On the Codebook Design for NOMA Schemes from Bent Functions

Chunlei Li [1], Constanza Riera [2], Palash Sarkar [1*] and Pantelimon Stănică [3]

[1] Department of Informatics, University of Bergen, Bergen, Norway.
[2] Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, Bergen, Norway.
[3] Applied Mathematics Department, Naval Postgraduate School, Monterey, CA 93943, USA.

*Corresponding author(s). E-mail(s): palash.sarkar@uib.no;
Contributing authors: chunlei.li@uib.no; csr@hvl.no;
pstanica@nps.edu;

Abstract

Uplink grant-free non-orthogonal multiple access (NOMA) is a promising technology for massive connectivity with low latency and high energy efficiency. In code-domain NOMA schemes, the requirements boil down to the design of codebooks that contain a large number of spreading sequences with low peak-to-average power ratio (PAPR) while maintaining low coherence. When employing binary Golay sequences with guaranteed low PAPR in the design, the fundamental problem is to construct a large set of n-variable quadratic bent or near-bent functions in a particular form such that the difference of any two is bent for even n or near-bent for odd n to achieve optimally low coherence. In this work, we propose a theoretical construction of NOMA codebooks by applying a recursive approach to those particular quadratic bent functions in smaller dimensions. The proposed construction yields desired NOMA codebooks that contain $6 \cdot N$ Golay sequences of length $N = 2^{4m}$ for any positive integer m and have the lowest possible coherence $1/\sqrt{N}$.

Keywords: NOMA, PAPR, coherence, bent and near-bent function, Walsh-Hadamard transform

1 Introduction

The massive connectivity of wireless devices is a fundamental aspect of machine-type communications [19], which must accommodate a large number of devices while ensuring minimal control overhead, low latency, and low power consumption for delay-sensitive and energy-efficient communication. Non-orthogonal multiple access (NOMA) [4, 7] has emerged as a solution for enabling massive device connectivity in 5G wireless systems. By permitting multiple devices to share common resources without scheduling, uplink grant-free NOMA is a promising approach to achieving massive connectivity with low latency and high energy efficiency [24]. In grant-free code-domain NOMA, a codebook comprises user-specific spreading sequences assigned to all devices, enabling on-demand activation while minimizing signaling overhead. In this NOMA scheme, the codebook should satisfy several key criteria: a large number of spreading sequences to support massive connectivity, low peak-to-average power ratio (PAPR) of each sequence for improved energy efficiency, low coherence for better performance in multiuser detection, and a small alphabet size to facilitate efficient hardware implementation. Considering these criteria simultaneously is challenging although the design of large sequence sets with low correlation has been extensively researched in the literature [9, 10, 16].

Golay complementary sequences [12] are a pair of sequences that have zero aperiodic correlation sum at all nonzero shifts, ensuring that each Golay sequence has PAPR upper bounded by 2 (see Subsection 2.2). The utility of Golay sequences in controlling the PAPR of orthogonal frequency division multiplexing (OFDM) schemes has been recognized since the 1950s. In 1999 Davis and Jedwab [8] established a fundamental connection between Golay sequences and Reed-Muller (RM) codes: all existing binary Golay sequences of length 2^n correspond to cosets of the first-order RM codes in the second-order binary RM codes, where the coset representatives are n-variable quadratic Boolean functions of algebraic normal form $Q_\pi(x) = \sum_{i=1}^{n-1} x_{\pi(i)}x_{\pi(i+1)}$, where $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ and π is a permutation on the set $\{1, 2, \ldots, n\}$. Such binary sequences were later referred to as Golay-Davis-Jedwab (GDJ) sequences in the literature.

In code-domain NOMA scheme, Yu [24] proposed a NOMA codebook design where the codebook is in the form of a spreading matrix having GDJ sequences as its columns (see Definition 2.6). In the design, each spreading sequence has PAPR upper bounded by 2. Meanwhile, an optimally low coherence of the codebook can be derived by choosing a set of L permutations $\{\pi_1, \ldots, \pi_L\}$ on $\{1, 2, \ldots, n\}$ such that for any two distinct permutations

π_{l_1}, π_{l_2}, the quadratic function $Q_{\pi_{l_1}}(x) + Q_{\pi_{l_2}}(x)$, $x \in \mathbb{F}_2^n$, is bent for even n and near-bent for odd n (see Definition 2.1). As a result, one obtains a NOMA codebook that contains $L \cdot 2^n$ binary spreading sequences of length 2^n with PAPR upper bounded by 2 and has an optimally low coherence, where L is termed the *overloading factor* of the codebook. For supporting massive connectity, the key task is then to make the overloading factor L as large as possible. In [24] Yu considered a computer search, which quickly became infeasible when n is larger than or equal to 9. Tian, Liu and Li in [22] proposed a graph-based approach that yields NOMA codebooks with overloading factor $L = 4$. Very recently, Liu et al. [15] used the quadratic Gold functions to generate NOMA codebooks of overloading factor L up to $\frac{p-1}{2}$, where p is the minimum prime factor of $n+1$ for even n (respectively, n for odd n). This approach can yield a relatively large overloading factor for carefully chosen n, especially when $n+1$ or n is an odd prime. On the other hand, the set size drops dramatically when the minimum prime factor of $n+1$ for even n (respectively, n for odd n) is small. For example, for positive integers n such that n modulo 6 equals 2 or 3, the minimum factor of $n+1$ or n is 3, and then $L = 1$; similarly, when n modulo 10 equals 4 or 5, the corresponding loading factor L is only 2.

