\Re(\rho_{ij}(\tau)), & \tau \in [2n], \tau \text{ even}, \\ 2\Re(\rho_{ij}^{(*)}(\tau)), & \tau \in [2n], \tau \text{ odd}. \end{cases} \qquad (36)$$

Thus in summary, we have in this subsection, expressed the correlation $\phi_{ij}(\tau)$ of two binary sequences $\{K_i(t)\}, \{K_j(t)\}$ belonging to $\mathcal{K}$ in terms of the quaternary correlation functions $\rho_{ij}(\tau)$, $\rho_{ij}^{(*)}(\tau)$, involving the pair of quaternary sequences $\{Q_i(t)\}, \{Q_j(t)\} \in \mathcal{Q}$ respectively, underlying the binary sequences $\{K_i(t)\}, \{K_j(t)\}$.

We next study the quaternary correlation values $\big(\rho_{ij}(\tau),\ \rho^{(*)}_{ij}(\tau)\big)$ appearing above separately for even and odd values of the time-shift parameter τ. We begin with the case of $\tau \in [2n]$, τ even, where we have

$$\begin{aligned}\rho_{ij}(\tau) &= \sum_{t=0}^{n-1} \imath^{Q(x_i,y_i,t+\tau)-Q(x_j,y_j,t)} \;=\; \imath^{(x_i-x_j)} \sum_{t=0}^{n-1} \imath^{T\left(\beta^{t+\tau}[1+2y_i]-\beta^{t}[1+2y_j]\right)}, \\ &= \imath^{(x_i-x_j)} \sum_{t=0}^{n-1} \imath^{T\left(\beta^{t}\left(\theta[1+2y_i]-[1+2y_j]\right)\right)} \;=\; \imath^{(x_i-x_j)} \left\{ -1 + \sum_{z\in\mathcal{T}_m} \imath^{T\left(z\left(\theta[1+2y_i]-[1+2y_j]\right)\right)} \right\}, \qquad (37)\end{aligned}$$

and where we have set $\theta = \beta^{\tau}$.

C. *Case $\tau = 0$*

For the case $\tau = 0$, we have $\theta = 1$ giving rise to:

$$\begin{aligned}\rho_{ij}(0) &= \imath^{(x_i-x_j)} \left\{ -1 + \sum_{z\in\mathcal{T}_m} \imath^{2T(z[y_i-y_j])} \right\} \\ &= \begin{cases} -\imath^{(x_i-x_j)}, & y_i \neq y_j, \\ n\imath^{(x_i-x_j)}, & y_i = y_j. \end{cases}\end{aligned}$$

Our interest is in the associated correlation parameter $\phi_{ij}(\tau)$, given by

$$\phi_{ij}(\tau) \;=\; \begin{cases} 2\Re(\rho_{ij}(\tau)), & \tau \text{ even} \\ 2\Re(\rho^{(*)}_{ij}(\tau)), & \tau \text{ odd.} \end{cases}$$

It follows that for $\tau = 0$, since $x_i, x_j \in \{0,1\}$, we have

$$\phi_{ij}(0) \;=\; \begin{cases} 0, & x_i \neq x_j, \\ -2, & x_i = x_j,\ y_i \neq y_j, \\ 2n, & x_i = x_j,\ y_i = y_j. \end{cases} \qquad (38)$$

D. *Case $\tau \in [2n]$, τ even, $\tau \neq 0$*

We note that $\tau \neq 0 \implies \theta \neq 1$. We have from (37) that

$$\begin{aligned}\rho_{ij}(\tau) &= \sum_{t=0}^{n-1} \imath^{Q(x_i,y_i,t+\tau)-Q(x_j,y_j,t)}, \\ &= \imath^{x_i-x_j} \left\{ -1 \;+\; \sum_{z\in\mathcal{T}_m} \imath^{T\left(z\left(\theta[1+2y_i]-[1+2y_j]\right)\right)} \right\}.\end{aligned}$$

To handle this case, we wish to bring the coefficient $\theta[1+2y_i]-[1+2y_j]$ into the general form

$$\theta[1+2y_i]-[1+2y_j] \;=\; \omega_1 + 2\omega_2, \quad \omega_1,\omega_2 \in \mathcal{T}_m.$$

This would then allow us to evaluate

$$\begin{aligned}\rho_{ij}(\tau) &= \imath^{x_i-x_j} \left\{ -1 \;+\; \sum_{z\in\mathcal{T}_m} \imath^{T\left(z[\omega_1+2\omega_2]\right)} \right\}, \\ &= \imath^{x_i-x_j} \left\{ -1 - 2^k \imath^{k-T(\omega_2/\omega_1)} \right\},\end{aligned}$$

by making use once again, of the closed-form expression

$$\Gamma\big(\omega_1+2\omega_2\big) \;=\; -2^k \imath^{k-T(\omega_2/\omega_1)},$$

for the exponential sum

$$\Gamma\big(\omega_1 + 2\omega_2\big) \;=\; \sum_{z \in \mathcal{T}_m} \imath^{T(\omega_1+2\omega_2)}, \;\; \omega_i \in \mathcal{T}_m, \;\; i = 1, 2, \;\; \omega_1 \neq 0,$$

appearing in (83) of the appendix. Towards this, we write

$$\begin{aligned} \theta[1+2y_i] - [1+2y_j] &= (\theta - 1) + 2(y_i\theta + y_j) \\ &= (\theta + 1 + 2\sqrt{\theta}) + 2(1 + \sqrt{\theta} + y_i\theta + y_j). \end{aligned}$$

We then make the change of variable

$$\begin{aligned} \theta_1 &:= (\theta + 1 + 2\sqrt{\theta}), \text{ and note that} \\ \theta_1 &= (\theta + 1) \pmod 2, \\ \sqrt{\theta_1} &= 1 + \sqrt{\theta} \pmod 2. \end{aligned}$$

We have used the fact here that in a field $\mathbb{F}_m$ of characteristic 2 and size 2^m, every element θ has a unique square root $\sqrt{\theta}$ given by $\sqrt{\theta} = \theta^{2^{m-1}}$. This leads to

$$[1+2y_i]\theta - [1+2y_j] \;=\; \theta_1 + 2\bigg(\sqrt{\theta_1} + y_i\theta_1 + (y_i + y_j)\bigg)$$

so that we have

$$\omega_1 \;=\; \theta_1, \quad\; \omega_2 \;=\; \psi,$$

where ψ is the unique element in $\mathcal{T}_m$ such that

$$\psi \;=\; \sqrt{\theta_1} + y_i\theta_1 + (y_i + y_j) \pmod 2.$$

It follows that the ratio

$$\frac{\omega_2}{\omega_1} \;=\; \sqrt{\theta_1^{-1}} + y_i + (y_i + y_j)\theta_1^{-1} \pmod 2.$$

Making the further change of variable $\mu^2 \triangleq \theta_1^{-1}$, we get

$$\frac{\omega_2}{\omega_1} \;=\; \mu + y_i + (y_i + y_j)\mu^2.$$

Note that μ and τ are related by:

$$\theta = \beta^\tau, \;\; \theta_1 = (\theta + 1) \pmod 2, \;\; \mu^2 = \theta_1^{-1} \pmod 2 \;\; \Rightarrow \mu = \sqrt{\frac{1}{1+\alpha^\tau}} \pmod 2,$$

since $\alpha^\tau = \beta^\tau \pmod 2$. This is well defined since we are dealing with the case $\tau \neq 0$. Thus the crosscorrelation $\phi_{ij}(\tau)$ is given by

$$\phi_{ij}(\tau) \;=\; 2\Re\left\{\imath^{x_i - x_j}\left[-1 - 2^k \imath^{k - T(e(y_i, y_j, \tau))}\right]\right\},$$

where $e(y_i, y_j, \tau)$ is the unique element belonging to the Teichmueller set $\mathcal{T}_m$ such that

$$e(y_i, y_j, \tau) \;:=\; \mu + y_i + (y_i + y_j)\mu^2 \pmod 2,$$

and where

$$\mu \;:=\; \sqrt{\frac{1}{1+\alpha^\tau}} \pmod 2. \tag{39}$$

1) Case $\tau \in [2n]$, τ Odd: The underlying quaternary correlation in the case of odd τ is given by

$$\begin{aligned}
\rho_{ij}^{(*)}(\tau) &:= \sum_{t=0}^{N-1} \imath^{3Q(x_i,y_i,t+\tau)-Q(x_j,y_j,t)}, \\
&= \imath^{3x_i-x_j}\left\{-1 \;+\; \sum_{z\in\mathcal{T}_m} \imath^{T\left(z\left(3\theta[1+2y_i]-[1+2y_j]\right)\right)}\right\}, \\
&= \imath^{3x_i-x_j}\left\{-1 \;+\; \sum_{z\in\mathcal{T}_m} \imath^{T\left(z\left(\theta[1+2(y_i+1)]-[1+2y_j]\right)\right)}\right\}.
\end{aligned}$$

Thus the difference between the case of τ even and τ odd, apart from the difference in the multiplicative factor $\imath^{x_i-x_j}$ versus $\imath^{3x_i-x_j}$ is that we need to replace y_i by $(1+y_i)$. Thus the crosscorrelation in the case τ odd is given by

$$\phi_{ij}(\tau) \;=\; 2\Re\left\{\imath^{3x_i-x_j}\left[-1-2^k\imath^{k-T(f(y_i,y_j,\tau))}\right]\right\},$$

where $f(y_i,y_j,\tau)$ is the unique element belonging to the Teichmueller set $\mathcal{T}_m$ such that

$$\begin{aligned}
f(y_i,y_j,\tau) &:= \mu+(1+y_i)+(\;(y_i+1)\;+y_j)\mu^2 \pmod 2, \\
&= (1+\mu+\mu^2)+y_i+(y_i+y_j)\mu^2 \pmod 2,
\end{aligned}$$

where once again, μ is related to the cyclic shift parameter τ by (39).

E. Summarizing Closed-Form Expressions for Family $\mathcal{K}$ Correlations

1) For $\tau = 0$, we have

$$\phi_{ij}(0) \;=\; \begin{cases} 0, & x_i \neq x_j, \\ -2, & x_i = x_j,\; y_i \neq y_j, \\ 2n, & x_i = x_j,\; y_i = y_j. \end{cases} \tag{40}$$

2) For $\tau \in [2n]$, τ even, $\tau \neq 0$, we have

$$\begin{aligned}
\phi_{ij}(\tau) &= 2\Re\left\{\imath^{x_i-x_j}\left[-1-2^k\imath^{k-T(e(y_i,y_j,\tau))}\right]\right\}, \\
&= (-2)\Re\left\{\imath^{x_i-x_j}\right\} \;+\; (-2^{k+1})\Re\left\{\imath^{x_i-x_j+k-T\left(e(y_i,y_j,\tau)\right)}\right\},
\end{aligned} \tag{41}$$

where $e(y_i,y_j,\tau)$ is the unique element belonging to the Teichmueller set $\mathcal{T}_m$ such that

$$e(y_i,y_j,\tau) \;=\; \mu+y_i+(y_i+y_j)\mu^2 \pmod 2, \tag{42}$$

and where μ is given

$$\mu \;=\; \sqrt{\frac{1}{1+\alpha^\tau}} \pmod 2. \tag{43}$$

3) For $\tau \in [2n]$, τ odd, we have

$$\begin{aligned}
\phi_{ij}(\tau) &= 2\Re\left\{\imath^{3x_i-x_j}\left[-1-2^k\imath^{k-T(f(y_i,y_j,\tau))}\right]\right\}, \\
&= (-2)\Re\left\{\imath^{3x_i-x_j}\right\} \;+\; (-2^{k+1})\Re\left\{\imath^{3x_i-x_j+k-T\left(f(y_i,y_j,\tau)\right)}\right\},
\end{aligned} \tag{44}$$

where $f(y_i,y_j,\tau)$ is the unique element belonging to the Teichmueller set $\mathcal{T}_m$ such that

$$f(y_i,y_j,\tau) \;=\; (1+\mu+\mu^2)+y_i+(y_i+y_j)\mu^2 \pmod 2, \tag{45}$$

and where μ is again given by (43).

F. Correlation spectrum of Family $\mathcal{K}$

By correlation spectrum of Family $\mathcal{K}$, we will mean the set of correlation values:

$$\{\phi(x_i, y_i, x_j, y_j, \tau) \mid (x_i, y_i) \in P,\ (x_j, y_j) \in P, \text{either } i \neq j \text{ or } \tau \neq 0\}$$

From equations (40), (41) and (44) above, we see that Family $\mathcal{K}$ has correlation spectrum that is a subset of the set

$$\{\pm 2, 0\} \ + \ \{0, \pm 2^{k+1}\} \ = \ \{0,\ \pm 2,\ \pm 2^{k+1},\ \pm 2 \pm 2^{k+1}\}.$$

Let us define:

$$\begin{aligned}
\phi_{a,\max} &:= \max_{0 \leq i \leq 1023} \{\ |\phi_{ii}(\tau)| \ \mid 1 \leq \tau \leq 2n-1\},\\
\phi_{c,\max} &:= \max_{\substack{0 \leq i,j \leq 1023\\ i \neq j}} \{\ |\phi_{i,j}, \tau)| \ \mid 0 \leq \tau \leq 2n-1\},\\
\phi_{\max} &= \max\{\phi_{a,\max},\ \phi_{c,\max}\}.
\end{aligned}$$

Thus we have that Family $\mathcal{K}$ has even-correlation parameters satisfying

$$\phi_{a,\max} \leq (2 + 2^{k+1}), \qquad \phi_{c,\max} \leq (2 + 2^{k+1}), \qquad \phi_{\max} \leq (2 + 2^{k+1}).$$

V. The Low-Even-Correlation Family $\mathcal{J}_{5,\text{LEC}}$

Each sequence in $\mathcal{J}_{5,\text{LEC}}$ is obtained by interleaving a set of 5 distinct $\mathbb{Z}_4$-linear sequences drawn from the family $\mathcal{K}$ having period $2(2^m - 1)$ for $m = 2 \pmod 4$. Each sequence in $\mathcal{K}$ is employed in the construction of at most one sequence in $\mathcal{J}_{5,\text{LEC}}$. Thus the set of interleaved sequences corresponding to two distinct sequences in $\mathcal{J}_{5,\text{LEC}}$ are disjoint. The method of interleaving employed is based on the Chinese Remainder Theorem (CRT). As sequences in Family $\mathcal{K}$ have period $2(2^m - 1)$ and as the integers $2(2^m - 1)$ and 5 are relatively prime for $m = 2 \pmod 4$, each sequence in $\mathcal{J}_{5,\text{LEC}}$ will turn out to have period $L = (5 \times 2(2^m - 1)) = 10(2^m - 1)$.

A. Family Size

There are in all, a total of 2^m Z_4-linear sequences

$$\{\ \{K(x, y, t)\} \ \mid x \in \{0, 1\},\ y \in H\},$$

of period $2n = 2(2^m - 1)$ in the family $\mathcal{K}$, which would suggest that one might be able to construct an IZ4 family of size $\lfloor \frac{2^m}{5} \rfloor$ IZ4 sequences. However, under the construction approach adopted here, the need for achieving symbol balance to within 2, forces a reduction in family size from $\lfloor \frac{2^m}{5} \rfloor$ to $M = 2\lfloor \frac{2^{m-1}}{6} \rfloor$. This is explained in greater detail in Remark 6 of Section VIII. The construction of Family $\mathcal{J}_{5,\text{LEC}}$ presented here will be such that all of the 5 sequences from $\mathcal{K}$ employed in the construction of a single sequence in Family $\mathcal{J}_{5,\text{LEC}}$ will share the same value of parameter x, either $x = 0$ or $x = 1$. Thus it is meaningful to categorize a sequence $\{J(t)\}$ belonging to $\mathcal{J}_{5,\text{LEC}}$ as being a sequence associated to parameter value $x = 0$ or $x = 1$. The Family $\mathcal{J}_{5,\text{LEC}}$ will be constructed in such a manner that $M/2$ sequences in $\mathcal{J}_{5,\text{LEC}}$ are associated to parameter $x = 0$ and an equal number, $M/2$, to parameter $x = 1$. Some subspaces and matrices that feature in the construction are identified below.

B. Admissible Subspaces

Definition 4 (Admissible Pair Subspaces (H, W))**.** *Let H be an $(m-1)$-dimensional subspace over $\mathbb{Z}_2$ of $\mathbb{F}_{2^m}$, having the property that $1 \notin H$. Thus $y \in H \Rightarrow (y + 1) \notin H$. As H has co-dimension 1, H will sometimes be referred to as a hyperplane. Let W be a two-dimensional subspace of H over $\mathbb{Z}_2$ having the form*

$$W \ := \ \langle \gamma_0, \gamma_1 \rangle \ = \ \{0, \gamma_0, \gamma_1, \gamma_0 + \gamma_1\},$$

where the elements γ_0, γ_1 belong to H and satisfy the trace conditions

$$tr(\gamma_0) = 1, \qquad tr(\gamma_1) = 0. \tag{46}$$

Any pair of subspaces (H, W) satisfying the above conditions will be termed as an admissible pair of subspaces. The subspaces H, W will also be individually referred to as admissible subspaces.

C. Admissible Parameter Matrix Y

Let (H, W) be an admissible pair of subspaces of the field $\mathbb{F}_{2^m}$. Thus W is of the form $W = \langle \gamma_0, \gamma_1 \rangle$, with $\text{tr}(\gamma_0) = 1$ and $\text{tr}(\gamma) = 0$. Under modulo-2 addition, W is a subgroup of H and H can be partitioned into the disjoint union of $2^{m-1}/4 = 2^{m-3}$ cosets of W. Let $\{g_a\}_{a=0}^{2^{m-3}-1}$ and $\{h_a\}_{a=0}^{2^{m-3}-1}$ be two sets of coset representatives for the cosets of W in H. The two sets could be disjoint, identical, or overlap partially.