Following Yu's construction [24], this paper aims to derive NOMA codebooks with overloading factors as large as possible. For the simplicity of presentation, two permutations π, ρ on the set $\{1, 2, \ldots, n\}$ will be referred to as *compatible* in this paper, denoted as $\pi \bowtie \rho$, if the corresponding quadratic function $Q_\pi(x) + Q_\rho(x)$ is bent (respectively, near-bent) when n is even (respectively, odd). The central mathematical problem in this paper is to construct a set of mutually compatible permutations of $\{1, 2, \ldots, n\}$ of set size L as large as possible. This problem will be studied from the perspective of Walsh-Hadamard spectra of the involved quadratic Boolean functions.

In this paper, we propose a recursive construction of large compatible sets of $\{1, 2, \ldots, n\}$, termed a *compatible set*, for infinitely many n. We denote by S_n the set of all permutations of $\{1, 2, \ldots, n\}$, and by IS_n the set of all permutations that are compatible with the identity permutation I_n of $\{1, 2, \ldots, n\}$. We start by investigating the conditions under which a permutation in IS_{n+m} can be derived from a permutation π in IS_n and a permutation ρ in IS_m (see Theorem 3.5). This allows us to obtain a list of permutations in IS_{n+4} from those in IS_n and IS_4. After a comprehensive analysis of compatible sets in dimension 4, we show that all those compatible sets can be recursively extended to a compatible set of the same size in dimension $4m$ for any $m \geq 2$ (see Theorem 3.11). Consequently, this yields NOMA codebooks of $6 \cdot 2^{4m}$ GDJ

sequences with optimally low coherence 2^{-2m}, which complements the result in [15].

The remainder of this paper is organized as follows. In Section 2 we recall basic and auxiliary results, and introduce the main research problems. In Section 3, we first investigate a general extension method for deriving permutations compatible with the identity permutation in Subsection 3.1; we then conduct a comprehensive analysis of compatible permutations in dimension 4 in Subsection 3.2; and finally, in Subsection 3.3, we present a recursive construction of compatible sets in dimension $4m$. The work is concluded in Section 4.

2 Preliminaries

Below we recall some basics of Boolean functions [5], spreading matrices in the context of NOMA schemes [24], and discusses the design of NOMA codebooks. Subsection 2.1 contains the Boolean-function material used in the proofs, whereas Subsection 2.2 records only the communication-theoretic background needed to formulate the codebook-design problem in NOMA schemes.

2.1 Boolean functions

Let n be a positive integer. Denote by $\mathbb{F}_2^n$ the n-dimensional vector space over the finite field $\mathbb{F}_2$. There is a natural one-to-one correspondence φ between the set $\{0, 1, \ldots, 2^n - 1\}$ and $\mathbb{F}_2^n$, namely, for an integer j with $0 \le j < 2^n$, one has $\varphi(j) = (j_1, \ldots, j_n) \in \mathbb{F}_2^n$ with $j = j_1 + j_2\, 2 + \cdots + j_n\, 2^{n-1}$. We shall identify an integer $j \in \{0, 1, \ldots, 2^n - 1\}$ as its corresponding vector $\varphi(j)$ and use them interchangeably when the context is clear. For $k = 1, 2, \ldots, n$, we will use e_k to denote the k-th row of the $n \times n$ identity matrix over $\mathbb{F}_2$.

An n-variable Boolean function is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. It can be represented by the *truth-table* as $(f(0), f(1), \ldots, f(2^n - 1))$ or by the unique *algebraic normal form* as

$$f(x) = \sum_{I \subseteq \{1,\ldots,n\}} a_I \left(\prod_{i \in I} x_i \right),$$

where the sum is taken modulo 2 and $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$. The *algebraic degree* of $f(x)$ is defined by $\deg(f) = \max\{|I| : a_I \neq 0\}$, where $|I|$ denotes the size of I (with the convention that the zero function has algebraic degree 0). An n-variable Boolean function is said to be *linear* when it is of the form $L_c(x) = c_1 x_1 + c_2 x_2 + \cdots + c_n x_n$ for a vector $c = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_2^n$, and is said to be *quadratic* when its algebraic degree is two.

Definition 2.1. *The Walsh-Hadamard transform of an n-variable Boolean function $f(x)$ at a point $c \in \mathbb{F}_2^n$ is given by*

$$W_f(c) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+L_c(x)}.$$

The set of Walsh-Hadamard coefficients $W_f(c)$ for all $c \in \mathbb{F}_2^n$ is called the Walsh-Hadamard spectrum of $f(x)$. The function $f(x)$ is said to be bent if its Walsh-Hadamard spectrum is $\{\pm 2^{\frac{n}{2}}\}$ for even n, and said to be near-bent if its Walsh-Hadamard spectrum is $\{0, \pm 2^{\frac{n+1}{2}}\}$ for odd n.

For a quadratic n-variable Boolean function $Q(x)$, its *bilinear mapping* is given by $B(x, y) = Q(x + y) + Q(x) + Q(y)$. The kernel of the bilinear mapping of $Q(x)$ is defined by $V_Q = \{y \in \mathbb{F}_2^n : B(x, y) = 0 \text{ for any } x \in \mathbb{F}_2^n\}$, and the rank of $Q(x)$ is given by $r = n - \dim_{\mathbb{F}_2}(V_Q)$ ($\dim_{\mathbb{F}_2}(V_Q)$ denotes the dimension of the vector space V_Q over $\mathbb{F}_2$). In addition, the bilinear mapping $B(x, y)$ of a quadratic function $Q(x)$ can be characterized by its corresponding symplectic matrix $\mathbf{B}$, which is defined as an $n \times n$ binary matrix such that for $1 \le i, j \le n$, the entry $\mathbf{B}(i, j) = 1$ if and only if $B(x, y)$ contains the term $x_i y_j$, or equivalently, $x_i x_j$ occurs in the quadratic function $Q(x)$. Consequently, the rank of a quadratic function $Q(x)$ is identical to the rank of the corresponding symplectic matrix $\mathbf{B}$ [17]. It is a well-known fact (see [17, p. 441] or [18, Ch. 16]) that the Walsh-Hadamard spectrum of $Q(x)$ depends upon its rank only, precisely,

$$W_Q(c) = \sum_{x \in \mathbb{F}_2^n} (-1)^{Q(x)+L_c(x)} = \begin{cases} \pm 2^{n-\frac{r}{2}}, & \text{if } Q(x) = 0 \text{ for all } x \in V_Q, \\ 0, & \text{otherwise.} \end{cases} \quad (1)$$

For a quadratic bent function, we introduce a condition that will be used in subsequent discussions.