An $(M \times 5)$ parameter-matrix $Y(H, W)$ will now be constructed, that is a function of the pair (H, W), and whose entries will be specified in two steps. For brevity, $Y(H, W)$ will simply be denoted by Y. For $a \in [M]$, and $j \in [5]$, the symbol $y_j^{(a)}$ will denote the element in the ath row and jth column of Y. We define for $a \in [M/2]$,

$$\begin{aligned} \big(y_1^{(a)},\ y_2^{(a)},\ y_3^{(a)},\ y_4^{(a)}\big) &:= \big(g_a,\ g_a + \gamma_0,\ g_a + \gamma_0 + \gamma_1,\ g_a + \gamma_1\big), && (47) \\ \big(y_1^{(a+M/2)},\ y_2^{(a+M/2)},\ y_3^{(a+M/2)},\ y_4^{(a+M/2)}\big) &:= \big(h_a,\ h_a + \gamma_0,\ h_a + \gamma_0 + \gamma_1,\ h_a + \gamma_1\big). && (48) \end{aligned}$$

Note that the right hand sides represent a specific ordering of elements in the cosets $g_a + W$, $h_a + W$ respectively. Note also that for all $a \in [M]$ we can write:

$$\big(y_1^{(a)},\ y_2^{(a)},\ y_3^{(a)},\ y_4^{(a)}\big) \;=\; \big(y_1^{(a)},\ \ y_1^{(a)} + \gamma_0,\ \ y_1^{(a)} + \gamma_0 + \gamma_1,\ \ y_1^{(a)} + \gamma_1\big) \;:=\; y_1^{(a)} + W. \qquad (49)$$

It remains to define the entries of the matrix Y corresponding to the first column, i.e., the entries $\{y_0^{(a)} \mid a \in [M]\}$. It follows from (46), (49) and linearity of the trace function that each coset

$$y_1^{(a)} + W \;=\; \big(y_1^{(a)},\ \ y_1^{(a)} + \gamma_0,\ \ y_1^{(a)} + \gamma_0 + \gamma_1,\ \ y_1^{(a)} + \gamma_1\big),\quad a \in [M],$$

contains two elements having trace-value zero and two elements having trace-value one. Recall that the 2^{m-3} cosets of W partition H. We define the coset-union sets

$$\begin{aligned} A_g &= \bigcup_{a=M/2}^{(2^{m-3}-1)} (g_a + W), \\ A_h &= \bigcup_{a=M/2}^{(2^{m-3}-1)} (h_a + W). \end{aligned}$$

Clearly the sets A_g and A_h are each of size $\big(4 \times (2^{m-3} - M/2)\big) = (2^{m-1} - 2M)$ and hence contain $(2^{m-2} - M)$ elements having trace value zero and the same number of elements having trace value one.

Let T_0 be a set of size $M/2$ obtained by selecting an arbitrary subset of $M/2$ (out of a total possible of $(2^{m-2} - M)$) elements in the set A_g having trace value $= (k+1) \pmod 2$. This is possible as

$$2^{m-2} - M \;=\; 2^{m-2} - 2\lfloor \frac{2^{m-1}}{6} \rfloor \;\geq\; M/2 \;=\; \lfloor \frac{2^{m-1}}{6} \rfloor.$$

Thus T_0 satisfies the conditions,

$$\begin{aligned} T_0 &\subseteq \{\theta \in A_g \mid \text{tr}(\theta) = (k+1) \pmod 2\}, \\ |T_0| &= M/2, && (50) \end{aligned}$$

(see Fig. 6). Next, we order the $M/2$ elements in the set T_0 and use the symbol $y_0^{(a)}$ to denote the ath element, $a \in [M/2]$ of T_0.

Correspondingly, let T_1 be a set of size $M/2$ obtained by selecting an arbitrary subset of $M/2$ (out of a total possible of $(2^{m-2} - M)$ elements in the set A_h having trace value $= k \pmod 2$, i.e.,

$$\begin{aligned} T_1 &\subseteq \{\theta \in A_h \mid \text{tr}(\theta) = k \pmod 2\} \\ |T_1| &= M/2. && (51) \end{aligned}$$

We order the $M/2$ elements in the set T_1 and use the symbol $y_0^{(a+M/2)}$ to denote the ath element, $a \in [M/2]$ of T_1. With this, we have defined all the entries $\{y_0^{(a)} \mid a \in [M]\}$, corresponding to the first column of the parameter matrix Y. Further, these entries satisfy

$$\text{tr}(y_0^{(a)}) \;=\; \begin{cases} (k+1) \pmod 2, & a \in [M/2], \\ k \pmod 2, & M/2 \leq a \leq (M-1). \end{cases} \qquad (52)$$

$g_0 + W$	$\{u \mid \text{tr}(u) = (k+1) \pmod 2\} \supseteq T_0$
$g_1 + W$	
$\vdots$	
$\vdots$	$\{u \mid \text{tr}(u) = k \pmod 2\}$
$g_{M/2-2} + W$	
$g_{M/2-1} + W$	

$h_0 + W$	$\{u \mid \text{tr}(u) = (k+1) \pmod 2\}$
$h_1 + W$	
$\vdots$	
$h_0 + W$	$\{u \mid \text{tr}(u) = k \pmod 2\} \supseteq T_1$
$h_{M/2-2} + W$	
$h_{M/2-1} + W$	

Figure 6: Illustrating the sets $\{\{g_a + W\}, \{h_a + W\}, T_0, T_1\}$ that appear in the construction of Family $\mathcal{J}_{5,\text{LEC}}$. The table (a) on the left shows the partitioning of the hyperplane H for the case $0 \leq a \leq (M/2-1)$, into three segments (i) $M/2$ cosets of W of the form $g_a + W$, (ii) the set of $(2^{m-2} - M)$ elements in the set A_g having trace-value $= (k+1) \pmod 2$, and (iii) the set of $(2^{m-2} - M)$ elements in set A_g having trace-value $= k \pmod 2$. The set T_0 is a subset of the set having size $M/2$ and trace value $(k+1) \pmod 2$. The table (b) on the right shows the analogous partitioning of the hyperplane H for the case $M/2 \leq a \leq (M-1)$. The set T_1 is in this case, a subset of the trace $= k \pmod 2$ elements of size $M/2$ of the set A_h.

This completes our specification of the parameter matrix Y. We will refer to any matrix Y constructed by following precisely these steps as an admissible parameter matrix. We will refer to the triple $\big(H, W, Y\big)$ as an admissible triple.

D. The Sum Matrix

Let $\big(H, W, Y\big)$ be an admissible triple as defined in Subsection V-C above. A matrix that will be helpful in establishing the even-correlation properties of Family $\mathcal{J}_{5,\text{LEC}}$ will now be identified. Let $a \in [M], b \in [M]$ be fixed and let S be the (4×4) matrix whose (j,k)th entry is the sum given by

$$S(j,k) \quad := \quad y_j^{(b)} + y_k^{(a)}, \quad j,k \in \{1,2,3,4\}.$$

The entries of S are displayed in Table VII.

Table VII: The sum-matrix S whose (j,k)th entry is given by $y_j^{(b)} + y_k^{(a)}$. The element Δ appearing in the table, denotes the sum $\Delta := y_1^{(a)} + y_1^{(b)}$.

Trace values of $\{y_i^{(a)} \mid i = 1,2,3,4\}$	$\text{tr}(y_1^{(a)})$	$\text{tr}(y_1^{(a)}) + 1$	$\text{tr}(y_1^{(a)}) + 1$	$\text{tr}(y_1^{(a)})$
$y_i^{(b)} \ / \ y_i^{(a)}$	$y_1^{(a)}$	$y_2^{(a)} = y_1^{(a)} + \gamma_0$	$y_3^{(a)} = y_1^{(a)} + \gamma_0 + \gamma_1$	$y_4^{(a)} = y_1^{(a)} + \gamma_1$
$y_1^{(b)}$	Δ	$\Delta + \gamma_0$	$\boxed{\Delta + \gamma_0 + \gamma_1}$	$\Delta + \gamma_1$
$y_2^{(b)} = y_1^{(b)} + \gamma_0$	$\Delta + \gamma_0$	Δ	$\Delta + \gamma_1$	$\boxed{\Delta + \gamma_0 + \gamma_1}$
$y_3^{(b)} = y_1^{(b)} + \gamma_0 + \gamma_1$	$\Delta + \gamma_0 + \gamma_1$	$\Delta + \gamma_1$	Δ	$\Delta + \gamma_0$
$y_4^{(b)} = y_1^{(b)} + \gamma_1$	$\boxed{\Delta + \gamma_1}$	$\Delta + \gamma_0 + \gamma_1$	$\Delta + \gamma_0$	Δ

Property 1 (Sum-Constant-Trace-Different Property)**.** *Let $\oplus$ denote addition modulo* 5*. For any $\nu \in [5]$, the multiset*

$$\left\{ y^{(a)}_{i \oplus \nu} + y^{(b)}_{i} \mid \ i \in \{1,2,3,4\}, \quad i \oplus \nu \in \{1,2,3,4\} \right\},$$

contains at least two identical sums

$$y^{(a)}_{i_1 \oplus \nu} + y^{(b)}_{i_1} \quad = \quad y^{(a)}_{i_2 \oplus \nu} + y^{(b)}_{i_2},$$

with $i_1 \in \{1,2,3,4\}$, $i_2 \in \{1,2,3,4\}$, $i_1 \neq i_2$, such that

$$tr(y^{(a)}_{i_1 \oplus \nu}) \quad \neq \quad tr(y^{(a)}_{i_2 \oplus \nu}).$$

Proof. This property can be verified simply by examining the entries of Table VII and verifying that for each value of ν, $\nu = 0,1,2,3,4$, the property holds. The boxed entries show that the property holds for the case $\nu = 2$. □

We will refer to Property 1 as the sum-constant-trace-different property of the admissible subspace pair (H, W).

E. Construction of the Low Even-Correlation Family $\mathcal{J}_{5,LEC}$

A formal description of the construction of Family $\mathcal{J}_{5,\text{LEC}}$ is provided below.

Construction 1 (Family $\mathcal{J}_{5,\text{LEC}}$)**.** *Let β be an element of $\mathbb{R}_{4^m}$ having order $n = 2^m - 1$. Let (H, W) be an admissible pair of subspaces as described in Section V-B and let $Y(H, W)$ be an admissible parameter matrix as defined in Section V-C. Let $y^{(a)}_j$ denote the entry in the ath row, $a \in [M]$, and jth column, $j \in [5]$, of $Y(H, W)$ where $M = 2\lfloor \frac{2^m-1}{6} \rfloor$. For $x \in \{0,1\} \subseteq \mathbb{Z}_4$, $y \in H$, we define the sequence*

$$K(x,y,t) \quad := \quad MSB\left\{3^t \left[x + T([1+2y]\beta^t)\right]\right\}, \ t \in [2n].$$

Then the low-even-correlation family $\mathcal{J}_{5,LEC}$, is a family of M binary sequences, each having period $L = 10(2^m - 1)$. The a-th sequence $\{J^{(a)}(t)\}$, $a \in [M]$, in the family is obtained by CRT-based interleaving of the 5 *$\mathbb{Z}_4$-linear sequences $\{K(x^{(a)},\ y^{(a)}_j,\ \ell)\}_{j=0}^{4}$, where*

$$x^{(a)} \quad = \quad \begin{cases} 0, & a \in [M/2], \\ 1, & M/2 \leq a \leq (M-1). \end{cases} \tag{53}$$

Thus the a-th sequence $\{J^{(a)}(t)\}$, $a \in [M]$, in Family $\mathcal{J}_{5,LEC}$, is given by

$$J^{(a)}(t) \quad = \quad K(x^{(a)},\ y^{(a)}_j,\ \ell), \quad t \in [L], \tag{54}$$

where $j = t \pmod 5$ and $\ell = t \pmod{2n}$.

Remark 3. *We summarize for future reference, information concerning the parameters $\left(x^{(a)},\ (y^{(a)}_j, j \in [5])\right)$ of sequences in Family $\mathcal{J}_{5,LEC}$.*

(a) From equations (52) *and* (53) *we see that for all sequences in the family, we have*

$$x^{(a)} \quad = \quad \begin{cases} 0, & a \in [M/2], \\ 1, & M/2 \leq a \leq (M-1), \end{cases} \tag{55}$$

and

$$tr(y^{(a)}_0) \quad = \quad x^{(a)} + k + 1, \textit{ for all } a \in [M]. \tag{56}$$

(b) From (49)*, we see that the parameters $\left(y^{(a)}_j,\ j \in [5]\right)$ satisfy:*

$$\left(y^{(a)}_j,\ j \in [5]\right) \quad = \quad \left(y^{(a)}_0, y^{(a)}_1, y^{(a)}_1 + \gamma_0, y^{(a)}_1 + \gamma_0 + \gamma_1, y^{(a)}_1 + \gamma_1 .\right), \quad \forall\ a \in [M]. \tag{57}$$

VI. Closed-Form Expression for the Correlation of Sequences in Family $\mathcal{J}_{5,\text{LEC}}$

A closed-form expression for the even correlation of a pair of sequences drawn from the Family $\mathcal{J}_{5,\text{LEC}}$ will be provided in this section. The a-th sequence $\{J^{(a)}(t)\}$ in $\mathcal{J}_{5,\text{LEC}}$ is obtained as noted in the prior section, by interleaving 5 $\mathbb{Z}_4$-linear sequences. Let the 5 sequences in $\mathcal{K}$ that are interleaved be denoted by $\Big\{\{K\big(x^{(a)}, y_j^{(a)}, t\big)\},\ j \in [5]\Big\}$, with $\big(x_j^{(a)}, y_j^{(a)}\big) \in P$, all $j \in [5]$. Recall that

$$K\big(x^{(a)}, y_j^{(a)}, t\big) \;=\; \text{MSB}\Bigg(3^t Q\big(x^{(a)}, y_j^{(a)}, t\big)\Bigg),$$

where

$$Q\big(x^{(a)}, y_j^{(a)}, t\big) \;=\; x^{(a)} \;+\; T\big([1+2y_j^{(a)}]\beta^t\big),$$

where β is an element of $\mathbb{R}_{4^m}$ having order $n = 2^m - 1$. The following abbreviation will be adopted:

$$K_j^{(a)}(\ell) \;:=\; K\big(x^{(a)},\ y_j^{(a)},\ \ell\big),\ \ \forall a \in [M],\ \ell \in [2n], j \in [5]. \tag{58}$$

Consider the correlation

$$\Omega(a,b,\tau) \;:=\; \sum_{t=0}^{L-1} (-1)^{J^{(a)}(t+\tau) - J^{(b)}(t)},$$

where $L := 10(2^m - 1)$, of a pair $\{J^{(a)}(t)\}$, $\{J^{(b)}(t)\}$ of sequences in $\mathcal{J}_{5,\text{LEC}}$, not necessarily distinct. Let λ, ν be defined by

$$\lambda \;=\; \tau \pmod{2n}, \qquad \nu \;=\; \tau \pmod{5}.$$

By the Chinese Remainder Theorem, the correlation of the sequences $\{J^{(a)}(t)\}$, $\{J^{(b)}(t)\}$ can be expressed in terms of correlations involving the component Z_4-linear sequences

$$\Big\{\{K_j^{(a)}(t)\}, \{K_j^{(b)}(t)\} \mid j \in [5]\Big\}$$

as shown below:

$$\begin{aligned}
\Omega(a,b,\tau) &= \sum_{t=0}^{N-1} (-1)^{J^{(a)}(t+\tau) - J^{(b)}(t)} \\
&= \sum_{j=0}^{4} \sum_{\ell=0}^{2n-1} (-1)^{K_{j\oplus\nu}^{(a)}(\ell+\lambda) - K_j^{(b)}(\ell)} \\
&= \sum_{j=0}^{4} \phi\Bigg(x^{(a)}, y_{j\oplus\nu}^{(a)}, x^{(b)}, y_j^{(b)},\ \lambda\Bigg).
\end{aligned} \tag{59}$$

Remark 4 (Advantage of CRT-based interleaving)**.** *As can be seen from* (59) *above, the correlation* $\Omega(a,b,\tau)$ *of a pair of sequences in Family* $\mathcal{J}_{5,\text{LEC}}$ *and corresponding to cyclic shift* τ*, is the sum of the correlations* $\phi\big(x^{(a)}, y_{j\oplus\nu}^{(a)}, x^{(b)}, y_j^{(b)},\ \lambda\big)$ *of* 5 *pairs*

$$\Bigg\{\Bigg(\{K_{j\oplus\nu}^{(a)}(\ell)\},\ \{K_j^{(b)}(\ell)\}\Bigg) \mid j \in [5]\Bigg\},$$

of sequences drawn from Family $\mathcal{K}$*, where in each case, the cyclic shift between sequences within each pair is the same and given by*

$$\lambda \;=\; \tau \pmod{2n}.$$

The fact that the cyclic shift λ *is the same independent of the index* j*, is a consequence of CRT-based interleaving. This significantly simplifies the problem of selecting the sequences to be interleaved so as to result in lower value of maximum correlation parameter* $\Omega_{\max}$*.*

The further discussion is broken up into four cases as shown in Fig. 7.

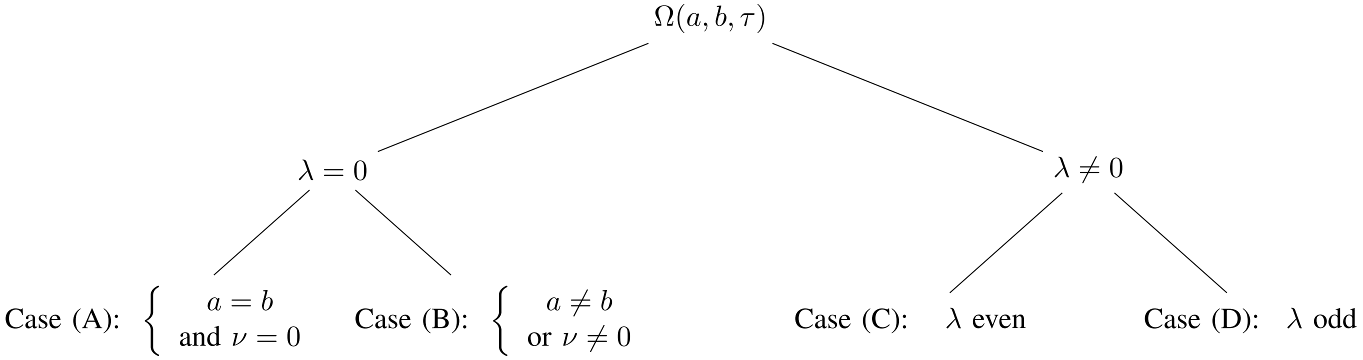

$\Omega(a,b,\tau)$
$\lambda = 0$
$\lambda \neq 0$
Case (A): $\left\{ \begin{array}{c} a = b \\ \text{and } \nu = 0 \end{array} \right.$
Case (B): $\left\{ \begin{array}{c} a \neq b \\ \text{or } \nu \neq 0 \end{array} \right.$
Case (C): λ even
Case (D): λ odd

Figure 7: Breaking up the correlation function of a pair of sequences from Family $\mathcal{J}_{5,\text{LEC}}$ into four different cases. A closed-form expression for the correlation is provided in each case.

A. *Case $a = b$ and $\lambda = \nu = 0$*

We have that

$$\lambda = 0,\ \nu = 0 \implies \tau = 0.$$

If in addition, $a = b$ we clearly have

$$\Omega(a,b,\tau) \quad = \quad L. \tag{60}$$

B. *Case $\lambda = 0$, and either $\nu \neq 0$ or $a \neq b$*

Recall from (38) that for $\lambda = 0$, the cross-correlation of a pair of distinct $\mathbb{Z}_4$-linear sequences $\{K(x_i, y_i, t)\}$, $\{K(x_j, y_j, t)\}$, is given by

$$\phi_{ij}(0) \quad = \quad \left\{ \begin{array}{rl} 0, & x_i \neq x_j, \\ -2, & x_i = x_j,\ y_i \neq y_j, \\ 2n, & x_i = x_j,\ y_i = y_j. \end{array} \right.$$

It follows as a result, that for $\lambda = 0$, and either $\nu \neq 0$ or $a \neq b$, we have that

$$\begin{aligned} \Omega(a,b,\tau) \quad &= \quad \sum_{j=0}^{4} \phi\Big(x^{(a)}, y^{(a)}_{j \oplus \nu}, x^{(b)}, y^{(b)}_j,\ 0\Big), \\ &= \quad \begin{cases} 0, & x^{(a)} \neq x^{(b)}, \\ -10, & x^{(a)} = x^{(b)},\ \text{but either } a \neq b \text{ or } \nu \neq 0. \end{cases} \end{aligned} \tag{61}$$

C. *Case λ even, $\lambda \neq 0$*

We focus next on the case λ even, $\lambda \neq 0$. A similar analysis will hold for the case λ odd. We begin with correlation expressions for the general case. From equations (36), (33) and (35), with τ replaced by λ and (x_i, y_i, x_j, y_j) replaced by $\big(x^{(a)}, y^{(a)}_{j \oplus \nu}, x^{(b)}, y^{(b)}_j\big)$ we have that

$$\phi\Big(x^{(a)}, y^{(a)}_{j \oplus \nu}, x^{(b)}, y^{(b)}_j,\ \lambda\Big) \quad = \quad \left\{ \begin{array}{ll} 2\Re\Big(\rho\big(x^{(a)}, y^{(a)}_{j \oplus \nu}, x^{(b)}, y^{(b)}_j,\ \lambda\big)\Big), & \lambda \text{ even}, \\ 2\Re\Big(\rho^*\big(x^{(a)}, y^{(a)}_{j \oplus \nu}, x^{(b)}, y^{(b)}_j,\ \lambda\big)\Big), & \lambda \text{ odd}, \end{array} \right.$$

where

$$\rho\big(x^{(a)}, y^{(a)}_{j \oplus \nu}, x^{(b)}, y^{(b)}_j,\ \lambda\big) \quad = \quad \sum_{\ell=0}^{n-1} \imath^{Q(x^{(a)}, y^{(a)}_{j \oplus \nu}, \ell + \lambda)\ -\ Q(x^{(b)}, y^{(b)}_j, \ell)},$$

and

$$\rho^{(*)}\big(x^{(a)}, y^{(a)}_{j\oplus\nu}, x^{(b)}, y^{(b)}_j,\ \lambda\big) \;=\; \sum_{\ell=0}^{n-1} \imath^{3Q(x^{(a)},y^{(a)}_{j\oplus\nu},\ell+\lambda)\;-\;Q(x^{(b)},y^{(b)}_j,\ell)}.$$

As a result, we can write,

$$\begin{aligned}
\Omega(a,b,\tau) \;&=\; \sum_{j=0}^{4}\phi\Big(x^{(a)}, y^{(a)}_{j\oplus\nu}, x^{(b)}, y^{(b)}_j,\ \lambda\Big),\\
&=\; \begin{cases} \sum_{j=0}^{4} 2\Re\left\{\sum_{\ell=0}^{n-1} \imath^{Q(x^{(a)},y^{(a)}_{j\oplus\nu},\ell+\lambda)\;-\;Q(x^{(b)},y^{(b)}_j,\ell)}\right\}, & \lambda \text{ even },\\ \sum_{j=0}^{4} 2\Re\left\{\sum_{\ell=0}^{n-1} \imath^{3Q(x^{(a)},y^{(a)}_{j\oplus\nu},\ell+\lambda)\;-\;Q(x^{(b)},y^{(b)}_j,\ell)}\right\}, & \lambda \text{ odd }. \end{cases}
\end{aligned}$$

By making use of the closed-from expression for correlation of sequences in Family $\mathcal{K}$ appearing in equation (41), we obtain that for the case λ even, $\lambda \neq 0$,

$$\begin{aligned}
\Omega(a,b,\tau) \;&=\; \sum_{j=0}^{4} 2\Re\left\{\sum_{\ell=0}^{n-1} \imath^{Q(x^{(a)},y^{(a)}_{j\oplus\nu},\ell+\lambda)\;-\;Q(x^{(b)},y^{(b)}_j,\ell)}\right\},\\
&=\; \sum_{j=0}^{4} 2\Re\left\{\imath^{(x^{(a)}-x^{(b)})}\left[-1-(2\imath)^k\imath^{-T\left(e(y^{(a)}_{j\oplus\nu},y^{(b)}_j,\lambda)\right)}\right]\right\},\\
&=\; (-2)\sum_{j=0}^{4}\Re\left\{\imath^{(x^{(a)}-x^{(b)})}\right\} \;-\; 2(2\imath)^k\sum_{j=0}^{4}\Re\left\{\imath^{x^{(a)}-x^{(b)}-T\left(e(y^{(a)}_{j\oplus\nu},y^{(b)}_j,\lambda)\right)}\right\},
\end{aligned}\tag{62}$$

where from (42), $e(y^{(a)}_{j\oplus\nu}, y^{(b)}_j, \lambda)$ is the unique element in $\mathcal{T}_m$, satisfying

$$e(y^{(a)}_{j\oplus\nu}, y^{(b)}_j, \lambda) \;:=\; \mu + y^{(a)}_{j\oplus\nu} + \mu^2(y^{(a)}_{j\oplus\nu} + y^{(b)}_j) \pmod 2,\tag{63}$$

with μ given from (43) by

$$\mu \;:=\; \sqrt{\frac{1}{1+\alpha^\lambda}} \pmod 2.\tag{64}$$

D. *Case λ odd*

A similar argument holds for the case λ odd. The only changes are that we replace $e(y^{(a)}_{j\oplus\nu}, y^{(b)}_j, \lambda)$ by $f(y^{(a)}_{j\oplus\nu}, y^{(b)}_j, \lambda)$ and $\big(x^{(a)} - x^{(b)}\big)$ by $\big(3x^{(a)} - x^{(b)}\big)$ for λ odd. Thus for λ odd, we have:

$$\begin{aligned}
\Omega(a,b,\tau) \;&=\; \sum_{j=0}^{4} 2\Re\left\{\sum_{\ell=0}^{n-1} \imath^{3Q(x^{(a)},y^{(a)}_{j\oplus\nu},\ell+\lambda)\;-\;Q(x^{(b)},y^{(b)}_j,\ell)}\right\},\\
&=\; \sum_{j=0}^{4} 2\Re\left\{\imath^{(3x^{(a)}-x^{(b)})}\left[-1-(2\imath)^k\imath^{-T\Big((f(y^{(a)}_{j\oplus\nu},y^{(b)}_j,\lambda)\Big)}\right]\right\},\\
&=\; (-2)\sum_{j=0}^{4}\Re\left\{\imath^{(3x^{(a)}-x^{(b)})}\right\} \;-\; 2(2\imath)^k\sum_{j=0}^{4}\Re\left\{\imath^{3x^{(a)}-x^{(b)}-T\Big((f(y^{(a)}_{j\oplus\nu},y^{(b)}_j,\lambda)\Big)}\right\},
\end{aligned}\tag{65}$$

where $f(y^{(a)}_{j\oplus\nu}, y^{(b)}_j, \lambda)$ is the unique element in $\mathcal{T}_m$, satisfying

$$f(y^{(a)}_{j\oplus\nu}, y^{(b)}_j, \lambda) \;:=\; (1+\mu+\mu^2) \;+\; y^{(a)}_{j\oplus\nu} + \mu^2(y^{(a)}_{j\oplus\nu} + y^{(b)}_j) \pmod 2,\tag{66}$$

with μ given from (43) by

$$\mu \;:=\; \sqrt{\frac{1}{1+\alpha^\lambda}} \pmod 2.$$

E. Correlation Summary

For a given cyclic-shift parameter $\tau \in [L]$, let $\lambda = \tau \pmod{2n}$ and $\nu = \lambda \pmod 5$ as above. In summary, we then have the following:

(a) for the case when τ is such that $\lambda = 0$, we have

$$\Omega(a,b,\tau) \;\; = \;\; \begin{cases} L, & \tau = 0 \text{ and } a = b, \\ 0, & \lambda = 0 \text{ and } x^{(a)} \neq x^{(b)}, \\ -10, & \lambda = 0, \; x^{(a)} = x^{(b)}, \text{ but either } a \neq b \text{ or } \nu \neq 0. \end{cases} \tag{67}$$

(b) for the case when τ is such that λ is even, but $\lambda \neq 0$, we have that $\Omega(a,b,\tau)$ is given by (62),

(c) for the case when τ is such that λ is odd, we have that $\Omega(a,b,\tau)$ is given by (65).

F. Criterion for Reducing $\Omega_{\max}$ from $\big(10(2^k)+10\big)$ to $\big(8(2^k)+10\big)$

It follows from an examination of (62), (65) and (67), that apart from the trivial case when $(a = b, \tau = 0)$, we have

$$|\;\Omega(a,b,\tau)\;| \;\; \leq \;\; 5(2(2^k+1)) = 10(2^k) \; + \; 10.$$

1) Case λ even, $\lambda \neq 0$: An examination of the 5-term summation

$$\sum_{j=0}^{4} \Re\left\{ \imath^{x^{(a)}-x^{(b)}+1-T\left(e(y^{(a)}_{j\oplus\nu},y^{(b)}_{j},\lambda)\right)} \right\} \tag{68}$$

appearing in (62) above for the case λ even, will reveal that the maximum correlation magnitude can be reduced for the case of λ even, $\lambda \neq 0$, from

$$5(2(2^k+1)) = 10(2^k) + 10 \text{ to } \; 4(2(2^k+1)) + 2 = 8(2^k) + 10,$$

if we can ensure that the possibility of

$$x^{(a)} - x^{(b)} + 1 - T\big(e(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda)\big) \;\; = \;\; 0 \pmod 2, \text{ all } j, \;\; j \in [5],$$

or equivalently,

$$T\big(e(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda)\big) = 1 \; + \; x^{(a)} \; + \; x^{(b)} \pmod 2, \text{ all } j, \;\; j \in [5], \tag{69}$$

is ruled out for any value of τ such that λ is even, $\lambda \neq 0$, and ν is arbitrary in the range $0 \leq \nu \leq 4$, by careful selection of the elements $\big(x^{(a)}, \{y^{(a)}_{j}\}_{j=0}^{4}\big)$ for $a \in [M]$. This is because if the possibility expressed in (69) is ruled out, then at least one of the summands in (68) will equal 0.

2) Case λ odd: The analogous statement in the case of λ odd is that the maximum correlation magnitude can be reduced from $\big(10(2^k)+10\big)$ to $\big(8(2^k)+10\big)$ if we can ensure that the possibility of

$$3x^{(a)} - x^{(b)} + 1 - T\big(f(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda)\big) \;\; = \;\; 0 \pmod 2,$$

or equivalently,

$$T\big(f(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda)\big) = 1 \; + \; x^{(a)} \; + \; x^{(b)} \pmod 2, \text{ all } j, \;\; j \in [5], \tag{70}$$

is ruled out for any value of τ such that λ is odd and ν is arbitrary in the range $0 \leq \nu \leq 4$, by careful selection of the elements $\big(x^{(a)}, \{y^{(a)}_{j}\}_{j=0}^{4}\big)$ for $a \in [M]$.

VII. Improved Upper Bound on $\Omega_{\max}$ for Family $\mathcal{J}_{5,\text{LEC}}$

We will now show that the low-even-correlation sequence family $\mathcal{J}_{5,\text{LEC}}$ constructed in Construction 1, has maximum nontrivial correlation magnitude $\Omega_{\max}$ upper bounded by $(8(2^k)+10)$. We first examine the criterion provided in (69) and (70) more closely. As before, for a given cyclic-shift parameter $\tau \in [L]$, we set $\lambda = \tau \pmod{2n}$ and $\nu = \lambda \pmod 5$.

1) For the case λ even, $\lambda \neq 0$, we need to avoid that

$$T\big(e(y^{(a)}_{j\oplus\nu}, y^{(b)}_j, \lambda)\big) = 1 \ + \ x^{(a)} \ + \ x^{(b)} \pmod 2, \ \text{all } j, \, j \in [5],$$

i.e., we need to avoid

$$\text{tr}(y^{(a)}_{j\oplus\nu}) \ + \ \text{tr}(\mu^2(y^{(a)}_{j\oplus\nu} + y^{(b)}_j)) = \text{tr}(\mu) + 1 \ + \ x^{(a)} \ + \ x^{(b)}, \quad \pmod 2, \ \text{all } j, \, j \in [5].$$

It follows that it suffices to ensure that for any given value of $a, b \in [M]$ and ν, $0 \leq \nu \leq 4$, the sum of the traces

$$\text{tr}(y^{(a)}_{j\oplus\nu}) + \text{tr}(\mu^2(y^{(a)}_{j\oplus\nu} + y^{(b)}_j)) \pmod 2,$$

is not the same for all $j \in [5]$.

2) For the case λ odd, we need to avoid that

$$T\big(f(y^{(a)}_{j\oplus\nu}, y^{(b)}_j, \lambda)\big) = 1 \ + \ x^{(a)} \ + \ x^{(b)} \pmod 2, \ \text{all } j, \, j \in [5],$$

i.e., we need to avoid

$$\text{tr}(y^{(a)}_{j\oplus\nu}) \ + \ \text{tr}(\mu^2(y^{(a)}_{j\oplus\nu} + y^{(b)}_j)) = \text{tr}(1 + \mu + \mu^2) + 1 \ + \ x^{(a)} \ + \ x^{(b)}, \quad \pmod 2, \ \text{all } j, \, j \in [5].$$

But here again, we see that it suffices to ensure that for any given value of $a, b \in [M]$ and ν, $0 \leq \nu \leq 4$, the sum of the traces

$$\text{tr}(y^{(a)}_{j\oplus\nu}) + \text{tr}(\mu^2(y^{(a)}_{j\oplus\nu} + y^{(b)}_j)) \pmod 2,$$

is not the same for all $j \in [5]$.

Thus we see that we end up with the same "sum-of-traces" criterion regardless of whether λ is even with $\lambda \neq 0$, or else, λ odd. We summarize this observation in the form of a Lemma.

Lemma 1 (Sum-of-traces condition)**.** *Let $\mathcal{J}_{5,LEC}$ be the low-even-correlation family of sequences constructed using Construction 1. For given value of cyclic shift $\tau \in [L]$, let $\lambda = \tau \pmod{2n}$ and $\nu = \lambda \pmod 5$. Then the parameters $\Omega_{a,\max}$, $\Omega_{c,\max}$ of the family $\mathcal{J}_{5,LEC}$ will satisfy*

$$\max\{\Omega_{a,\max}, \ \Omega_{c,\max}\} \quad \leq \quad (8(2^k) + 10),$$

if the parameters $\{\big(x^{(a)}, \{y^{(a)}_j\}_{j=0}^4\big) \mid a \in [M]\}$ can be verified to satisfy the sum-of-traces criterion below namely, that for any fixed value of $a, b \in [M]$, $\lambda \neq 0$, and ν, $0 \leq \nu \leq 4$, the sum of traces

$$\sigma(j) \quad := \quad tr(y^{(a)}_{j\oplus\nu}) + tr(\mu^2(y^{(a)}_{j\oplus\nu} + y^{(b)}_j)) \pmod 2, \tag{71}$$

where $\mu = (1 + \alpha^\lambda)^{-\frac{1}{2}}$, does not take on the same value for at least one value of j, $j \in [5]$.

Theorem 1. *Let $\mathcal{J}_{5,LEC}$ be the low-even-correlation family of sequences constructed using Construction 1. Then the parameters $\Omega_{a,\max}$, $\Omega_{c,\max}$ of the family $\mathcal{J}_{5,LEC}$ satisfy the upper bound*

$$\max\{\Omega_{a,\max}, \ \Omega_{c,\max}\} \quad \leq \quad (8(2^k) + 10),$$

Proof. We will prove the theorem by verifying that the parameters

$$\{\big(x^{(a)}, \{y^{(a)}_j\}_{j=0}^4\big) \mid a \in [M]\},$$

of $\mathcal{J}_{5,\text{LEC}}$ satisfy for any $a, b \in [M]$, $\lambda \neq 0$, and any ν, $0 \leq \nu \leq 4$, the sum-of-traces criterion appearing in Lemma 1. The sum-of-traces criterion requires that for any fixed value of λ, $\lambda \neq 0$, and ν, $0 \leq \nu \leq 4$, the sum of traces

$$\sigma(j) \quad := \quad \text{tr}(y^{(a)}_{j\oplus\nu}) + \text{tr}(\mu^2(y^{(a)}_{j\oplus\nu} + y^{(b)}_j)) \pmod 2,$$

where $\mu = (1+\alpha^{\lambda})^{-\frac{1}{2}}$, is not the same for at least one value of j, $j \in [5]$. However, this property is ensured by the sum-constant, trace-different property which states that for any value of ν, $0 \leq \nu \leq 4$ there are at least two distinct values j_1, j_2 of index $j \in \{1,2,3,4\}$ such that

$$\begin{array}{rcl} j_1 \oplus \nu \in \{1,2,3,4\}, & & j_2 \oplus \nu \in \{1,2,3,4\} \\ y^{(a)}_{j_1 \oplus \nu} + y^{(b)}_{j_1} & = & y^{(a)}_{j_2 \oplus \nu} + y^{(b)}_{j_2}, \end{array}$$

but

$$\mathrm{tr}(y^{(a)}_{j_1 \oplus \nu}) \neq \mathrm{tr}(y^{(a)}_{j_2 \oplus \nu}),$$

so we are done. □

Remark 5 (Freedom in selecting the $j=0$ sequence)**.** *The sum-of-traces criterion requires that for any value of ν, $0 \leq \nu \leq 4$, the 5 trace-sums $\{\sigma(j)\}_{j=0}^{4}$ are not all the same. But the proof of Theorem 1 above shows that this statement is true even if we restrict attention to the subset*

$$\{\sigma(j) \mid j \in \{1,2,3,4\},\ j \oplus \nu \in \{1,2,3,4\}\}.$$

This tells us that in order to lower maximum correlation parameters $\Omega_{a,\max}, \Omega_{c,\max}$, in constructing the a-th sequence, $\{J^{(a)}(t)\}$ in $\mathcal{J}_{5,\mathrm{LEC}}$, for $a \in [M]$, it is only necessary to carefully select the four sequences $\{K^{(a)}_j(t)\}$ for $j = 1,2,3,4$. *The sequence $\{K^{(a)}_0(t)\}$ can be freely chosen. This freedom in selecting the sequence $\{K^{(a)}_0(t)\}$ will be employed in Section IX to improve odd-correlation properties while maintaining even-correlation properties and balance for the case $m = 10$ and period $L = 10230$.*

VIII. Constructing the Balanced Family $\mathcal{J}_{5,\mathrm{BAL}}$

We examine in Section VIII-A, the symbol balance of sequences $\{J^{(a)}(t)\}$, $a \in [M]$, constituting the low-even-correlation family $\mathcal{J}_{5,\mathrm{LEC}}$ constructed in Construction 1. We will show that the sequences in $\mathcal{J}_{5,\mathrm{LEC}}$, do not satisfy the property of having symbol balance to within 2; they are only guaranteed to have symbol balance to within $((4 \times 2^k) + 10)$ and may therefore be said to only be weakly balanced. For this reason, we present in Subsection VIII-B below, a modification of Construction 1, that results in a modified sequence family $\mathcal{J}_{5,\mathrm{BAL}}$. We will show that sequences within family $\mathcal{J}_{5,\mathrm{BAL}}$ have symbol balance to within 2, while continuing to have maximum nontrivial correlation magnitude $\Omega_{\max}$ upper bounded by $2(5+4(2^k))$.