Definition 2.2. *Let $n \ge 4$ be an even integer, and let i, j be integers with $1 \le i < j \le n$. A quadratic bent function $Q(x)$ on $\mathbb{F}_2^n$ is said to satisfy the Walsh-Hadamard condition (WHC) on (i, j) if*

$$\prod_{\alpha, \beta \in \mathbb{F}_2} W_Q(c + \alpha e_i + \beta e_j) = 2^{2n}, \quad \forall\, c \in \mathbb{F}_2^n,$$

where e_i and e_j denote the i-th row and j-th row, respectively, of the $n \times n$ identity matrix over $\mathbb{F}_2$.

2.2 NOMA codebooks from complementary sequences

For a complex-valued sequence $\mathbf{a} = (a_0, \ldots, a_{N-1})$, its *aperiodic autocorrelation* $C_{\mathbf{a}}(\tau)$ at a shift τ, where τ is an integer with $|\tau| < N$, is defined as follows:

$$C_{\mathbf{a}}(\tau) = \begin{cases} \sum_{i=0}^{N-\tau-1} a_i a_{i+\tau}^*, & 0 \le \tau < N, \\ \sum_{i=0}^{N+\tau-1} a_{i-\tau} a_i^*, & -N < \tau < 0, \end{cases}$$

where a_i^* denotes the complex conjugate of a_i. A pair of sequences $\mathbf{a}, \mathbf{b}$ of length N is called a *Golay complementary pair* [12] if they satisfy

$$C_{\mathbf{a}}(\tau) + C_{\mathbf{b}}(\tau) = 0 \tag{2}$$

for any integer τ with $0 < |\tau| < N$.

Each sequence of such a complementary pair is called a *Golay complementary sequence.*

Definition 2.3. *For a unimodular sequence* $\mathbf{a} = (a_0, a_1, \ldots, a_{N-1})$ *with* $|a_i| = 1$ *for* $0 \le i < N$*, the peak-to-average power ratio (PAPR) of the associated OFDM signal is defined by*

$$\mathrm{PAPR}(\mathbf{a}) = \frac{\max_{t\in[0,1)} \left| \sum_{i=0}^{N-1} a_i e^{2\pi\sqrt{-1}\, it} \right|^2}{N}.$$

Note that

$$\left| \sum_{i=0}^{N-1} a_i e^{2\pi\sqrt{-1}\, it} \right|^2 = N + \sum_{0<|\tau|<N} C_{\mathbf{a}}(\tau) e^{2\pi\sqrt{-1} t\tau}.$$

For a Golay complementary pair $(\mathbf{a}, \mathbf{b})$, due to their complementary property as in (2), one obtains $\mathrm{PAPR}(\mathbf{a}) + \mathrm{PAPR}(\mathbf{b}) = 2$. This indicates that each Golay complementary sequence has PAPR upper bounded by 2 since the value of PAPR is always non-negative. This low-PAPR property is precisely the reason why Golay complementary sequences are useful for PAPR control in multi-carrier OFDM schemes. In 1999 Davis and Jedwab [8] established a fundamental relation between binary Golay complementary pairs of length 2^n and quadratic Boolean functions of particular forms as below.

Lemma 2.4 ([8, Th. 3])**.** *Let* π *be a permutation of* $\{1, 2, \ldots, n\}$ *and*

$$Q_\pi(x) = \sum_{i=1}^{n-1} x_{\pi(i)} x_{\pi(i+1)}.$$

Let $c = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_2^n$ *and*

$$f_\pi^c(x) = Q_\pi(x) + L_c(x) = \sum_{i=1}^{n-1} x_{\pi(i)} x_{\pi(i+1)} + \sum_{i=1}^{n} c_i x_i.$$

For $\epsilon, \epsilon' \in \mathbb{F}_2$, *define the functions*

$$a(x) = f_\pi^c(x) + \epsilon,$$
$$b(x) = f_\pi^c(x) + x_{\pi(1)} + \epsilon'.$$

Let $\mathbf{a} = (a_0, a_1, \ldots, a_{2^n-1}), \mathbf{b} = (b_0, b_1, \ldots, b_{2^n-1})$ *be two sequences associated with the functions* $a(x)$ *and* $b(x)$ *given by* $a_j = (-1)^{a(\varphi(j))}$ *and* $b_j = (-1)^{b(\varphi(j))}$, *respectively, for* $0 \le j < 2^n$. *Then the sequences* $\mathbf{a}$ *and* $\mathbf{b}$ *form a binary Golay complementary pair of length* 2^n.

For compressed sensing-based joint channel estimation and multiuser detection in uplink grant-free NOMA, Yu [24] proposed a codebook in the form of a spreading matrix, which should have low coherence to minimize interference and a large number of columns to accommodate sufficiently many user devices. We first recall the *coherence* of a spreading matrix.