A. Weak Balance of Family $\mathcal{J}_{5,LEC}$

Recall from (28), that in the case of a sequence $\{K(x,y,t)\}$ lying within the family $\mathcal{K}$, we have that

$$\sum_{t=0}^{2n-1} (-1)^{K(x,y,t)} = (-2)\Re\{\imath^{x}\} - 2^{k+1}\Re\{\imath^{x+k-T(y)}\}.$$

Each sequence $\{J^{(a)}(t)\}$ within Family $\mathcal{J}_{5,\mathrm{LEC}}$, is obtained by interleaving the 5 $\mathbb{Z}_4$-linear sequences $\Big\{\{K(x^{(a)}, y^{(a)}_j, t)\} \mid j \in [5]\Big\}$. As a result, we have that

$$\begin{aligned} \sum_{t=0}^{10n-1} (-1)^{J^{(a)}(t)} &= \sum_{j=0}^{4}\sum_{t=0}^{2n-1} (-1)^{K(x^{(a)},\ y^{(a)}_j,\ t)}, \\ &= (-10)\Re\{\imath^{x^{(a)}}\} - 2^{k+1}\sum_{j=0}^{4}\Re\{\imath^{x^{(a)}+k-T(y^{(a)}_j)}\}. \end{aligned} \tag{72}$$

Let us define the elements

$$\begin{aligned} u^{(a)}_j &:= x^{(a)} + k - T(y^{(a)}_j), \quad (\mathrm{mod}\ 2), \quad j \in [5], \\ &= x^{(a)} + k + \mathrm{tr}(y^{(a)}_j), \quad (\mathrm{mod}\ 2), \quad j \in [5], \end{aligned}$$

belonging to $\mathbb{F}_2$. As the set of elements $\{y_j^{(a)}\}_{j=1}^4$ represent a coset of W in H, of the 4 values of $u_j^{(a)}$, $j = 1, 2, 3, 4$, two have value 0 and 2 have value 1. The two 1 values contribute 0 to the balance since $\Re(\imath) = 0$. The two 0 values each contribute $\{\pm 2^{k+1}\}$ to the balance. It follows that to ensure balance to within 2, it is necessary that the remaining 5th term corresponding to $j = 0$ contribute nothing, i.e., it is necessary to ensure that

$$x^{(a)} + k + \mathrm{tr}(y_0^{(a)}) \;\;=\;\; 1 \pmod 2,$$

i.e., ensure that

$$\mathrm{tr}(y_0^{(a)}) \;\;=\;\; (x^{(a)} + k + 1) \pmod 2, \;\; \forall a \in [M]. \tag{73}$$

We will refer to this as the trace condition for symbol balance. From equation (56) in Remark 3 following Construction 1, we see that sequences in family $\mathcal{J}_{5,\mathrm{LEC}}$ satisfy this condition. Thus we can drop the term associated to index $j = 0$ in the sum on the right of equation (72), leading to the following expression for sequence balance

$$\sum_{t=0}^{10n-1} (-1)^{J^{(a)}(t)} \;\;=\;\; (-10)\Re\{\imath^{x^{(a)}}\} - 2^{k+1} \sum_{j=1}^{4} \Re\{\imath^{x^{(a)}+1-T(y_j^{(a)})}\}.$$

Again, because the set of elements $\{y_j^{(a)}\}_{j=1}^4$ form a coset, we know that the value of the 4-term sum

$$\sum_{j=1}^{4} \Re\{\imath^{x^{(a)}+1-T(y_j^{(a)})}\} \text{ equals either } 0 \text{ or else}, \pm 2.$$

As a result, we see that balance to within 2 cannot be attained in the present setup, we are only guaranteed to have symbol balance B in the range $10 \leq B \leq ((4 \times 2^k) + 10)$. We introduce in the subsection below, a modification to the construction of Family $\mathcal{J}_{5,\mathrm{LEC}}$ in Construction 1 by introducing certain ± 1 multiplicative terms, which we term as Flipping Factors (FF) (see Definition 1). We will refer to the modified construction as the Balanced Construction and will use the notation $\mathcal{J}_{5,\mathrm{BAL}}$ to denote the balanced sequence family resulting from the construction.

Remark 6 (Explaining Upper Bound of $2\lfloor \frac{2^{m-1}}{6} \rfloor$ on Family Size)**.** *The construction procedure outlined here for both Families $\mathcal{J}_{5,LEC}$ and $\mathcal{J}_{5,BAL}$ has the feature that each sequence $\{J^{(a)}(t)\}$ belonging to either family is derived by interleaving sequences from $\mathcal{K}$ possessing the same x parameter, namely, $x^{(a)}$. As noted above, in this setting, to ensure that each sequence has balance to within 2, we must meet the trace condition for symbol balance, namely that*

$$tr(y_0^{(a)}) \;\;=\;\; (x^{(a)} + k + 1) \pmod 2, \;\; \forall a \in [M].$$

Let us consider the case when $(x^{(a)} + k + 1) = 0$. It follows from this condition for balance that each sequence $\{J^{(a)}(t)\}$ is obtained by interleaving 5 sequences from $\mathcal{K}$ having y-parameters $\big(y_j^{(a)}, j \in [5]\big)$, with $y_j^{(a)}$ satisfying:

$$tr(y_j^{(a)}) \;\;=\;\; 0,$$

for $j = 0$ and two other non-zero values of j, $j \in [5]$. But there are only $2^{m-1}/2$ parameters y, $t \in H$, having trace-value equal to zero. For this reason the size of Families $\mathcal{J}_{5,LEC}$, $\mathcal{J}_{5,BAL}$ is upper bounded by the value $2 \times \big(\lfloor 2^{m-1}/6 \rfloor\big)$.

B. The Balanced Construction

Associated to each index a, $a \in [M]$, we introduce a set of 5 FF corresponding to the set of 5 binary variables

$$\{\epsilon_j^{(a)} \in \{0, 1\}\}, \;\; j \in [5], \tag{74}$$

that are used to selectively complement the 5 $\mathbb{Z}_4$-linear sequences $\{K_j^{(a)}(t)\}_{j=0}^4$ that are interleaved to yield the sequence $\{J^{(a)}(t)\}$ belonging to Family $\mathcal{J}_{5,\mathrm{LEC}}$ in Construction 1. The reason for regarding these as FF is because they appear in balance and correlation expressions, in the multiplicative ± 1 form $(-1)^{\epsilon_j^{(a)}}$.

Construction 2 (Family $\mathcal{J}_{5,\mathrm{BAL}}$)**.** *Let β be an element of $\mathbb{R}_{4^m}$ having order $n = 2^{10} - 1$. Let (H, W) be an admissible pair of subspaces as described in Section V-B and let $Y(H, W)$ be an admissible parameter matrix as defined* *in Section V-C. Let* $y_j^{(a)}$ *denote the entry in the ath row,* $a \in [M]$*, and jth column,* $j \in [5]$*, of* $Y(H,W)$*. Let* $\{\epsilon_j^{(a)} \mid a \in [M], j \in [5]\}$ *be a collection of FF as defined in* (74)*. For* $x \in \{0,1\} \subseteq \mathbb{Z}_4$*,* $y \in H$*, we define the sequence*

$$K(x,y,t) \ := \ \mathit{MSB}\left\{3^t\left[x+T([1+2y]\beta^t)\right]\right\}, \ t \in [2n].$$

Then the Balanced Family $\mathcal{J}_{5,BAL}$*, is a family of* $M = 2\lfloor 2^{m-1}/6 \rfloor$ *binary sequences, each having period* $10n$*. The a-th sequence* $\{J^{(a)}(t)\}$*,* $a \in [M]$*, in the family is obtained by CRT-based interleaving of the* 5 $\mathbb{Z}_4$*-linear sequences* $\left\{\{K(x^{(a)},\ y_j^{(a)},\ \ell)\ +\ \epsilon_j^{(a)}\}\right\}_{j=0}^{4}$*, where*

$$x^{(a)} \ = \ \begin{cases} 0, & a \in [M/2], \\ 1, & M/2+1 \leq a \leq (M-1). \end{cases}$$

Thus the a-th sequence $\{J^{(a)}(t)\}$*,* $a \in [M]$*, in Family* $\mathcal{J}_{5,BAL}$*, is given by*

$$J^{(a)}(t) \ = \ K(x^{(a)},\ y_j^{(a)},\ \ell)\ +\ \epsilon_j^{(a)}, \quad t \in N, \tag{75}$$

in which $j = t \pmod 5$ *and* $\ell = t \pmod{2n}$*, and where, further, the FF are chosen in such a manner that each sequence* $\{J^{(a)}(t)\}$*,* $a \in [M]$*, has symbol balance to within* 2*.*

Remark 7. *1) It is shown in Section VIII-C below, that the FF* $\left(\epsilon_j^{(a)}, j \in [5]\right)$*,* $a \in [M]$ *can be selected in such a way that each sequence* $\{J^{(a)}(t)\}$ *has symbol balance to within* 2*.*

2) An inspection of Constructions 1 and 2, will show that apart from the addition of FF $\{\epsilon_j^{(a)}\}$*, the balanced Family* $\mathcal{J}_{5,BAL}$ *is identical to the low-even-correlation Family* $\mathcal{J}_{5,LEC}$*. Thus if we set* $\epsilon_j^{(a)} = 0$ *for all* $a \in [M], j \in [5]\}$ *in the construction of Family* $\mathcal{J}_{5,BAL}$*, we will recover Family* $\mathcal{J}_{5,LEC}$*.*

C. Selection of FF to Achieve Balance

In this section, we will show how it is possible to select the FF so as to ensure that each sequence in Family $\mathcal{J}_{5,\mathrm{BAL}}$ has symbol balance to within 2. It will be shown below that the introduction of these FF does not impact the maximum magnitude of an even correlation, so that the correlation parameters $\Omega_{a,\max}$, $\Omega_{c,\max}$ associated to Family $\mathcal{J}_{5,\mathrm{BAL}}$ remain upper bounded by the value $((8 \times 2^k) + 10)$.

With the introduction of these FF, from (72), we have that the balance expression for a sequence $\{J^{(a)}(t)\}$ in the balanced Family $\mathcal{J}_{5,\mathrm{BAL}}$ becomes:

$$\begin{aligned} \sum_{t=0}^{10n-1} (-1)^{J^{(a)}(t)} \ &= \ \sum_{j=0}^{4}\sum_{t=0}^{2n-1} (-1)^{K\left(x^{(a)},\ y_j^{(a)}, t\right)\ +\ \epsilon_j^{(a)}}, \\ &= \ (-2)\sum_{j=0}^{4}(-1)^{\epsilon_j^{(a)}}\Re\{\imath^{x^{(a)}}\} - 2^{k+1}\sum_{j=0}^{4}(-1)^{\epsilon_j^{(a)}}\Re\{\imath^{x^{(a)}+k-T(y_j^{(a)})}\}. \end{aligned}$$

The same argument as before tells us that to attain balance to within 2, we must continue to have

$$\mathrm{tr}(y_0^{(a)}) \ = \ x^{(a)} + k + 1 \pmod 2. \tag{76}$$

Focusing on the term

$$-2^{k+1}\sum_{j=0}^{4}(-1)^{\epsilon_j^{(a)}}\Re\{\imath^{x^{(a)}+k-T(y_j^{(a)})}\},$$

we see that in order to achieve balance within 2, we must make this term equal to 0 in value. There are 5 terms in the sum. Of these, on account of our choice in (76), the term $j = 0$ contributes 0. The same is true of 2 other values in the summation, since in the set $\{y_j^{(a)}, j = 1,2,3,4\}$, two of the elements have binary trace value $= 0$ and two have binary trace value equal to 1. Thus we are left with 2 terms, say associated to $j = j_1$ and $j = j_2$, where the terms

$$-2^{k+1}(-1)^{\epsilon_j^{(a)}}\Re\{\imath^{x^{(a)}+1-T(y_j^{(a)})}\}, \ \text{for } j = j_1, j_2,$$

take on values $\pm 2^{k+1}$. Clearly, by appropriately choosing the two FF $\epsilon_{j_1}^{(a)}, \epsilon_{j_2}^{(a)}$, we can ensure that the overall contribution of the term multiplied by -2^{k+1} equals zero.

With this choice of FF, the expression for sequence balance reduces to

$$\sum_{t=0}^{10n-1} (-1)^{J^{(a)}(t)} \;\; = \;\; (-2)\sum_{j=0}^{4}(-1)^{\epsilon_j^{(a)}} \Re\{\imath^{x^{(a)}}\}.$$

If $x^{(a)} = 1$, then the value of the sum

$$\sum_{j=0}^{4}(-1)^{\epsilon_j^{(a)}} \Re\{\imath^{x^{(a)}}\}$$

is zero. If $x^{(a)} = 0$, then the value of this term equals

$$(-2)\sum_{j=0}^{4}(-1)^{\epsilon_j^{(a)}},$$

which can take on values in the set

$$\{\pm 10,\ \pm 6,\ \pm 2\}.$$

However, we still have the freedom to choose the values of the three remaining FF, i.e., the FF $\epsilon_j^{(a)}$, for $j \in \{0, 1, 2, 3, 4\} \setminus \{j_1, j_2\}$. By exercising this choice, it is clear that we can ensure that the magnitude of the balance equals at most 2.

D. No Impact on Upper Bound on Correlation Values

We show here that the flipping of individual Z_4-linear sequences does not impact the upper bound of $2(5+4(2^k))$ on even-correlation values. Thus, all non-trivial even correlation magnitudes in the balanced Family $\mathcal{J}_{5,\text{BAL}}$, will be shown to be upper bounded by the value $2(5+4(2^k))$. To see this, we go back and examine how the reduction in maximum nontrivial correlation magnitude from $2(5+5(2^k))$ to $2(5+4(2^k))$ was achieved in the case of Family $\mathcal{J}_{5,\text{LEC}}$. We can clearly, ignore the trivial case when $a = b, \tau = 0$.

1) Case $\lambda = 0$, and either $\nu \neq 0$ or $a \neq b$: The cross-correlation between two sequences in Family $\mathcal{J}_{5,\text{BAL}}$ can be expressed in the form

$$\begin{aligned}\Omega(a, b, \tau) \;\; &:= \;\; \sum_{t=0}^{10n-1} \imath^{J^{(a)}(t+\tau) - J^{(b)}(t)}, \\ &= \;\; \sum_{j=0}^{4}\sum_{\ell=0}^{2n-1}(-1)^{K_{j\oplus\nu}^{(a)}(\ell+\lambda) - K_j^{(b)}(\ell) + \epsilon_{j\oplus\nu}^{(a)} + \epsilon_j^{(b)}}.\end{aligned}$$

Let us define

$$q(a, b, j, \nu) \;\; = \;\; \epsilon_{j\oplus\nu}^{(a)} + \epsilon_j^{(b)} \pmod 2,$$

and let us adopt the abbreviation $q(j)$ in place of $q(a, b, j, \nu)$. Then in the presence of the FF, we have that

$$\Omega(a, b, \tau) \; = \; \sum_{j=0}^{4}(-1)^{q(j)} \; \phi\Big(x^{(a)}, y_{j\oplus\nu}^{(a)}, x^{(b)}, y_j^{(b)},\; \lambda\Big).$$

Recall from (38) that for $\lambda = 0$, the cross-correlation of a pair of distinct $\mathbb{Z}_4$-linear sequences $\{K(x_i, y_i, t)\}, \{K(x_j, y_j, t)\}$ is given by

$$\phi_{ij}(0) \;\; = \;\; \begin{cases} \;\; 0, & x_i \neq x_j, \\ -2, & x_i = x_j,\; y_i \neq y_j. \end{cases}$$

It follows as a result, that for $\lambda = 0$, and either $\nu \neq 0$ or $a \neq b$, we have in the case of Family $\mathcal{J}_{5,\text{BAL}}$ that

$$\mid \Omega(a, b, \tau) \mid \;\; = \;\; \mid \sum_{j=0}^{4} \phi\Big(x^{(a)}, y_{j\oplus\nu}^{(a)}, x^{(b)}, y_j^{(b)},\; 0\Big) \mid \leq \;\; 10,$$

just as was the case with Family $\mathcal{J}_{5,\text{LEC}}$.

2) $\lambda \neq 0$: In this case, in the presence of the FF, from (62), we see that the correlation values are given by

$$\begin{aligned}\Omega(a,b,\tau) \ &= \ \sum_{j=0}^{4}(-1)^{q(j)} \ \phi\Big(x^{(a)}, y^{(a)}_{j\oplus\nu}, x^{(b)}, y^{(b)}_{j}, \ \lambda\Big), \\ &= \begin{cases} \sum_{j=0}^{4}(-1)^{q(j)} \ \Big((-2)\Re\{\imath^{(x^{(a)}-x^{(b)})}\} \ - 2^{k+1}\Re\left\{\imath^{(x^{(a)}-x^{(b)}) \ + \ k-T(e(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda)}\right\}\Big), & \lambda \text{ even}, \\ \sum_{j=0}^{4}(-1)^{q(j)} \ \Big((-2)\Re\{\imath^{(3x^{(a)}-x^{(b)})}\} \ - 2^{k+1}\Re\left\{\imath^{(3x^{(a)}-x^{(b)}) \ + \ k-T(f(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda)}\right\}\Big), & \lambda \text{ odd}, \end{cases}\end{aligned} \tag{77}$$

where μ, $e(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda)$ and $f(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda)$ are as defined earlier in equations (64), (63) and (66). Let us define

$$A \ := \ \sum_{j=0}^{4}\Re\left\{\imath^{(x^{(a)}-x^{(b)}) \ + \ k-T(e(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda)}\right\}, \quad \text{for } \lambda \text{ even } \lambda \neq 0, \tag{78}$$

$$B \ := \ \sum_{j=0}^{4}\Re\left\{\imath^{(3x^{(a)}-x^{(b)}) \ + \ k-T(f(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda)}\right\}, \quad \text{for } \lambda \text{ odd}. \tag{79}$$

The subspace and coset-decomposition-based construction of Family $\mathcal{J}_{5,\text{LEC}}$ was able to bring down the value of maximum correlation magnitude from $2(5+5(2^k))$ to $2(5+4(2^k))$ by ensuring for the case λ even, that at least one term in the set

$$\left\{\imath^{(x^{(a)}-x^{(b)}) \ + \ k-T(e(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda)} \mid j \in [5]\right\},$$

was imaginary, so that there were at most 4 nonzero summands on the right, in the expression for A in (78). This led to the bound

$$|A| \ \leq \ 4.$$

The corresponding result for the λ odd case is that that at least one term in the set

$$\left\{\imath^{(3x^{(a)}-x^{(b)}) \ + \ k-T(f(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda)} \mid j \in [5]\right\},$$

was imaginary, so that we analogously had at most 4 nonzero summands on the right in the expression for B in (79), leading to the bound

$$|B| \ \leq \ 4.$$

The addition of FFs $\{\epsilon^{(a)}_{j}\}_{j=0}^{4}$ to the interleaved sequences does not impact this argument since this merely causes the terms A, B to be replaced by corresponding terms A', B' given by

$$A' \ := \ \sum_{j=0}^{4}(-1)^{q(j)} \ \Re\left\{\imath^{(x^{(a)}-x^{(b)}) \ + \ 1-T(e(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda)}\right\},$$

$$B' \ := \ \sum_{j=0}^{4}(-1)^{q(j)} \ \Re\left\{\imath^{(3x^{(a)}-x^{(b)}) \ + \ 1-T(f(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda)}\right\}.$$

The introduction of the multiplicative factors $(-1)^{q(j)}$ multiplying individual terms in each summand of A, B, clearly does not change the number of zero summands and thus even in the presence of FF, the corresponding bounds

$$|A'| \ \leq \ 4, \qquad |B'| \ \leq \ 4,$$

continue to hold. It follows that the maximum even-correlation magnitude, even in the case of the balanced Family $\mathcal{J}_{5,\text{BAL}}$, is upper bounded by the value $2(5+4(2^k))$.

IX. Constructing Family $\mathcal{J}_{\text{NAV}}$ of Period 10230

The focus in this section is on the case $m = 10$ corresponding to period $L = 10230$ that is commonly encountered in a GNSS setting, see Table II. Note that $10 = 2 \pmod 4$, so that the results derived in prior sections for the families $\mathcal{J}_{\text{5,LEC}}$, $\mathcal{J}_{\text{5,BAL}}$ are applicable here. The sequences in Family $\mathcal{J}_{\text{5,BAL}}$ have symbol balance within 2 and have even-correlation parameters $\Omega_{a,\max}$, $\Omega_{c,\max}$ upper bounded by the value $2(5 + 4(2^k))$. However as discussed in Section I-A, in the setting of a GNSS, two important additional design considerations are lowering of odd-correlation values and pairing for orthogonality. Thus the aim in this section, is to perform operations on the sequences within the balanced Family $\mathcal{J}_{\text{5,BAL}}$, that preserve balance and even-correlation properties while at the same time

- lowering maximum odd-correlation magnitudes $\Omega^{(\text{odd})}_{a,\max}$ and $\Omega^{(\text{odd})}_{c,\max}$,
- and permitting a pairing of the sequence set into pairs, where within each pair $\{J^{(a)}(t)\}$, $\{J^{(b)}(t)\}$, the sequences are perfectly orthogonal at zero shift.

A. *List of Permissible Operations*

A list of operations that help ensure lower maximum odd-correlation magnitude and the orthogonal-pairs property is provided here, that are permissible in the sense that they preserve the balance and even-correlation properties of Family $\mathcal{J}_{\text{5,BAL}}$.

1) **Cyclically shifting the entire sequence:** Replacing each sequence $\{J^{(a)}(t)\}$ of period 10230 by an appropriate cyclic shift $\{J^{(a)}(t+\tau^{(a)})\}$, where $(t+\tau^{(a)})$ is computed modulo $10n$ clearly does not impact symbol balance or even-correlation properties. Odd-correlation properties are however, affected by cyclic shifts and thus one can use the flexibility in choice of cyclic shift parameters $\tau^{(a)}$ to lower maximum odd-correlation magnitudes $\Omega^{(\text{odd})}_{a,\max}$ and $\Omega^{(\text{odd})}_{c,\max}$.
2) **Exercise Flexibility in Selecting Sequence $\{K_0^{(a)}(t)\}$:** As pointed out in Remark 5, there is considerable flexibility in selecting the sequence $\{K_0^{(a)}(t)\}$ associated to index $j = 0$ within the framework of Construction 1 of Family $\mathcal{J}_{\text{5,LEC}}$. While Construction 2 of Family $\mathcal{J}_{\text{5,BAL}}$ introduces flipping factors $\{\epsilon_j^{(a)}\}$ to achieve symbol balance to within 2, it retains all of the flexibility in selecting sequence $\{K_0^{(a)}(t)\}$ that Construction 1 provides. It follows from Section V-C that for a given index $a \in [M]$ and corresponding value $x^{(a)}$, the only restriction in selecting the remaining parameter $y_0^{(a)}$ is that
$$y_0^{(a)} \quad \in \quad \begin{cases} T_0, & \text{if} \ \ x^{(a)} = 0 \ \ \text{or equivalently, for} \ \ 0 \leq a \leq 84, \\ T_1, & \text{if} \ \ x^{(a)} = 1 \ \ \text{or equivalently, for} \ \ 85 \leq a \leq 169, \end{cases}$$
where the sets T_0, T_1 are as defined in equations (50) and (51) respectively. This flexibility can be used to minimize odd-correlation parameters $\Omega^{(\text{odd})}_{a,\max}$ and $\Omega^{(\text{odd})}_{c,\max}$.
3) **Selection of the Flipping Factors:** In Construction 2, the FFs are chosen so as to ensure that each sequence $\{J^{(a)}(t)\}$ in Family $\mathcal{J}_{\text{5,BAL}}$, has symbol balance to within 2. However, there is some flexibility in the selection of the FF employed. This flexibility in selection of flipping patterns can also be employed to lower odd-correlation magnitudes.
4) **Imparting a Different Cyclic Shift to the Single, $j = 0$ Sequence $\{K_0^{(a)}(t)\}$:** In both Constructions 1 and 2, generating Families $\mathcal{J}_{\text{5,LEC}}$ and $\mathcal{J}_{\text{5,BAL}}$ respectively, the 5 sequences $\{K_j^{(a)}(\ell)\}_{j=0}^4$ that are interleaved to obtain a single sequence $\{J^{(a)}(t)\}$ are all "in-phase" as they are given by expressions of the form:
$$K_j^{(a)}(\ell) \quad = \quad \text{MSB}\left\{3^\ell \left(x^{(a)} + T\big([1 + 2y_j^{(a)}]\beta^{\ell+\lambda_j^{(a)}}\big)\right)\right\},$$
with cyclic-shift-parameter $\lambda_j^{(a)}$ set equal to 0, i.e., $\lambda_j^{(a)} = 0$. Our proof of the upper bound $2(5 + 4(2^{m/2}))$ on $\Omega_{\max}$ assumed this form of the $\mathbb{Z}_4$-linear sequences being interleaved. Clearly the balance property of the interleaved sequence $\{J^{(a)}(t)\}$ remains unaffected if we replace any constituent interleaved sequence $\{K^{(a)}(\ell)\}$ by a cyclic shift $\{K^{(a)}(\ell + \lambda_j^{(a)})\}$.

   We will now show that the even-correlation properties remain unaffected even if we replace just the $j = 0$ sequences $\{K_0^{(a)}(\ell)\}$ for $a \in [M]$, by the cyclic shift $\{K_0^{(a)}(\ell+\lambda_0^{(a)})\}$, where the addition $(\ell+\lambda_0^{(a)})$ is computed modulo $2n$. Thus under this procedure, the phase of the remaining sequences $\left\{\{K_j^{(a)}(\ell)\} \mid j = 1,2,3,4\right\}$ is kept unchanged, i.e., they are not cyclically shifted.

To see this, we rewrite the expression for the correlation of a pair of sequences in Family $\mathcal{J}_{\text{NAV}}$ appearing in (59) to account for this change. We only consider the case $\nu \neq 0$ here. The case $\nu = 0$ can be similarly argued.

$$\begin{aligned}
\Omega(a,b,\tau) &= \sum_{t=0}^{10n-1} \imath^{J^{(a)}(t+\tau) - J^{(b)}(t)} \\
&= \underbrace{\sum_{\ell=0}^{2n-1} (-1)^{K_\nu^{(a)}(\ell+\lambda) - K_0^{(b)}(\ell+\lambda_0^{(b)})}}_{\Gamma_1 \;\Leftrightarrow\; (j=0) \text{ term}} + \underbrace{\sum_{\ell=0}^{2n-1} (-1)^{K_0^{(a)}(\ell+\lambda_0^{(a)}+\lambda) - K_{5\ominus\nu}^{(b)}(\ell)}}_{\Gamma_2 \;\Leftrightarrow\; (j\oplus\nu=0) \text{ term}} \\
&\quad + \underbrace{\sum_{\substack{0\le j\le 4,\\ j\neq 0,\ j\oplus\nu\neq 0}} \sum_{\ell=0}^{2n-1} (-1)^{K_j^{(a)}(\ell+\lambda) - K_j^{(b)}(\ell)}}_{\Gamma_3 \;\Leftrightarrow\; (j\neq 0, j\oplus\nu\neq 0) \text{ term}} .
\end{aligned}$$

In the equation above, by $5 \ominus \nu$ we mean the subtraction $(5-\nu) \pmod 5$. Also, clearly, the terms Γ_1, Γ_2 are each upper bounded in magnitude by the value $(2+2^{k+1})$. Thus it suffices to show that the term Γ_3 satisfies the upper bound

$$\Gamma_3 \;\;\le\;\; 2 + 2(2+2^{k+1}) \;=\; 6 + 2^{k+2}.$$

This will ensure that

$$|\,\Gamma_1 + \Gamma_2 + \Gamma_3\,| \;\;\le\;\; (8(2^k) + 10).$$

To show that $\Gamma_3 \le 134$, we first note from equations (41) and (44) that

$$\Gamma_3 \;=\; (-2) \sum_{\substack{0\le j\le 4,\\ j\neq 0,\ j\oplus\nu\neq 0}} \Re\left\{\imath^{(x^{(a)}-x^{(b)})}\right\} \;-\; 2^{k+1} \sum_{\substack{0\le j\le 4,\\ j\neq 0,\ j\oplus\nu\neq 0}} \Re\left\{\imath^{x^{(a)}-x^{(b)}+1-T\left(e(y_{j\oplus\nu}^{(a)},y_j^{(b)},\mu)\right)}\right\},$$

for λ even, $\lambda \neq 0$, and

$$\Gamma_3 \;=\; (-2) \sum_{\substack{0\le j\le 4,\\ j\neq 0,\ j\oplus\nu\neq 0}} \Re\left\{\imath^{(3x^{(a)}-x^{(b)})}\right\} \;-\; 2^{k+1} \sum_{\substack{0\le j\le 4,\\ j\neq 0,\ j\oplus\nu\neq 0}} \Re\left\{\imath^{3x^{(a)}-x^{(b)}+1-T\left(f(y_{j\oplus\nu}^{(a)},y_j^{(b)},\mu)\right)}\right\},$$

for λ odd. From our earlier Remark 5, appearing in Section VII, it follows that at least one summand in the three-term sum

$$\sum_{\substack{0\le j\le 4,\\ j\neq 0,\ j\oplus\nu\neq 0}} \Re\left\{\imath^{x^{(a)}-x^{(b)}+1-T\left(e(y_{j\oplus\nu}^{(a)},y_j^{(b)},\mu)\right)}\right\}$$

for the case λ even, $\lambda \neq 0$ is zero. It follows then that

$$\Gamma_3 \;\;\le\;\; 2 + 2(2^{k+1}) \;=\; 6 + 2^{k+2},$$

as desired. Similarly, at least one summand in the three-term sum

$$\sum_{\substack{0\le j\le 4,\\ j\neq 0,\ j\oplus\nu\neq 0}} \Re\left\{\imath^{3x^{(a)}-x^{(b)}+1-T\left(f(y_{j\oplus\nu}^{(a)},y_j^{(b)},\mu)\right)}\right\}$$

has the value zero for the case λ odd, so once again, we obtain the same upper bound $\Gamma_3 \le 6 + 2^{k+2}$.

Remark 8 (Admissible Cyclic Shifts)**.** *We note that operation* 1 *above permits cyclic shifting each sequence* $\{J_t^{(a)})\}$ *belonging to Family* $\mathcal{J}_{\text{NAV}}$ *by an arbitrary cyclic shift. Operation* 4 *permits constituent sequence* $K_o^{(a)}(t)$

to be cyclically shifted prior to interleaving by an amount that is different from the cyclic shift applied to the remaining 4 *sequences* $\{K_j^{(a)}(t)\}, j = 1, 2, 3, 4\}$. *It follows from this that symbol balance and even-correlation bound* $\Omega_{\max}$ *remain unchanged if we apply cyclic shifts* $\{\lambda_j^{(a)}, j \in [5]\}$ *to the constituent sequences* $\Big\{ \{K_j^{(a)}(t)\},\ j \in [5]\Big\}$, *prior to interleaving, that satisfy*

$$\lambda_i^{(a)} \;\; = \;\; \lambda_j^{(a)},\ i, j \in \{1, 2, 3, 4\}.$$

Construction 3 (Family $\mathcal{J}_{\text{NAV}}$). *Let* $m = 10$ *and let* β *be an element of* $\mathbb{R}_{4^m}$ *having order* $n = 2^m - 1 = 2^{10} - 1$. *Let* (H, W) *be an admissible pair of subspaces as described in Section V-B and let* $Y(H, W)$ *be an admissible parameter matrix as defined in Section V-C. Let* $y_j^{(a)}$ *denote the entry in the* a*th row,* $a \in [M]$*, and* j*th column,* $j \in [5]$*, of* $Y(H, W)$. *Let* $\{\epsilon_j^{(a)} \mid a \in [M], j \in [5]\}$ *be a collection of flipping factors as defined in* (74)*. For* $x \in \{0, 1\} \subseteq \mathbb{Z}_4$*,* $y \in H$*, we define the sequence*

$$K(x, y, t) \;\; := \;\; \mathit{MSB}\left\{3^t \left[x + T([1 + 2y]\beta^t)\right]\right\},\ t \in [2n].$$

Then the IZ4 Family $\mathcal{J}_{\mathit{NAV}}$*, is a family of* $M = 170$ *binary sequences, each having period* $10n = 10230$*. The* a*-th sequence* $\{J^{(a)}(t)\}$*,* $a \in [M]$*, in the family is obtained by CRT-based interleaving of the* 5 $\mathbb{Z}_4$*-linear sequences* $\Big\{\{K(x^{(a)},\ y_j^{(a)},\ \ell + \lambda_j^{(a)})\ +\ \epsilon_j^{(a)}\}\Big\}_{j=0}^{4}$*, where, the parameters*

$$\Big\{x^{(a)},\ \big(y_j^{(a)}, j \in [5]\big),\ \big(\lambda_j^{(a)}, j \in [5]\big)\ \big(\epsilon_j^{(a)}, j \in [5]\big)\Big\}$$

satisfy the following requirements:

a)

$$x^{(a)} \;\; = \;\; \begin{cases} 0, & a \in [M/2], \\ 1, & M/2 + 1 \le a \le (M - 1), \end{cases}$$

b) $\lambda_i^{(a)} = \lambda_j^{(a)}$ *for all* $a \in [M]$*,* $1 \le i, j \le 4$*,*

c) the FF $\big(\epsilon_j^{(a)}, j \in [5]\big)$*,* $a \in [M]$*, are chosen in such a manner that each sequence* $\{J^{(a)}(t)\}$*,* $a \in [M]$*, has symbol balance to within* 2*,*

d) the list of permissible operations given above is used to ensure that

- *there exists a pairing*

  $$\{(a_i, b_i) \mid a_i, b_i \in [M],\ i \in [M/2]\}$$

  of parameters such that for each $i \in [M/2]$*, the corresponding pair of sequences* $\big(\{J^{(a_i)}(t)\}, \{J^{(b_i)}(t)\}\big)$ *are orthogonal when in-phase, i.e.,*

  $$\sum_{t=0}^{N-1} (-1)^{J^{(a_i)}(t) + J^{(b_i)}(t)} \;\; = \;\; 0,$$

  and further that

- *Family* $\mathcal{J}_{\mathit{NAV}}$ *has low values of odd-correlation parameters* $\Omega_{a,\max}^{(\mathit{odd})}$ *and* $\Omega_{c,\max}^{(\mathit{odd})}$*.*

Table III lists the even and odd correlation, symbol balance and orthogonal-pairs properties of an example of Construction 3.

X. Coupled Binary Shift-Register Implementation

The IZ4 sequence family $\mathcal{J}_{\text{NAV}}$ having period $L = 10230$ and size $M = 170$, can be simply generated using a pair of coupled 55-bit binary shift registers (SR) along with a 5-bit cycling SR that carries out the flipping operation.