Definition 2.5. *Given an* $N \times K$ *matrix* $\mathbf{\Phi}$ *over the complex field* $\mathbb{C}$, *the coherence of* $\mathbf{\Phi}$ *is given by*

$$\mu(\mathbf{\Phi}) = \max_{1 \le k_1 \ne k_2 \le K} \frac{|\langle \mathbf{a}_{k_1}, \mathbf{a}_{k_2} \rangle|}{\|\mathbf{a}_{k_1}\|_2 \, \|\mathbf{a}_{k_2}\|_2},$$

where $\mathbf{a}_{k_1}, \mathbf{a}_{k_2}$ *are the* k_1*-th,* k_2*-th columns of* $\mathbf{\Phi}$, *respectively, and the notation* $\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=0}^{N-1} a_i b_i^*$ *denotes the inner product between two sequences* $\mathbf{a}$ *and* $\mathbf{b}$, *and* $\|\mathbf{a}\|_2 = \sqrt{\langle \mathbf{a}, \mathbf{a} \rangle}$ *is the* L^2*-norm of a sequence* $\mathbf{a}$. *The ratio* K/N *is called the overloading factor of the matrix* $\mathbf{\Phi}$.

In [24], Yu proposed a framework for designing the uplink grant-free NOMA scheme based on the complementary sequences in Lemma 2.4, referred to as the GDJ sequences in the literature. Here we recall the basics of the framework in [24]. Arrange all the GDJ sequences associated with the quadratic functions $f_\pi^c(x) = Q_\pi(x) + L_c(x)$, where $c \in \mathbb{F}_2^n$, in a spreading matrix column by column, where the columns are indexed by c. Then we obtain a $2^n \times 2^n$ orthogonal spreading matrix, in which any two columns indexed by c_1, c_2 are orthogonal (since their inner product is equal to $\sum_{x \in \mathbb{F}_2^n} (-1)^{L_{c_1+c_2}(x)}$, which vanishes at any different indices $c_1, c_2 \in \mathbb{F}_2^n$). Observe that for any sequence $\mathbf{s}$

associated with the function $a(x) = f_\pi^c(x) + 1$ or $b(x) = f_\pi^c(x) + x_{\pi(1)} + \epsilon'$ with $\epsilon' \in \mathbb{F}_2$ as in Lemma 2.4, the column $\mathbf{s}'$ indexed by the vector c or $c + e_{\pi(1)}$ (which differs from c at the $\pi(1)$-th position) in the existing spreading matrix satisfies $|\langle \mathbf{s}', \mathbf{s} \rangle| = 2^n$, which is the highest coherence. This indicates that one cannot add more GDJ sequences derived from the same permutation π into the existing spreading matrix. To further widen the spreading matrix while maintaining low coherence, Yu [24] adopted more permutations of $\{1, 2, \ldots, n\}$ and proposed the following non-orthogonal spreading matrix.

Definition 2.6. *Consider L distinct permutations $\pi_1, \ldots, \pi_L$ of $\{1, \ldots, n\}$. Let $N = 2^n$ and define an $N \times LN$ non-orthogonal spreading matrix as follows:*

$$\mathbf{\Phi} = \frac{1}{\sqrt{N}} \left[\mathbf{\Phi}_1, \ldots, \mathbf{\Phi}_L \right], \tag{3}$$

where for each $1 \le \ell \le L$,

$$\mathbf{\Phi}_\ell = \left[\mathbf{a}_{\pi_\ell}^{(0)}, \mathbf{a}_{\pi_\ell}^{(1)}, \ldots, \mathbf{a}_{\pi_\ell}^{(N-1)} \right]_{N \times N}$$

is a column-wise orthogonal matrix consisting of GDJ sequences $\mathbf{a}_{\pi_\ell}^{(c)}$ associated with the n-variable quadratic functions $f_{\pi_\ell}^c(x) = Q_{\pi_\ell}(x) + L_c(x)$ as in Lemma 2.4, where c runs through all vectors in $\mathbb{F}_2^n$.

The coherence of the above spreading matrix can be characterized in the following way [24, Th. 1].

Lemma 2.7. *Let $\mathbf{\Phi}$ be an $N \times LN$ spreading matrix defined as in (3). For $1 \le \ell_1 \ne \ell_2 \le L$, and $\pi_{\ell_1}, \pi_{\ell_2} \in \{\pi_1, \ldots, \pi_L\}$, let $\mathbf{B}_{\ell_1,\ell_2}$ be an $n \times n$ binary symplectic matrix defined as follows: for $1 \le i, j \le n$, $\mathbf{B}_{\ell_1,\ell_2}(i,j) = 1$ if and only if the quadratic form $Q_{\pi_{\ell_1}}(x) + Q_{\pi_{\ell_2}}(x)$ contains the term $x_i x_j$. Then the coherence of the spreading matrix $\mathbf{\Phi}$ is given by*

$$\mu(\mathbf{\Phi}) = \frac{1}{\sqrt{2^{r_{\min}}}}, \text{ where } r_{\min} = \min_{1 \le \ell_1 \ne \ell_2 \le L} \operatorname{rank}\left(\mathbf{B}_{\ell_1,\ell_2}\right). \tag{4}$$

To have a low coherence of the above spreading matrix, it is desirable to keep $r_{\min}$ as large as possible. Since each matrix $\mathbf{B}_{\ell_1,\ell_2}$ is a skew-symmetric matrix over $\mathbb{F}_2$, which has the maximum rank n for even n (respectively, $n-1$

for odd n), the coherence $\mu(\mathbf{\Phi})$ has the following lower bounds:

$$\mu(\mathbf{\Phi}) \geq \begin{cases} \frac{1}{\sqrt{2^n}} \text{ for even } n, \\ \frac{1}{\sqrt{2^{n-1}}} \text{ for odd } n. \end{cases} \tag{5}$$

From Definition 2.6, the coherence of the spreading matrix $\mathbf{\Phi}$ in (3) can be characterized by the Walsh-Hadamard transforms of the quadratic Boolean functions $Q_{\pi_{\ell_1}}(x) + Q_{\pi_{\ell_2}}(x)$. In the language of the Walsh-Hadamard transform, for $1 \leq \ell_1 \neq \ell_2 \leq L$, the quadratic function $Q_{\pi_{\ell_1}}(x)+Q_{\pi_{\ell_2}}(x)$ in Lemma 2.7 with rank r has Walsh-Hadamard spectrum $\{0, \pm 2^{n-\frac{r}{2}}\}$. Define

$$W(\mathbf{\Phi}) = \max_{1\leq \ell_1 \neq \ell_2 \leq L} \max_{c \in \mathbb{F}_2^n} \mid W_{Q_{\pi_{\ell_1}}+Q_{\pi_{\ell_2}}}(c) \mid . \tag{6}$$

Then we have

$$W(\mathbf{\Phi}) = \frac{2^n}{\sqrt{2^{r_{\min}}}}, \text{ where } r_{\min} = \min_{1\leq \ell_1 \neq \ell_2 \leq L} \operatorname{rank}\left(Q_{\pi_{\ell_1}}(x) + Q_{\pi_{\ell_2}}(x)\right),$$

which gives a characterization of coherence of the spreading matrix $\mathbf{\Phi}$ in terms of Walsh-Hadamard transforms as follows:

$$\mu(\mathbf{\Phi}) = \frac{W(\mathbf{\Phi})}{2^n}. \tag{7}$$

Equivalently, the equality in (5) is achieved when the quadratic function $Q_{\pi_{\ell_1}} + Q_{\pi_{\ell_2}}(x)$, for any $1 \leq \ell_1 \neq \ell_2 \leq L$, is a bent function for even n, and a near-bent function for odd n.

2.3 Discussions of the NOMA codebook design

In this subsection we discuss the advantages of Yu's construction of NOMA codebooks and the research problems that require further investigation.

Low PAPR and Small Alphabet. Constructing spreading sequences with low PAPR is generally challenging. The GDJ sequences are binary sequences which have low PAPR upper bounded by 2 independent of their sequence lengths.

Optimally Low Coherence. Consider a generic $N \times K$ complex-valued matrix $\mathbf{\Psi}$ in which each column has L^2 norm $\sqrt{N}$. According to the well-known Welch bound [23], the coherence of $\mathbf{\Psi}$ satisfies

$$\mu(\mathbf{\Psi}) \geq \sqrt{\frac{K-N}{(K-1)N}}.$$

Matrices that achieve the equality in the Welch bound have various applications in communications. However, it is rather challenging to construct them for $K \geq N+2$ even without the restriction of low PAPR (see [10, 21] and references therein). When $N = 2^n$ and the entries of $\mathbf{\Psi}$ take values ± 1, each column of $\mathbf{\Psi}$ can be associated with a certain n-variable Boolean function. In this case, the coherence of $\mathbf{\Psi}$ can be characterized by the Walsh-Hadamard transform at the zero point for n-variable Boolean functions as shown in (7). Consequently, when $K > N$, the coherence of $\mathbf{\Psi}$ satisfies $\mu(\mathbf{\Psi}) \geq \frac{1}{\sqrt{N}}$, since for any nonlinear n-variable Boolean function, the maximum magnitude of its Walsh-Hadamard coefficients is at least $2^{\frac{n}{2}}$ [5, 6]. Furthermore, when columns of $\mathbf{\Psi}$ are associated with quadratic Boolean functions, the coherence of $\mathbf{\Psi}$ for odd n satisfies $\mu(\mathbf{\Psi}) \geq \sqrt{\frac{2}{N}}$ as in (5). We see that the two lower bounds on the coherence of matrices $\mathbf{\Psi}$ that are generated from n-variable Boolean functions are close to the generic Welch bound $\sqrt{\frac{K-N}{(K-1)N}}$ on generic complex-valued matrices in the case of $K = LN$, where the Welch bound becomes $\sqrt{\frac{1}{N+\frac{N-1}{L-1}}}$.

The spreading matrix $\mathbf{\Phi}$ in Definition 2.6 has an attractive property: the coherence of $\mathbf{\Phi}$ can take a low value (close to the Welch bound) when the symplectic matrix $\mathbf{B}_{\ell_1,\ell_2}$ for any $1 \leq \ell_1 \neq \ell_2 \leq L$ has a largest possible rank, namely, n for even n or $n-1$ for odd n.

Overloading Factor. The spreading matrix $\mathbf{\Phi}$ in (3) is required to have an overloading factor $L = K/N$ as large as possible to accommodate sufficiently many devices.

Interestingly, this problem was also raised earlier by Paterson [20] in the context of algebraic coding theory, where he considered GDJ sequences for OFDM codes and gave a relatively trivial upper bound on L for even n. More specifically, for any quadratic function $Q_\pi(x) = \sum_{i=1}^{n-1} x_{\pi(i)}x_{\pi(i+1)}$, its corresponding symplectic matrix $\mathbf{B}$ with $\mathbf{B}(i,j) = 1$ if and only if $x_i x_j$ occurs in $Q_\pi(x)$ has the following property: its first row has a zero as its first entry and Hamming weight either 1 or 2. This implies that there are at most $(n-1)+\binom{n-1}{2} = \binom{n}{2}$ different choices of the first row of $\mathbf{B}$. For the GDJ-based construction under consideration, the sum of two relevant symplectic matrices is required to have rank n for even n, so one can have at most $\binom{n}{2}$ symplectic matrices with different first rows. Consequently, there are at most $\binom{n}{2}$ permutations on $\{1, 2, \ldots, n\}$ that are mutually compatible. This gives the following upper bound on the overloading factor of the spreading matrix $\mathbf{\Phi}$ in Definition 2.6 that has the lowest coherence $2^{-\frac{n}{2}}$:

$$L \leq n(n-1)/2. \tag{8}$$

This upper bound for $n = 4$ can be easily confirmed to be tight. However, it appears far from being tight for large values $n \geq 6$ according to the experimental results as in [15, Table III].