Let an index $a \in [M]$ be fixed. For simplicity, we will write $\{J(t)\}$, $\{K_j(t)$, (x, y_j) and ϵ_j in place of $\{J^{(a)}(t)\}$, $\{K_j^{(a)}(t)\}$, $(x^{(a)}, y_j^{(a)})$ and $\epsilon_j^{(a)}$ respectively. Since interleaving is carried out based on the CRT, we have that

$$J(t) \;\; = \;\; K_j(\ell + \lambda_j)\ + \epsilon_j,$$

where λ_j is the cyclic shift imparted to the jth interleaved sequence and where

$$\ell \;=\; t \pmod{2n}, \quad \text{and} \quad j = t \pmod{5}.$$

Let the sequence $\{R(t)\}$ be defined by

$$R(t) \;=\; K_j(\ell + \lambda_j),$$

so that

$$J(t) \;=\; R(t) + \epsilon_j, \text{ where } j = t \pmod{5}.$$

We focus first on the implementation of the sequence $\{R(t)\}$. The flipping factors $\{\epsilon_j\}$ will be taken into account at a later stage. It follows that for $0 \le j \le 4$, we have

$$\begin{aligned} R(5t+j) &= K_j\Big(5t + j + \lambda_j \pmod{2n}\Big) \\ &= \text{MSB}\left\{3^{5t+j+\lambda_j}\left[x \;+\; T\big(\beta^{5t+j+\lambda_j}[1+2y_j]\big)\right]\right\}. \end{aligned}$$

Set

$$\eta = 3\beta, \qquad \gamma_j = \eta^{j+\lambda_j}[1+2y_j], \qquad u_j = x3^{j+\lambda_j}.$$

Then we can write

$$R(5t+j) \;=\; \text{MSB}\left\{u_j 3^{5t} \;+\; T\left(\gamma_j \eta^{5t}\right)\right\}.$$

Next, setting

$$\begin{aligned} \varphi &= \eta^5 \;=\; 3\beta^5, \\ Q_j(t) &= T(\gamma_j \varphi^t), \\ P_j(t) &= u_j 3^{5t} \;=\; u_j 3^t, \\ R_j(t) &= Q_j(t) + P_j(t), \end{aligned}$$

we obtain

$$R(5t+j) \;=\; \text{MSB}\left\{P_j(t) + Q_j(t)\right\}.$$

We now seek to identify the least-degree linear recursion satisfied by the sum sequence $\{P_j(t) + Q_j(t)\}$. Let $f(x) = \sum_{k=0}^{10} f_k x^k$ be the minimum polynomial of β^5 over $\mathbb{Z}_4$. Then we have that

$$\sum_{k=0}^{10} f_k 3^{5k}(3\beta)^{5k} \;=\; 0 \implies \sum_{k=0}^{10} f_k 3^k \varphi^k \;=\; 0.$$

It follows that

$$g(x) \;=\; \sum_{k=0}^{10} \underbrace{f_k 3^k}_{g_k} x^k,$$

is the minimum polynomial of $\varphi = 3\beta^5$. We have

$$P_j(t+1) + P_j(t) \;=\; u_j 3^t(3+1) \;=\; 0.$$

Thus the characteristic polynomial of the sequence $\{P_j(t)\}$ is $(x+1)$. It follows that the characteristic polynomial of the sum sequence

$$R_j(t) \;=\; Q_j(t) + P_j(t)$$

is given by $(x+1)g(x)$. When α has minimum polynomial $x^{10} + x^3 + 1$, it turns out that the minimum polynomial $m_{\alpha^5}(x)$ of α^5 over $\mathbb{Z}_2$ is given by

$$m_{\alpha^5}(x) \;=\; x^{10} + x^8 + x^3 + x^2 + 1.$$

Employing Graeffe's root-squaring method to lift $m_{\alpha^5}(x)$, one obtains the minimum polynomial $f(x)$ of β^5 over $\mathbb{Z}_4$:

$$\begin{aligned} f(x^2) &= (x^{10} + x^8 + x^2 + 1)^2 - x^6, \\ &= x^{20} + 2x^{18} + x^{16} + 2x^{12} + 2x^8 + 3x^6 + x^4 + 2x^2 + 1 \\ \text{thus} \quad f(x) &= x^{10} + 2x^9 + x^8 + 2x^6 + 2x^4 + 3x^3 + x^2 + 2x + 1. \end{aligned}$$

We have

$$g(x) = \sum_{k=0}^{10} f_k 3^k x^k.$$

Thus:

$$g(x) = x^{10} + 2x^9 + x^8 + 2x^6 + 2x^4 + x^3 + x^2 + 2x + 1.$$

We have

$$\begin{aligned} h(x) &= (1+x)g(x) \\ &= x^{11} + 3x^{10} + 3x^9 + x^8 + 2x^7 + 2x^6 + 2x^5 + 3x^4 + 2x^3 + 3x^2 + 3x + 1. \end{aligned}$$

This leads to the recursion:

$$\begin{aligned} R_j(t+11) &= R_j(t+10) + R_j(t+9) + 3R_j(t+8) + 2R_j(t+7) \\ &\quad +2R_j(t+6) + 2R_j(t+5) + R_j(t+4) + 2R_j(t+3) + R_j(t+2) + R_j(t+1) + 3R_j(t). \end{aligned}$$

Since each of the 5 interleaved sequences satisfies this recursion, we have that the interleaved sequence $R(t)$ satisfies the recursion:

$$\begin{aligned} R(t+55) &= R(t+50) + R(t+45) + 3R(t+40) + 2R(t+35) \\ &\quad +2R(t+30) + 2R(t+25) + R(t+20) + 2R(t+15) + R(t+10) + R(t+5) + 3R(t). \end{aligned}$$

Let

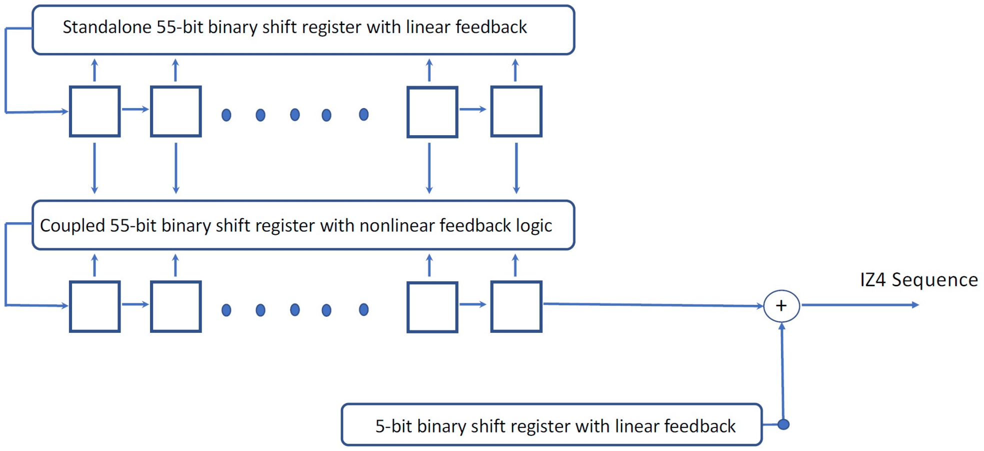

Standalone 55-bit binary shift register with linear feedback
Coupled 55-bit binary shift register with nonlinear feedback logic
+
IZ4 Sequence
5-bit binary shift register with linear feedback

Figure 8: Generating sequences in Family $\mathcal{J}_{\text{NAV}}$ using a pair of coupled 55-bit shift registers and a 5-bit pure cyclic shift register. The upper register generates the LSB sequence $\{R_0(t)\}$ and the middle SR generates the sequence $\{R_1(t)\}$. Different sequences are generated by changing the initial conditions accordingly.

$$R(t) = R_0(t) + 2R_1(t), \quad \text{all } t.$$

Then, taken modulo 2, this gives the following recursion for $\{R_0(t)\}$:

$$\begin{aligned} R_0(t+55) &= R_0(t+50)+R_0(t+45)+R_0(t+40) \\ &\quad +R_0(t+20)+R_0(t+10)+R_0(t+5)+R_0(t) \end{aligned}$$

The recursion for $\{R_1(t)\}$ takes on the nonlinear form:

$$\begin{aligned} R_1(t+55) &= \big(R_1(t+50)+R_1(t+45)+R_1(t+40)+R_1(t+20)+R_1(t+10)+R_1(t+5)+R_1(t)\big) \\ &\quad + \big(R_0(t+40)+R_0(t+35)+R_0(t+30)+R_0(t+25)+R_0(t+15)+R_0(t)\big) \\ &\quad \sigma_2\big(R_0(t+50),R_0(t+45),R_0(t+40),R_0(t+20),R_0(t+10),R_0(t+5),R_0(t)\big). \end{aligned}$$

where the second elementary-symmetric function $\sigma_2(a,b,c,d,e,f,g)$ is the sum of all possible products taken 2 at a time:

$$\begin{aligned} \sigma_2(a,b,c,d,e,f,g) &= ab+ac+ad+ae+af+ag+bc+bd+be+bf+bg+ \\ &\quad cd+ce+cf+cg+de+df+dg+ef+eg+fg. \end{aligned}$$

From this we see that it is possible to generate the sequence $\{R(t)\}$ using a pair of coupled binary SR. A simple cycling SR can be used to account of the presence of the FF:

$$J(t) \;=\; R(t)+\epsilon_j, \text{ where } j=t \pmod 5.$$

XI. Construction of Additional families Obtained by Adopting the Same S-I-F Approach

The S-I-F approach can be used to construct additional families of low-correlation binary sequences having length of the form $2\ell(2^m-1)$ for ℓ odd, $\ell \geq 7$ for m such that $(2^m-1,\ell)=1$. We illustrate in Section XI-A with the case $\ell=7$. The same general approach can also be used to construct families of low-correlation quaternary sequences having period of the form $\ell(2^m-1)$, once again for m such that $(\ell,2^m-1)=1$. Examples with $\ell=5,7$ are provided below in Sections XI-B and Section XI-C respectively.

A. A Binary Sequence Family Having Period $14(2^m-1)$

To ensure that $(7,2^m-1)=1$ for $m=2k$ even, it can be verified that we must have $m=2,4 \pmod 6$. The S-I-F approach can be applied to construct a family of binary sequences having size $M=\frac{2^m}{8}=2^{m-3}$, maximum correlation upper bounded by the quantity:

$$\Omega_{\max} \;\leq\; 10(2^k)+14,$$

and symbol balance to within 2. Note that naive interleaving would result in a weaker correlation bound of $14(2^k+1)$. Since the construction approach is very similar to that used in the construction of families $\mathcal{J}_{5,\text{LEC}}$, $\mathcal{J}_{5,\text{BAL}}$, we only provide a sketch of the construction. The starting point is once again, the sequence family

$$\mathcal{K} \;=\; \left\{\{K(x,y,t)\}_{t=0}^{2n-1} \mid x\in\{0,1\}, y\in H\right\},$$

where $K(x,t)$ is as defined in (15) and where H as before, is a subspace of $\mathbb{F}_{2^m}$ of dimension $(m-1)$ that does not contain 1. As before, the construction of Family $\mathcal{J}_{7,\text{LEC}}$ presented here will be such that all of the 7 sequences from $\mathcal{K}$ employed in the construction of a single sequence in Family $\mathcal{J}_{7,\text{LEC}}$ will share the same value of parameter x, either $x=0$ or $x=1$. Again, the Family $\mathcal{J}_{7,\text{LEC}}$ will be constructed in such a manner that $M/2$ sequences in $\mathcal{J}_{7,\text{LEC}}$ are associated to parameter $x=0$ and an equal number, $M/2$, to parameter $x=1$. To construct this family we apply an admissible parameter matrix $Y(H,W)$. While H is unchanged, the subspace W is however, different and chosen in this case to be a three-dimensional subspace of H given by

$$W \;=\; \langle\gamma_0,\gamma_1,\gamma_2\rangle \;=\; \{0,\gamma_0,\gamma_1,\gamma_0+\gamma_1,\gamma_2,\gamma_0+\gamma_2,\gamma_1+\gamma_2\},$$

where $\{\gamma_i\}_{i=0}^{2}$ are selected such that $\text{tr}(\gamma_i)=1,\ i=0,1,2$. Since W is a subgroup of H under modulo-2 addition, the set H can be partitioned as the disjoint union of 2^{m-4} cosets of W. Let $\{g_a\}_{a=0}^{2^{m-4}-1}$ and $\{h_a\}_{a=0}^{2^{m-4}-1}$ be two sets of coset representatives for the cosets of W in H. We set

$$x^{(a)} \;=\; \begin{cases} 0, & a\in[M/2], \\ 1, & M/2\leq a\leq(M-1), \end{cases}$$

and associate the coset representatives $\{g_a\}$ and $\{h_a\}$ with $\mathbb{Z}_4$-linear sequences having parameters $x^{(a)} = 0$ and $x^{(a)} = 1$ respectively. We do this by selecting the coset representatives $\{g_a\}$ and $\{h_a\}$ such that

$$\begin{aligned} \mathrm{tr}(g_a) + k + x^{(a)} &= \mathrm{tr}(g_a) + k \ = \ 0 \mod 2, \quad 0 \le a \le M/2 - 1, && (80) \\ \mathrm{tr}(h_a) + k + x^{(a+M/2)} &= \mathrm{tr}(h_a) + k + 1 \ = \ 0 \mod 2, \quad 0 \le a \le M/2 - 1. && (81) \end{aligned}$$

This can always be done. This selection will be used to ensure that the sequences have symbol balance to within 2. Next, for $0 \le a \le M/2 - 1$, we set:

$$\begin{aligned} \big(y_j^{(a)}, j = 0, 1, \cdots, 6\big) &= \big(g_a, g_a + \gamma_0, g_a + \gamma_1, g_a + \gamma_0 + \gamma_1, g_a + \gamma_2, g_a + \gamma_0 + \gamma_2, g_a + \gamma_1 + \gamma_2\big), \\ \big(y_j^{(a+M/2)}, j = 0, 1, \cdots, 6\big) &= \big(h_a, h_a + \gamma_0, h_a + \gamma_1, h_a + \gamma_0 + \gamma_1, h_a + \gamma_2, h_a + \gamma_0 + \gamma_2, h_a + \gamma_1 + \gamma_2\big). \end{aligned}$$

a) Even-Correlation Properties: The upper bound on correlation can be established by setting up the sum-matrix (see Table VIII) S for this case. The (j, k)th entry of S is given by $y_j^{(b)} + y_k^{(a)}$. It follows that each entry in the table is of the form $\Delta + u$ where $\Delta = y_0^{(a)} + y_0^{(b)}$ and u is a linear combination of the $\gamma_i, i = 0, 1, 2$. The summand Δ has been omitted for clarity and the table only displays the corresponding value of u. The boxed entries illustrate the sum-constant, trace-different property along an example wrap-around diagonal. The sum-constant, trace-different property in this case has the property this time, that every parallel diagonal has *two* sets of elements satisfying the sum-constant, trace-different property. Using this it is straightforward to verify the correlation bound

Table VIII: The sum-matrix S whose (j, k)th entry is given by $y_j^{(b)} + y_k^{(a)}$.

$\mathrm{tr}(\cdot)$	0	1	1	0	1	0	0
$y_j^{(b)}/y_k^{(a)}$	0	γ_0	γ_1	$\gamma_0+\gamma_1$	γ_2	$\gamma_0+\gamma_2$	$\gamma_1+\gamma_2$
0	0	γ_0	γ_1	$\gamma_0+\gamma_1$	$\boxed{\gamma_2}$	$\gamma_0+\gamma_2$	$\gamma_1+\gamma_2$
γ_0	γ_0	0	$\gamma_0+\gamma_1$	γ_1	$\gamma_0+\gamma_2$	$\boxed{\gamma_2}$	$\gamma_0+\gamma_1+\gamma_2$
γ_1	γ_1	$\gamma_0+\gamma_1$	0	γ_0	$\gamma_1+\gamma_2$	$\gamma_0+\gamma_1+\gamma_2$	γ_2
$\gamma_0+\gamma_1$	$\gamma_0+\gamma_1$	γ_1	γ_0	0	$\gamma_0+\gamma_1+\gamma_2$	$\gamma_1+\gamma_2$	$\gamma_0+\gamma_2$
γ_2	γ_2	$\boxed{\gamma_0+\gamma_2}$	$\gamma_1+\gamma_2$	$\gamma_0+\gamma_1+\gamma_2$	0	γ_0	γ_1
$\gamma_0+\gamma_2$	$\gamma_0+\gamma_2$	γ_2	$\gamma_0+\gamma_1+\gamma_2$	$\gamma_1+\gamma_2$	γ_0	0	$\gamma_0+\gamma_1$
$\gamma_1+\gamma_2$	$\gamma_1+\gamma_2$	$\gamma_0+\gamma_1+\gamma_2$	γ_2	$\boxed{\gamma_0+\gamma_2}$	γ_1	$\gamma_0+\gamma_1$	0

$$\Omega_{\max} \ \le \ 2(5(2^k) + 7) \ = \ 10(2^k) + 14.$$

This has been experimentally verified for $m = 10, k = 5$, corresponding to sequence length 14322, when the above bound evaluates to 334.

b) Balance Property: The expression for symbol balance in the presence of flipping factors $\{\epsilon_j \in \{0, 1\}\}_{j=0}^{6}$ is given by:

$$\begin{aligned} \sum_{t=0}^{14n-1} (-1)^{J^{(a)}(t)} &= \sum_{j=0}^{6} \sum_{t=0}^{2n-1} (-1)^{K\left(x^{(a)},\ y_j^{(a)}, t\right) \ + \ \epsilon_j^{(a)}}, \\ &= (-2) \sum_{j=0}^{6} (-1)^{\epsilon_j^{(a)}} \Re\{\imath^{x^{(a)}}\} - 2^{k+1} \sum_{j=0}^{6} (-1)^{\epsilon_j^{(a)}} \Re\{\imath^{x^{(a)} + k - T(y_j^{(a)})}\}. \end{aligned}$$

Our choice of coset leaders as in (80), (81), has ensured that for each $0 \le a \le M - 1$, there are exactly three values of index $j, 0 \le j \le 6$, for which the trace condition

$$\mathrm{tr}(y_j^{(a)}) \ = \ (x^{(a)} + k + 1),$$

is satisfied. For these three values of j, the term $\Re\left\{\imath^{x^{(a)}+k-T(y_j^{(a)})}\right\}$ evaluates to zero. Thus in the sum,

$$\sum_{j=0}^{6}(-1)^{\epsilon_j^{(a)}}\Re\{\imath^{x^{(a)}+k-T(y_j^{(a)})}\},$$

exactly four terms survive, and the corresponding flipping factors can be used to ensure that this sum equals zero. The remaining three flipping factors can be used to ensure that symbol balance to within 2 is achieved.