Based on the above analysis, natural, albeit challenging, problems arise.

Main Problem 1. *Let $N = 2^n$ with $n \geq 6$ and $\mathbf{\Phi}$ be the $N \times LN$ spreading matrix given in Definition 2.6.*

(i) Give an improved upper bound (tighter than the Paterson bound in (8)) on the overloading factor L such that the spreading matrix $\mathbf{\Phi}$ can maintain the optimally low coherence

$$\mu(\mathbf{\Phi}) = \begin{cases} \frac{1}{\sqrt{2^n}} & \text{for even } n, \\ \frac{1}{\sqrt{2^{n-1}}} & \text{for odd } n. \end{cases}$$

(ii) Construct a spreading matrix $\mathbf{\Phi}$ with a large overloading factor L for infinitely many n.

3 A Construction by Permutation Extension

This section is dedicated to a recursive construction of NOMA codebooks in dimension $4m$ for positive integers $m \geq 2$. After the introduction of basic notations and results, Subsection 3.1 considers the derivation of permutations compatible with the identity permutation and Subsection 3.2 analyzes compatible sets in dimension 4. These two subsections prepare results for Subsection 3.3 which recursively constructs compatible sets of size 6 from dimension 4 to higher dimensions $4m$ for $m \geq 2$.

Denote by I_n the identity permutation and by S_n the set of all permutations of $\{1, 2, \ldots, n\}$. As is customary, we write a permutation as $\pi = [i_1, i_2, \ldots, i_n]$ to mean that π is defined by $\pi(1) = i_1, \pi(2) = i_2, \ldots, \pi(n) = i_n$. Given a permutation $\pi = [i_1, i_2, \ldots, i_n]$, we refer to the permutation $\widetilde{\pi} = [i_n, i_{n-1}, \ldots, i_1]$ as its *reverse*.

We introduce the notion of *compatible permutations* below.

Definition 3.1. *Two permutations π_1, π_2 in S_n are said to be compatible, denoted by $\pi_1 \bowtie \pi_2$, if the corresponding quadratic function $Q_{\pi_1}(x) + Q_{\pi_2}(x) = \sum_{i=1}^{n-1} x_{\pi_1(i)} x_{\pi_1(i+1)} + \sum_{i=1}^{n-1} x_{\pi_2(i)} x_{\pi_2(i+1)}$ is bent for even n and near-bent for odd n. In addition, a subset $S \subset S_n$ is called a compatible set if any two permutations in S are compatible.*

It is desirable to have a compatible set with set size as large as possible. We first give some basic properties for compatible permutations.

Lemma 3.2. *Let $\widetilde{\pi}$, π^{-1} denote, respectively, the reverse and compositional inverse of a permutation π in S_n. Then for any two permutations π, $\sigma \in S_n$, we have:*

(i) $\sigma \bowtie \pi$ *if and only if* $\sigma \bowtie \widetilde{\pi}$;

(ii) $I_n \bowtie \pi$ *if and only if* $I_n \bowtie \pi^{-1}$;

(iii) $\pi \bowtie \sigma$ *if and only if* $I_n \bowtie \sigma^{-1} \circ \pi$, *where* $\circ$ *is the composition operator.*

Proof It is easy to see that $Q_\pi(x) = Q_{\widetilde{\pi}}(x)$, so $Q_\sigma(x) + Q_\pi(x)$ and $Q_\sigma(x) + Q_{\widetilde{\pi}}(x)$ represent the same function, which implies claim (i). It can be observed that $Q_{I_n}(x_1, \ldots, x_n) + Q_\pi(x_1, \ldots, x_n) = Q_{\pi^{-1}}(x_{\pi(1)}, \ldots, x_{\pi(n)}) + Q_{I_n}(x_{\pi(1)}, \ldots, x_{\pi(n)})$, which means that $Q_{I_n} + Q_\pi$ and $Q_{I_n} + Q_{\pi^{-1}}$ have the same Walsh-Hadamard spectrum. This implies claim (ii). Finally, with $(y_1, \ldots, y_n) = \left(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}\right)$, we have

$$\begin{aligned} Q_{I_n}(x_1, \ldots, x_n) + Q_{\sigma^{-1}\circ\pi}(x_1, \ldots, x_n) &= \sum_{i=1}^{n-1} (x_i x_{i+1} + x_{\sigma^{-1}\circ\pi(i)} x_{\sigma^{-1}\circ\pi(i+1)}) \\ &= \sum_{i=1}^{n-1} (y_{\sigma(i)} y_{\sigma(i+1)} + y_{\pi(i)} y_{\pi(i+1)}) \\ &= Q_\sigma(y_1, \ldots, y_n) + Q_\pi(y_1, \ldots, y_n), \end{aligned}$$

which implies claim (iii) when the Walsh-Hadamard transforms of the above quadratic functions are considered. □

By Lemma 3.2 (i), it is readily seen that the relations $\pi \bowtie \rho$, $\pi \bowtie \widetilde{\rho}$, $\widetilde{\pi} \bowtie \rho$ and $\widetilde{\pi} \bowtie \widetilde{\rho}$ are equivalent. In addition, it follows Lemma 3.2 (ii) and (iii) that $\pi \bowtie \sigma$ if and only if $I_n \bowtie \pi^{-1} \circ \sigma$. Without loss of generality, we can always assume that a compatible set $S \subset S_n$ contains the identity permutation I_n (since one can obtain I_n by applying the inverse of a permutation to all the others in a compatible set). From now on, we will focus only on compatible sets containing I_n. For ease of presentation, we denote by IS_n the set of all permutations in S_n that are compatible with I_n, i.e.,

$$IS_n = \{\pi \in S_n \,|\, \pi \bowtie I_n\}.$$

Below we consider an approach to constructing permutations compatible with I_{n+m} from permutations in IS_n and IS_m for positive integers n and m.

3.1 Extending permutations from IS_n and IS_m to IS_{n+m}

This subsection considers extending a permutation $\pi \in IS_n$ with another permutation $\rho \in IS_m$ to obtain a permutation in IS_{n+m}. This sets a good starting point for constructing compatible sets in $(n+m)$ variables. We will consider the following extension

$$\pi\rho^R = [\pi(1), \ldots, \pi(n), \rho(1)+n, \ldots, \rho(m)+n]. \tag{9}$$

For the above extension, it can be verified that for $\pi, \sigma \in S_n$ and $\rho, \varrho \in S_m$,

$$(\pi\rho^R) \circ (\sigma\varrho^R) = (\pi \circ \sigma)(\rho \circ \varrho)^R. \tag{10}$$

In particular, taking $\sigma = \pi^{-1}$ and $\varrho = \rho^{-1}$, we have $(\pi\rho^R) \circ (\pi^{-1}(\rho^{-1})^R) = I_{n+m}$, indicating

$$(\pi\rho^R)^{-1} = \pi^{-1}(\rho^{-1})^R. \tag{11}$$

The following lemma discusses the compatibility between two of such permutations in IS_{n+m}.

Lemma 3.3. *Suppose two permutations $\pi_1\rho_1^R$ and $\pi_2\rho_2^R$ are compatible with I_{n+m}. Then*

$$\pi_1\rho_1^R \bowtie \pi_2\rho_2^R \text{ if and only if } (\pi_1^{-1} \circ \pi_2)(\rho_1^{-1} \circ \rho_2)^R \bowtie I_{n+m}.$$

Proof The statement follows directly from Lemma 3.2 (*iii*), (10) and (11). □

In this paper we are mainly concerned with the case of even dimensions. Note that there are only two permutations in S_2, namely I_2 and $\widetilde{I_2}$, and $\widetilde{I_2}$ is not compatible with I_2. For the above extension, then, the cases where $n = 2$ or $m = 2$ cannot lead to useful compatible permutations in IS_{n+m}. We will discuss extensions for $n, m \geq 4$.

In Definition 2.2 we introduced the WHC for quadratic bent functions. Below we discuss when WHC can be satisfied, which will be frequently used.

Let n be a positive integer, and i, j be two integers with $1 \leq i < j \leq n$. Let $u, v \in \mathbb{F}_2$ and define a flat $\Omega_{u,v} = \{(x_1, \ldots, x_n) \in \mathbb{F}_2^n : x_i = u, x_j = v\}$. It is clear that $\mathbb{F}_2^n$ can be partitioned as $\mathbb{F}_2^n = \Omega_{0,0} \sqcup \Omega_{0,1} \sqcup \Omega_{1,0} \sqcup \Omega_{1,1}$. For a quadratic function $Q(x)$, we denote the $(n-2)$-variable Boolean function $Q|_{x_i=u,x_j=v}(x)$ (which is obtained by restricting $Q(x)$ on the flat $\Omega_{u,v}$) for short as $\mathsf{Q}|_{u,v}(\hat{x})$, where $\hat{x} \in \mathbb{F}_2^{n-2}$ denotes the vector obtained by removing

x_i, x_j from x in $\mathbb{F}_2^n$. For instance, assuming $n = 4$, $(i, j) = (1, 3)$ and $Q(x) = x_1x_2 + x_1x_4 + x_2x_4 + x_3x_4$, we obtain $\mathsf{Q}|_{0,0}(\hat{x}) = Q|_{x_1=0,x_3=0}(x) = x_2x_4$, and similarly $\mathsf{Q}|_{0,1}(\hat{x}) = x_2x_4 + x_4$, $\mathsf{Q}|_{1,0}(\hat{x}) = x_2x_4 + x_2 + x_4$ and $\mathsf{Q}|_{1,1}(\hat{x}) = x_2x_4 + x_2$, where $\hat{x} = (x_2, x_4)$. Note that for $n = 4$, the restriction functions for certain quadratic functions $Q(x)$ can have algebraic degree one; e.g., for $Q(x) = x_1x_2+x_1x_3+x_1x_4+x_3x_4$ and $(i, j) = (1, 3)$, all the restriction functions $\mathsf{Q}|_{u,v}(\hat{x})$ have algebraic degree one. For fixed integers i, j with $1 \le i < j \le n$, the functions $\mathsf{Q}|_{0,0}(\hat{x}), \mathsf{Q}|_{0,1}(\hat{x}), \mathsf{Q}|_{1,0}(\hat{x}), \mathsf{Q}|_{1,1}(\hat{x})$ are decompositions of $Q(x)$ as discussed in [3, Sec. V].

For an even integer n, the following proposition discusses the relation between the Walsh-Hadamard transforms of a bent function $Q(x)$ and its decompositions $\mathsf{Q}|_{u,v}(\hat{x})$ for $u, v \in \mathbb{F}_2$ with respect to certain $1 \le i < j \le n$.