B. A Quaternary Sequence Family Having Period $5(2^m-1)$

By adopting the same S-I-F approach as above, but interleaving this time, quaternary Family A sequences [13], [33], [34] in place of $\mathbb{Z}_4$-linear sequences, it is possible to construct families of low-correlation, quaternary sequences having period $5(2^m-1)$ and $(7(2^m-1)$. We deal with the case when the period is $5(2^m-1)$ in the present subsection, and period $7(2^m-1)$ in the subsection following. Here again, the selection of the specific sequences to be interleaved is guided by the closed-form expression appearing in Theorem 2 for an exponential sum over the Galois ring.

a) Quaternary Family $\mathcal{A}$: Family $\mathcal{A}$ is the family of (2^m+1) quaternary sequences of period $n=2^m-1$ given by

$$\mathcal{A} \;\; = \;\; \left\{\{T([1+2y]\alpha^t)\} \mid y \in \mathcal{T}_m\right\} \;\cup\; \{2T(\alpha^t)\}.$$

The construction we present in this subsection assumes that $m=2k=2 \pmod 4$. Our construction will not make use of the sequence $\{2T(\alpha^t)\}$, so we will work with the smaller (by one) family $\mathcal{A}^*$ defined by

$$\mathcal{A}^* \;\; = \;\; \{\{Q(y,t)\} \mid y \in \mathcal{T}_m\},$$

where by a slight abuse in notation, we define [2]

$$Q(y,t) \;\; := \;\; T([1+2y]\beta^t), \;\; y \in \mathcal{T}_m, \;\; t \in [n].$$

Let W be a two-dimensional subspace of $\mathbb{F}_{2^m}$ as introduced in Section V:

$$W \;\; = \;\; \{0,\gamma_0,\gamma_1,\gamma_0+\gamma_1\},$$

where $\text{tr}(\gamma_0)=1$, $\text{tr}(\gamma_1)=1$. The 2^{m-2} cosets of W in $\mathbb{F}_{2^m}$ partition $\mathbb{F}_{2^m}$. Set

$$M = \lfloor\frac{2^m}{5}\rfloor.$$

Let $\{u_a\}_{a=0}^{2^{m-2}-1}$ be an ordered set of 2^{m-2} coset representatives of the cosets of W in $\mathbb{F}_{2^m}$. Let Y be an $(M\times 5)$ array, defined as follows. The (a,j)th element $0\le a\le M-1$, $0\le j\le 4$, of Y will be denoted by $y_j^{(a)}$. We set

$$(y_1^{(a)},y_2^{(a)},y_3^{(a)},y_4^{(a)}) \;\; = \;\; (u_a,u_a+\gamma_0,u_a+\gamma_1,u_a+\gamma_0+\gamma_1), \quad a\in[M].$$

The cosets of W associated to the subset of coset representatives $\{u_a\}_{a=M}^{2^{m-2}-1}$ contain a total of (2^m-4M) elements. We select an arbitrary subset of size M from the set

$$\{u_a+W \mid M\le a\le 2^{m-2}-1\},$$

order them in some arbitrary fashion, and assign to these M elements, the labels $\{y_0^{(a)} \mid 0\le a\le (M-1)\}$. This is possible since

$$M=\lfloor\frac{2^m}{5}\rfloor \;\;\Rightarrow\;\; 2^m-4M \;\ge\; M.$$

This completes description of the matrix Y. We now define Family $\mathcal{Q}_{5,\text{LEC}}$ as follows. The ath sequence $\{J_{\text{Q5}}^{(a)}(t)\}$, $a\in[M]$ of Family $\mathcal{Q}_{5,\text{LEC}}$ is obtained by CRT-based interleaving the 5 quaternary sequences:

$$\{\{Q(y_j^{(a)},\ell)\} \mid j=0,1,2,3,4\}.$$

Thus we have

$$J_{\text{Q5}}^{(a)}(t) \;\; = \;\; Q(y_j^{(a)},\ell), \quad j=t \pmod 5, \quad \ell=t \pmod n.$$

[2] The function $Q(y,t)$ introduced in the present subsection is the same as the function $Q(x,y,t)$ introduced earlier in Section III with parameter $x=0$.

b) Even-Correlation Properties: The correlation $\rho_{ab}(\tau)$ between two sequences in Family $\mathcal{Q}_{5,\text{LEC}}$ at shift τ with

$$\nu = \tau \pmod 5 \qquad \lambda = \tau \pmod n$$

is defined by

$$\begin{aligned}
\rho_{ab}(\tau) \;&:=\; \sum_{t=0}^{5n-1} \imath^{J_{\text{Q5}}^{(a)}(t+\tau)-J_{\text{Q5}}^{(b)}(t)}, \\
&=\; \sum_{j=0}^{4}\sum_{\ell=0}^{n-1} \imath^{Q(y_{j\oplus\nu}^{(a)},\ell+\lambda)-Q(y_j^{(b)},\ell)}, \\
&=\; \sum_{j=0}^{4}\left\{-1 \;-\; 2^k \imath^{k-T(e(y_{j\oplus\nu}^{(a)},\, y_j^{(b)},\, \lambda))}\right\}, \\
&=\; -5 - 2^k \left\{\sum_{j=0}^{4} \imath^{k-T(e(y_{j\oplus\nu}^{(a)},\, y_j^{(b)},\, \lambda))}\right\},
\end{aligned}$$

where as before,

$$e(y_{j\oplus\nu}^{(a)}, y_j^{(b)}, \lambda) \;=\; \mu + y_{j\oplus\nu}^{(a)} + \mu^2(y_{j\oplus\nu}^{(a)} + y_j^{(b)}).$$

A sum-matrix table identical to the sum-matrix table appearing in Table VII can be set up here. The same sum-constant, trace-different property holds here as well and ensures that not all the 5 terms

$$\left\{\imath^{k-T(e(y_{j\oplus\nu}^{(a)},\, y_j^{(b)},\, \lambda))}\right\}_{j=0}^{4},$$

are either all 5 real or all 5 imaginary. This results in the upper bound on maximum even-correlation parameter $\Omega_{\max}$ given by

$$\Omega_{\max} \;\leq\; \sqrt{(5 + 4(2^k))^2 + (2^k)^2}.$$

This has been verified through simulation to hold for the case $m = 10$ yielding the value $\Omega_{\max} = 136.795$.

c) Symbol Balance: We define the symbol balance expression for the quaternary sequence $J_{\text{Q5}}^{(a)}(t)$ to be given by

$$\begin{aligned}
\left|\sum_{t=0}^{5n-1} \imath^{J_{\text{Q5}}^{(a)}(t)}\right| \;&=\; \left|\sum_{j=0}^{4}\sum_{\ell=0}^{n-1} \imath^{Q(y_j^{(a)},\ell)}\right|, \\
&=\; \left|\sum_{j=0}^{4}\left\{-1 \;-\; 2^k \imath^{k-T(y_j^{(a)})}\right\}\right|.
\end{aligned}$$

With the inclusion of flipping factors $\{\phi_j\}_{j=0}^4$, $\phi_j \in \{\pm 1\}$ that change the signs of the constituent quaternary sequences that are being interleaved, this changes to

$$\begin{aligned}
\left|\sum_{t=0}^{5n-1} (-1)^{J_{\text{Q5}}^{(a)}(t)}\right| \;&=\; \left|\sum_{j=0}^{4}\left\{-1(-1)^{\phi_j} \;-\; (-1)^{\phi_j} 2^k \imath^{k-T(y_j^{(a)})}\right\}\right|, \\
&=\; \left|-\sum_{j=0}^{4}(-1)^{\phi_j} \;-\; 2^k \imath^k \sum_{j=0}^{4}(-1)^{\phi_j} \imath^{-T(y_j^{(a)})}\right|.
\end{aligned}$$

It is straightforward to verify that the flipping factors do not impact the value of $\Omega_{\max}$. Since the subset $\{y_j^{(a)}, j = 1, 2, 3, 4\}$ forms a subspace, it follows that of the 4 binary trace values

$$T(y_j^{(a)}) \pmod 2 \;=\; \text{tr}((y_j^{(a)}), j = 1, 2, 3, 4,$$

two are equal to 0 and two are equal to 1. Equivalently, two values $\imath^{-T(y_j^{(a)})}$ are real and two are imaginary. Thus by appropriate choice of flipping factors $\{\phi_j, j=1,2,3,4\}$, one can establish that the contribution to symbol balance of the terms corresponding to $j=1,2,3,4$ is zero. By further utilizing the remaining freedom in selecting the flipping factors, one can ensure that each sequence $\{J_{\text{Q5}}^{(a)}(t)\}$ has symbol balance

$$|\sum_{t=0}^{5n-1}(-1)^{J_{\text{Q5}}^{(a)}(t)}| \quad \leq \quad (1+2^k).$$

This has been verified through simulation to hold for the case $m=10$. We use $\mathcal{Q}_{\text{5,BAL}}$ to denote sequence family $\mathcal{Q}_{\text{5,LEC}}$ after the incorporation of flipping factors. Thus the symbol balance of Family $\mathcal{Q}_{\text{5,BAL}}$ is identical to that of Family $\mathcal{A}$ as the symbol balance for Family $\mathcal{A}$ is also given by $(1+2^k)$.

C. A Quaternary Sequence Family Having Period $7(2^m-1)$

By adopting the same S-I-F approach as above, but interleaving this time, 7 quaternary Family $\mathcal{A}^*$ sequences of period 2^m-1 where

$$m \quad = \quad 2 \text{ or } 4 \pmod 6,$$

it is possible to construct families of low-correlation, quaternary sequences having period $(7(2^m-1))$. Let W be a three-dimensional subspace as in Section XI-A given by

$$W \quad = \quad \langle\gamma_0,\gamma_1,\gamma_2\rangle \quad = \quad \{0,\gamma_0,\gamma_1,\gamma_0+\gamma_1,\gamma_2,\gamma_2+\gamma_0,\gamma_2+\gamma_1\},$$

where $\{\gamma_i\}_{i=0}^{2}$ are selected such that $\text{tr}(\gamma_i)=1,\ i=0,1,2$. The 2^{m-3} cosets of W in $\mathbb{F}_{2^m}$ partition $\mathbb{F}_{2^m}$. Set

$$M=2^{m-3}.$$

Let $\{u_a\}_{a=0}^{2^{m-3}-1}$ be an ordered set of 2^{m-3} coset representatives of the cosets of W. Let Y be an $(M\times 7)$ array, defined as follows. The (a,j)th element $0\le a\le M-1$, $0\le j\le 6$, of Y will be denoted by $y_j^{(a)}$. We set

$$(y_0^{(a)},y_1^{(a)},\cdots,y_6^{(a)}) \quad = \quad \big(u_a,u_a+\gamma_0,u_a+\gamma_1,u_a+\gamma_0+\gamma_1,u_a+\gamma_2,u_a+\gamma_2+\gamma_0,u_a+\gamma_2+\gamma_1\big).$$

We now define Family $\mathcal{Q}_{\text{7,LEC}}$ as follows. The ath sequence $\{J_{\text{Q7}}^{(a)}(t)\}$, $a\in[M]$ of Family $\mathcal{Q}_{\text{7,LEC}}$ is obtained by interleaving the 7 quaternary sequences:

$$\{\{Q(y_j^{(a)},\ell)\}\mid j=0,1,2,\cdots,6\}.$$

Thus we have

$$J_{\text{Q7}}^{(a)}(t) \quad = \quad Q(y_j^{(a)},\ell), \quad j=t \pmod 7, \quad \ell=t \pmod n.$$

1) Even-Correlation Properties: The correlation $\rho_{ab}(\tau)$ between two sequences in Family $\mathcal{Q}_{\text{7,LEC}}$ at shift τ with

$$\nu=\tau \pmod 7 \qquad \lambda=\tau \pmod n$$

is given by

$$\begin{aligned}
\rho_{ab}(\tau) \quad &= \quad \sum_{t=0}^{n-1}\imath^{J_{\text{Q7}}^{(a)}(t+\tau)-J_{\text{Q7}}^{(b)}(t)}, \\
&= \quad \sum_{j=0}^{6}\sum_{\ell=0}^{n-1}\imath^{Q(y_{j\oplus\nu}^{(a)},\ell+\lambda)-Q(y_j^{(b)},\ell)}, \\
&= \quad \sum_{j=0}^{6}\left\{-1 \ - \ 2^k\imath^{k-T(e(y_{j\oplus\nu}^{(a)},y_j^{(b)},\lambda))}\right\}, \\
&= \quad -7-2^k\left\{\sum_{j=0}^{6}\imath^{k-T(e(y_{j\oplus\nu}^{(a)},y_j^{(b)},\lambda))}\right\},
\end{aligned}$$

where

$$e(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda) \;=\; \mu + y^{(a)}_{j\oplus\nu} + \mu^{2}(y^{(a)}_{j\oplus\nu} + y^{(b)}_{j}).$$

A sum-matrix table identical to the sum-matrix table appearing in Table VIII can be set up here. The same sum-constant, trace-different property holds here as well and ensures that there are at least two real terms as well as at least two imaginary terms in the set

$$\left\{ \imath^{k-T(e(y^{(a)}_{j\oplus\nu}, y^{(b)}_{j}, \lambda))} \right\}_{j=0}^{6} .$$

This results in the upper bound on maximum even-correlation parameter $\Omega_{\max}$ given by

$$\Omega_{\max} \;\leq\; \sqrt{(7+5(2^{k}))^{2} + (2(2^{k}))^{2}}.$$

This has been verified on MATLAB to hold for the case $m = 10$ yielding the value

$$\Omega_{\max} \;=\; 178.8435.$$

2) Symbol Balance: We define the symbol balance expression for the quaternary sequence $J^{(a)}_{\mathrm{Q7}}(t)$ to be given by

$$\begin{aligned} | \sum_{t=0}^{7n-1} \imath^{J^{(a)}_{\mathrm{Q7}}(t)} | \;&=\; \sum_{j=0}^{6} \sum_{\ell=0}^{n-1} \imath^{Q(y_{j}^{(a)}, \ell)}, \\ &=\; \sum_{j=0}^{6} \left\{ -1 \;-\; 2^{k} \imath^{k-T(y_{j}^{(a)})} \right\}. \end{aligned}$$

With the inclusion of flipping factors $\{\phi_j\}_{j=0}^{6}$, $\phi_j \in \{\pm 1\}$ that change the signs of the constituent quaternary sequences that are being interleaved, this changes to

$$\begin{aligned} | \sum_{t=0}^{7n-1} (-1)^{J^{(a)}_{\mathrm{Q7}}(t)} \;&=\; \sum_{j=0}^{6} \left\{ -1(-1)^{\phi_j} \;-\; (-1)^{\phi_j} 2^{k} \imath^{k-T(y_{j}^{(a)})} \right\}, \\ &=\; -\sum_{j=0}^{6} (-1)^{\phi_j} \;-\; 2^{k} \imath^{k} \sum_{j=0}^{6} (-1)^{\phi_j} \imath^{-T(y_{j}^{(a)})}. \end{aligned}$$

It is straightforward to verify that the flipping factors do not impact the value of $\Omega_{\max}$. Since the subset $\{y_j^{(a)}, j = 0, 1, \cdots, 6\}$ form a subspace, it follows that of the 7 binary trace values

$$T(y_{j}^{(a)}) \pmod 2 \;=\; \mathrm{tr}((y_{j}^{(a)}), j = 1, 2, \cdots, 7$$

three or more are equal to 0 and three or more are equal to 1. Equivalently, three of the 7 values $\imath^{-T(y_j^{(a)})}$ are real and three of them are imaginary. It can be verified that by appropriate choice of flipping factors $\{\phi_j, j = 0, 1, 2, \cdots, 6\}$, one can ensure that each sequence $\{J^{(a)}_{\mathrm{Q7}}(t)\}$ once again, has symbol balance

$$| \sum_{t=0}^{7n-1} (-1)^{J^{(a)}_{\mathrm{Q7}}(t)} | \;\leq\; (1 + 2^{k}),$$

where we note that $n = 2^{m} - 1$ and $m = 2k$. We use $\mathcal{Q}_{7,\mathrm{BAL}}$ to denote sequence family $\mathcal{Q}_{7,\mathrm{LEC}}$ after the incorporation of flipping factors. Thus the symbol balance of Family $\mathcal{Q}_{7,\mathrm{BAL}}$ is identical to that of Family $\mathcal{A}$.

XII. Conclusions

The principal contribution of this paper is the construction of a family $\mathcal{J}_{\text{NAV}}$ of sequences having period 10230, low values of worst-case even and odd-correlation, good symbol balance, and the orthogonal-pairs property. The period and the properties of Family $\mathcal{J}_{\text{NAV}}$, make $\mathcal{J}_{\text{NAV}}$ well-suited to being used as the spreading code family employed in a GNSS setting, to provide satellite-based accurate positioning, time and velocity information. As can be seen from the entries in Table III, the family compares well with existing GNSS spreading code families, including having worst-case even correlation magnitude that is lower by 4.5dB.

The $\mathcal{J}_{\text{NAV}}$ family is constructed using a Select-Interleave-Flip (S-I-F) approach under which $\mathbb{Z}_4$-linear sequences are interleaved using the Chinese Remainder Theorem and then selectively flipped in terms of polarity. Both selection and flipping are guided by the availability of a closed-form expression for an exponential sum over Galois rings. Sequence Family $\mathcal{J}_{\text{NAV}}$ admits a simple, shift-register implementation.

It is shown that the same S-I-F approach can be made more generally, to yield low-correlation binary sequences having period of the form $10(2^m-1)$ for $m = 2 \pmod 4$ and $14(2^m-1)$ for $m = 2, 4 \pmod 6$ having asymptotic (nontrivial) even-correlation magnitudes upper bounded by $2.53\sqrt{L}$ and $2.67\sqrt{L}$ respectively, where L is the sequence period.

By replacing the base $\mathbb{Z}_4$-linear sequence family with quaternary sequence Family $\mathcal{A}$, it is possible to generate using once again, the same S-I-F approach, low-correlation quaternary low-correlation sequence families having period of the form $5(2^m-1)$ for $m = 2 \pmod 4$ and $7(2^m-1)$ for $m = 2, 4 \pmod 6$ and asymptotic (nontrivial) even-correlation magnitudes upper bounded by $1.84\sqrt{L}$ and $2.04\sqrt{L}$ respectively. The quaternary sequence families have symbol balance that is on par with that of Family $\mathcal{A}$.

Acknowledgement

This work could not have been carried out without the support and encouragement of Distinguished Scientists from the Indian Space Research Organization (ISRO), Senior Faculty at the Indian Institute of Science (IISc) and Senior Faculty and Staff at IISc's Intellectual Property and Technology Licensing (IPTeL) Centre. We would also like to thank the Associate Editor and the reviewers for their helpful comments which has resulted in an improved manuscript.

References

[1] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," in *IEEE Transactions on Information Theory*, vol. 13, no. 4, pp. 619-621, October 1967.

[2] R. Gold, “Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Transactions on Information Theory*, vol. 14, n0. 1, pp.154-156, January 1968.

[3] T. Kasami, “Weight distribution formula for some class of cyclic codes,” Coordinated Sci. Lab., Univ. of Illinois, Urbana, Tech. Rep. R-285, pp. 1–32, 1966.

[4] T. Kasami, “Weight distribution of Bose-Chaudhuri-Hocquenghem codes in *Combinatorial Mathematics and its Applications*, Chapel Hill, NC: University of North Carolina Press pp. 335-357, 1969.

[5] B. R. McDonald, *Finite rings with identity*, vol. 28, Marcel Dekker Incorporated, 1974.

[6] F. J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland, 1977.

[7] J. Olsen, R. Scholtz and L. Welch, “Bent-function sequences,” in *IEEE Transactions on Information Theory*, vol. 28, no. 6, pp. 858-864, November 1982.

[8] Jong-Seon No and P. V. Kumar, “A new family of binary pseudorandom sequences having optimal periodic correlation properties and larger linear span,” in *IEEE Transactions on Information Theory*, vol. 35, no. 2, pp. 371-379, March 1989.

[9] A. A. Nechaev, “Kerdock code in a cyclic form,” *Disc. Math. Appl.*, vol. 1, no. 4, pp.365-384, 1991.

[10] S. Boztas and P. V. Kumar “Binary sequences with Gold-like correlation but larger linear span”, *IEEE Transactions on Information Theory*, vol. 40, no. 2, pp. 532-537, March 1994.

[11] A. Barg, “Two families of low-correlated binary sequences,” *Applicable Algebra in Engineering, Communication and Computing*, vol. 7, pp. 433-437, 1996.

[12] P. Udaya and M. U. Siddiqi, “Optimal biphase sequences with larger linear complexity derived from sequences over Z_4,” *IEEE Transactions on Information Theory*, vol. 42, no. 1, pp. 206-216 Jan. 1996.

[13] T. Helleseth and P. V. Kumar, “Sequences with low correlation”, chapter in *Handbook of Coding Theory*, edited by V. Pless and C. Huffman, Elsevier Science Publishers, pp. 1765-1853, 1998.

[14] Xiaohu Tang, Parampalli Udaya and Pingzhi Fan, “Generalized binary Udaya–Siddiqi sequences,”, *IEEE Transactions on Information Theory* , vol 53, no. 3, pp. 1225-1230, March 2007.

[15] A. R. Hammons, Jr., P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solè, “The Z_4-linearity of $\mathbb{Z}_4$-linear Preparata, Goethals and related codes,” *IEEE Transactions on Information Theory*, vol. 40, no. 2, pp. 301-319, March 1994.

[16] Guang Gong, “New designs for signal sets with low cross correlation, balance property, and large linear span: $GF(p)$ Case,” *IEEE Transactions on Information Theory*, vol. 48, no. 11, Nov. 2002, pp. 2847-2867, Nov. 2002. .

[17] K. G. Paterson, “Binary sequence sets with favorable correlations from difference sets and MDS codes,” *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 172-180, January 1998. pp. 172–180.

[18] J.J. Rushanan, “Weil sequences: A family of binary sequences with good correlation properties,” *IEEE IEEE International Symposium on Information Theory*, pp. 1648-1652, July 9–14, 2006.

[19] J. Rushanan, “The spreading and overlay codes for the L1C signal,” *Journal of Navigation*, vol. 54, no. 1 pp. 43-51, 2007.

[20] J.J. Rushanan, “Spreading code derived from Weil sequences,” U.S. Patent no. US 7,511,637, Mar 31, 2009.

[21] Zhang Guohua and Zhou Quan, “Pseudonoise codes constructed by Legendre sequence,” *Electronics Letters*, vol. 38, no. 8, pp. 376–377, 2002.

[22] Xingli Sun, “Performance analysis of BDS-3 B1C and GPS L1C data/pilot component pseudo random noise codes,” *Journal of Applied Geodesy*, vol. 12, no. 4, pp. 267-278, 2018.

[23] P. V . Kumar, T. Helleseth and A. R. Calderbank, A. R. Hammons, Jr., “Large families of quaternary sequences with low correlation,” *IEEE Transactions on Information Theory*, vol. 42 no. 2, pp. 579-592, March 1996.

[24] China Satellite Navigation Office, *BeiDou Navigation Satellite System Signal in Space Interface Control Document*, Open Service Signal B1C (Version 1.0), December 2017.

[25] Satellite Navigation Programme, U. R. Rao Satellite Centre, Indian Space Research Organization, *NavIC Signal in Space ICD for Standard Positioning Service in L1 Frequency*, version 1.0, Bangalore October 2022.

[26] S. Mishra, D. Dharmappa (joint work with P. V. Kumar), “Novel Interleaved Z_4-Linear PRN Codes for NavIC L1-SPS,” *Fifteenth Meeting of the UN International Committee on Global Navigation Satellite Systems (ICG-15)*, Vienna, 29 September, 2021.

[27] P. V. Kumar, D. Dharmappa and S. Mishra, “Interleaved $\mathbb{Z}_4$-Linear Sequences with Improved Correlation for Satellite Navigation,” *2021 IEEE International Symposium on Information Theory*, Melbourne, Australia, pp. 1665-1670, 2021.

[28] P. Vijay Kumar, Dileep Dharmappa and Sugandh Mishra, “Method and system for generating spreading codes based on interleaved Z4-linear sequences for navigation systems,” Indian Patent No. 383332, granted November 30, 2021.

[29] P. Vijay Kumar, Dileep Dharmappa and Sugandh Mishra, “Interleaved $\mathbb{Z}_4$-Linear Sequences With Low Correlation for Global Navigation Satellite Systems,” https://ece.iisc.ac.in/~pvkece/.

[30] L. R. Welch, “Lower bounds on the minimum correlation of signals,” *IEEE Transactions on Information Theory*, vol. 20, no. 3, pp. 397-399, 1974.

[31] Stefan Wallner, “Navigation system using spreading codes based on pseudo-random noise sequences,” U.S. patent No. US 10,088,573, October 2, 2018.

[32] Navstar GPS Space Segment/User Segment L1C Interfaces, *Interface specification IS-GPS-800D*, September 24, 2013.

[33] P. Solé, “A quaternary cyclic code and a family of quadriphase sequences with low correlation properties,” *Coding Theory and Applications, Lecture Notes in Computer Science*, vol. 388, Berlin: Springer-Verlag, pp. 193–201, 1989.

[34] S. Boztaş, R. Hammons, and P. V. Kumar, “4-phase sequences with near-optimum correlation properties,” *IEEE Transactions on Information Theory*, vol. 38, no. 3, pp. 1101-1113, 1992.

[35] P. V. Kumar, T. Helleseth and A. R. Calderbank, “ An upper bound for Weil exponential sums over Galois rings and applications,” *IEEE Transactions on Information Theory*, vol. 41, no. 2, pp. 456-468, March 1995.

[36] K. Yang, T. Helleseth, P. V. Kumar and A. Shanbhag, “On the weight hierarchy of Kerdock codes over $\mathbb{Z}_4$,” *IEEE Transactions on Information Theory* , vol 42, no. 5, pp. 1587-1593, September 1996.

[37] A. Weil, “Sur les courbes algebriques et les varietes qui s’en deduisent,” *Publ. Inst. Math. Univ. Strasbourg* vol. 7, pp.1-85, 1945.

[38] A. Weil, “On Some exponential sums,” *Proc. Nat. Acad. Sci.*, vol. 34, pp.204-207, 1948.

[39] O. Moreno, Z. Zhang, P. V. Kumar and V. Zinoviev, “New constructions of optimal cyclically permutable constant weight codes,” *IEEE Transactions on Information Theory*, vol. 41, no. 2, pp. 448-455, March 1995.

Appendix

A. Galois Rings

a) Basic Irreducible Polynomial over $\mathbb{Z}_4$: For an integer $m \geq 1$, we will use $\mathbb{F}_{2^m}$ to denote a finite field of characteristic 2 and size 2^m. Let $\mathbb{Z}_4$, $\mathbb{Z}_2$ denote the rings of integers modulo 4 and 2 respectively. Let $\mu : \mathbb{Z}_4 \mapsto \mathbb{Z}_2$ denote the modulo-2 reduction map on $\mathbb{Z}_4$, i.e., $\mu(b) = b \pmod 2),\ b \in \mathbb{Z}_4$. Given a polynomial $A(x) = \sum_{i=0}^{d} A_i x^i$ over $\mathbb{Z}_4$, we define $\mu(A)$ to be the polynomial over $\mathbb{F}_2$ given by $\mu(A) = \sum_{i=0}^{d} \mu(A_i) x^i$. If $A(x) \in \mathbb{Z}_4[x]$ is monic and $\mu(A)$ is irreducible, it follows that $A(x)$ is irreducible over $\mathbb{Z}_4$ and we will say that $A(x)$ is a basic irreducible.

Let $f(x)$ be a primitive (irreducible) polynomial over $\mathbb{F}_2$ of degree $m \geq 1$. Let the polynomial $F(x)$ over $\mathbb{Z}_4$ be defined by

$$F(x^2) = (-1)^m f(x)\ f(-x), \tag{82}$$

where on the right, we regard f as a polynomial over $\mathbb{Z}_4$ with $\{0, 1\}$ coefficients. It is straightforward to verify that $\mu(F) = f$ and it follows therefore, that $F(x)$ is a basic irreducible over $\mathbb{Z}_4$. This method of deriving a basic irreducible polynomial over $\mathbb{Z}_4$ starting from a binary irreducible polynomial is known as Graeffe’s root-squaring method.

Example 1. *Let $f(x) = x^{10} + x^3 + 1$. It is known that $f(x)$ is a primitive, binary polynomial of degree $m = 10$. An application of* (82) *gives us*

$$F(x^2) \;=\; (x^{10}+1)^2 - (x^3)^2 \;=\; x^{20} + 2x^{10} + 3x^6 + 1$$

so that

$$F(x) \;=\; x^{10} + 2x^5 + 3x^3 + 1.$$

As we have seen, $\mu(F) = f$. Thus $x^{10} + 2x^5 + 3x^3 + 1$ is an example of a basic irreducible polynomial.

b) Galois Ring Construction: Set $\mathbb{R}_{4^m} = \mathbb{Z}_4[x]/(F(x))$, then $\mathbb{R}_{4^m} \cong \mathbb{Z}_4[\beta]$, where β belongs to some extension ring of $\mathbb{Z}_4$ and satisfies $F(\beta) = 0$. Clearly $\mathbb{R}_{4^m}$ contains 4^m elements and every element z in $\mathbb{R}_{4^m}$ can be uniquely expressed in the form

$$z = \sum_{i=0}^{m-1} z_i \beta^i,\ z_i \in \mathbb{Z}_4.$$

It is also clear that $\mathbb{R}_{4^m}$ is a commutative ring with identity under the usual definitions of addition and multiplication. Rings arising in this manner are Galois Rings (GR) [5].

The modulo-2 mapping μ is a ring homomorphism that maps the elements of $\mathbb{Z}_4[x]/(F(x))$ to the elements of the finite field $\mathbb{F}_{2^m} := \mathbb{Z}_2[x]/(f(x))$ where $f(x) = F(x) \pmod 2$ is the binary primitive polynomial used to derive the basic irreducible $F(x)$. The finite field $\mathbb{F}_{2^m} \cong \mathbb{F}_2[\alpha]$, where α belongs to some extension field of $\mathbb{F}_2$ and satisfies $f(\alpha) = 0$. Clearly, we may assume that the image of β in the GR under the map μ is the element $\alpha = \mu(\beta)$ in the finite field, and we may write $\alpha = \beta \pmod 2$. Then since $f(\alpha) = 0$, α is a primitive element of $\mathbb{F}_{2^m}$ and hence has order n, where $n := 2^m - 1$. It can be verified using (82) that the element β in the GR also has order n.

c) Teichmuller Set: Set

$$\mathcal{T}_m = \{0\} \cup \{1, \beta, \beta^2, \cdots, \beta^{n-1}\}.$$

Since $\mu(\beta^i) = \alpha^i$, it follows that an element in $\mathcal{T}_m$ is uniquely defined by its reduction modulo 2. Every element $(x + 2y),\ x, y \in \mathcal{T}_m$ belongs to $\mathbb{R}_{4^m}$. It can be verified that

$$x_1 + 2y_1 = x_2 + 2y_2 \ \text{ iff } \ x_1 = x_2 \text{ and } y_1 = y_2.$$

Thus every element z in $\mathbb{R}_{4^m}$ has a unique expression of the form

$$z = x + 2y,\ x, y \in \mathcal{T}_m.$$

The set $\mathcal{T}_m$ is commonly referred to as the set of Teichmuller representatives or simply as the Teichmuller set. Given an element $x \in \mathcal{T}_m$, any element of the form

$$y \;=\; x^{2^{m-1}}(1 + 2\theta),$$

satisfies $y^2 = x$, but only one of them, namely $x^{2^{m-1}}$, belongs to $\mathcal{T}_m$. Keeping this in mind, given an element $x \in \mathcal{T}_m$, by $\sqrt{x}$ we will mean the square root $x^{2^{m-1}}$ of x lying in $\mathcal{T}_m$. If

$$(x_1 + 2y_1) + (x_2 + 2y_2) = x + 2y,\ \text{where } x, y, x_i, y_i \in \mathcal{T}_m,$$

then by raising both sides to the 2^mth power, we see that

$$x = x_1 + x_2 + 2\sqrt{x_1 x_2},$$

and consequently that

$$2y \;=\; 2(y_1 + y_2 + \sqrt{x_1 x_2}).$$

A simpler means of identifying x given x_1, x_2 is to simply note that $x = x_1 + x_2 \pmod 2$.

d) Trace Function: The automorphisms of the finite field $\mathbb{F}_2[\alpha]$ are known to form a cyclic group of size m under composition generated by the map:

$$\sigma : \alpha \mapsto \alpha^2.$$

Let $\sigma : \mathbb{R}_{4^m} \mapsto \mathbb{R}_{4^m}$ be defined by

$$\sigma(x + 2y) = x^2 + 2y^2,\ x, y \in \mathcal{T}_m.$$

It can be verified that σ is an automorphism of $\mathbb{R}_{4^m}$. For $b = b_0 + 2b_1$, in $\mathbb{Z}_4$, $b_0, b_1 \in \mathbb{F}_2$,

$$\sigma(b_0 + 2b_1) = b_0^2 + 2b_1^2 = b_0 + 2b_1,$$

and therefore σ fixes $\mathbb{Z}_4$. The maps

$$\sigma^i : x + 2y \mapsto x^{2^i} + 2y^{2^i},\ 0 \leq i \leq m-1$$

represent the set of m automorphisms of $\mathbb{R}_{4^m}$ that fix $\mathbb{Z}_4$. The trace function $T_m : \mathbb{R}_{4^m} \mapsto \mathbb{Z}_4$ is defined by

$$T_m(x + 2y) = \sum_{i=0}^{m-1} \sigma^i(x + 2y) = \sum_{i=0}^{m-1} (x^{2^i} + 2y^{2^i}), x, y \in \mathcal{T}_m.$$

It is straightforward to show that $T_m(\cdot)$ is linear over $\mathbb{Z}_4$, i.e., for $x \in \mathbb{R}_{4^m}$, $a, b \in \mathbb{Z}_4$,

$$T_m(ax + b) \quad = \quad aT_m(x) + b.$$

It can be shown that $T_m(\cdot)$ takes on all values in $\mathbb{Z}_4$ equally often. The reduction modulo 2 of $T_m(\cdot)$ gives us the binary trace function $\mathrm{tr}_m(\cdot) : \mathbb{F}_{2^m} \mapsto \mathbb{F}_2$ of the finite field defined by

$$\mathrm{tr}_k(x) = \sum_{i=0}^{m-1} x^{2^i}, x \in \mathbb{F}_{2^m}.$$

e) An Exponential Sum over Galois Rings: Define the exponential sum

$$\Gamma_m\big([1 + 2\gamma]\big) \quad := \quad \sum_{x \in \mathcal{T}_m} \imath^{T_m([1+2\gamma]x)}$$

Lemma 2.

$$\Gamma_m(1 + 2\gamma) \quad = \quad \imath^{-T_m(\gamma)}\Gamma_m(1).$$

Proof:

$$\Gamma_m(1) \quad = \quad \sum_{x \in \mathcal{T}_m} \imath^{T_m(x)}.$$

Given $x \in \mathcal{T}_m$, let $y \in \mathcal{T}_m$ be such that $x \ = \ (y + \gamma + 2\sqrt{y\gamma})$. Then as x varies over $\mathcal{T}_m$, so does y. We can thus write

$$\begin{aligned} \Gamma_m(1) \quad &= \quad \sum_{y \in \mathcal{T}_m} \imath^{T_m(y+\gamma+2\sqrt{y\gamma})}, \ = \ \imath^{T_m(\gamma)} \sum_{y \in \mathcal{T}_m} \imath^{T_m(y[1+2\gamma])}, \\ &= \quad \imath^{T_m(\gamma)}\Gamma_m([1 + 2\gamma]). \end{aligned}$$

□

Theorem 2 (Closed-Form Expression for Exponential Sum)**.** *[36]*

$$\begin{aligned} \Gamma_m\big([1 + 2\gamma]\big) \quad &= \quad -(-(1 + \imath))^m \imath^{-T_m(\gamma)}, \\ &= \quad -2^k \imath^{k-T_m(\gamma)}, \ \textit{ for } m = 2k. \end{aligned} \tag{83}$$

Proof. From the theory of L-functions of exponential sums, see [35], we have that

$$\Gamma_m(1) \quad = \quad \sum_{x \in \mathcal{T}_m} \imath^{T_m(x)} \quad = \quad -(\Gamma_1(1))^m \quad = \quad -(-[1 + \imath])^m,$$

since

$$\Gamma_1(1) \quad = \quad \sum_{x \in \mathcal{T}_1} \imath^{T_1(x)} \quad = \quad \sum_{x \in \{0,1\}} \imath^x \quad = \quad 1 + \imath.$$

The result then follows from Lemma 2. □