Proposition 3.4. *Let $n \ge 4$ be an even integer and i, j be integers with $1 \le i < j \le n$. Assume $Q(x)$ is a quadratic bent function on $\mathbb{F}_2^n$, and $\mathsf{Q}|_{u,v}(\hat{x}) = Q|_{x_i=u,x_j=v}(x)$, where $u, v \in \mathbb{F}_2$, denotes one of the four components of the decomposition of $Q(x)$ for fixed i and j. Then for any $c \in \mathbb{F}_2^n$, the Walsh-Hadamard transforms $W_Q(c)$ and $W_{\mathsf{Q}|_{u,v}}(\hat{c})$, where $\hat{c}$ is obtained by removing c_i, c_j from $c \in \mathbb{F}_2^n$, satisfy one of the following:*

(i) three of $|W_{\mathsf{Q}|_{u,v}}(\hat{c})|$ are zero and the remaining one equals $2^{\frac{n}{2}}$; this is equivalent to $\prod_{\alpha,\beta\in\mathbb{F}_2} W_Q(c + \alpha e_i + \beta e_j) = 2^{2n}$, the WHC on (i, j); or

(ii) $|W_{\mathsf{Q}|_{u,v}}(\hat{c})| = 2^{\frac{n-2}{2}}$ for all $u, v \in \mathbb{F}_2$ with three of them having the same sign and the remaining one having the opposite sign; this is equivalent to $\prod_{\alpha,\beta\in\mathbb{F}_2} W_Q(c + \alpha e_i + \beta e_j) = -2^{2n}$,

where e_i, e_j are as given in Definition 2.2.

Proof According to the definition of $\mathsf{Q}|_{u,v}(\hat{x})$, the Walsh-Hadamard transform of $Q(x)$ at $c \in \mathbb{F}_2^n$ satisfies

$$\begin{aligned}
W_Q(c) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{Q(x)+L_c(x)} \\
&= \sum_{x_i,x_j\in\mathbb{F}_2} \sum_{\hat{x}\in\mathbb{F}_2^{n-2}} (-1)^{Q(x)+c_ix_i+c_jx_j+L_{\hat{c}}(\hat{x})} \\
&= \sum_{u,v\in\mathbb{F}_2} \sum_{\hat{x}\in\mathbb{F}_2^{n-2}} (-1)^{\mathsf{Q}|_{u,v}(\hat{x})+c_iu+c_jv+L_{\hat{c}}(\hat{x})} \\
&= \sum_{u,v\in\mathbb{F}_2} (-1)^{c_iu+c_jv} W_{\mathsf{Q}|_{u,v}}(\hat{c}) \\
&= W_{\mathsf{Q}|_{0,0}}(\hat{c}) + (-1)^{c_i} W_{\mathsf{Q}|_{1,0}}(\hat{c}) + (-1)^{c_j} W_{\mathsf{Q}|_{0,1}}(\hat{c}) + (-1)^{c_i+c_j} W_{\mathsf{Q}|_{1,1}}(\hat{c}) \\
&= \pm 2^{\frac{n}{2}}.
\end{aligned} \tag{12}$$

In a similar manner, for $\alpha, \beta \in \mathbb{F}_2$, we have

$$\begin{aligned} W_Q(c+\alpha e_i+\beta e_j) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{Q(x)+(c_i+\alpha)x_i+(c_j+\beta)x_j+L_{\hat{c}}(\hat{x})} \\ &= \sum_{u,v\in\mathbb{F}_2} (-1)^{(c_i+\alpha)u+(c_j+\beta)v} W_{\mathsf{Q}|_{u,v}}(\hat{c}), \end{aligned}$$

which gives

$$\begin{bmatrix} W_Q(c) \\ W_Q(c+e_i) \\ W_Q(c+e_j) \\ W_Q(c+e_i+e_j) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} W_{\mathsf{Q}|_{0,0}}(\hat{c}) \\ (-1)^{c_i} W_{\mathsf{Q}|_{1,0}}(\hat{c}) \\ (-1)^{c_j} W_{\mathsf{Q}|_{0,1}}(\hat{c}) \\ (-1)^{c_i+c_j} W_{\mathsf{Q}|_{1,1}}(\hat{c}) \end{bmatrix}. \tag{13}$$

Note that when $n = 4$, the quadratic function $\mathsf{Q}|_{u,v}(\hat{x})$ for all $u, v \in \mathbb{F}_2$ can have algebraic degree one or two, and when $n > 4$, the functions $\mathsf{Q}|_{u,v}(\hat{x})$ for all $u, v \in \mathbb{F}_2$ are quadratic. We start with the case where $n = 4$ and $\mathsf{Q}|_{u,v}(\hat{x})$ has algebraic degree one for each $u, v \in \mathbb{F}_2$.

When $n = 4$ and $\mathsf{Q}|_{u,v}(\hat{x})$ has algebraic degree one, it is well known that the Walsh-Hadamard transforms $W_{\mathsf{Q}|_{u,v}}(\hat{c})$ equals 2^{n-2} or -2^{n-2} at one point $\hat{c}$ and equals zero at all the remaining points $\hat{c} \in \mathbb{F}_2^2$. In addition, it follows from (12) that for any $c \in \mathbb{F}_2^n$,

$$W_{\mathsf{Q}|_{0,0}}(\hat{c}) + (-1)^{c_i} W_{\mathsf{Q}|_{1,0}}(\hat{c}) + (-1)^{c_j} W_{\mathsf{Q}|_{0,1}}(\hat{c}) + (-1)^{c_i+c_j} W_{\mathsf{Q}|_{1,1}}(\hat{c}) = \pm 2^{\frac{n}{2}}.$$

For $n = 4$, one has $n - 2 = n/2 = 2$ and four choices of $\hat{c}$ in $\mathbb{F}_2^{n-2}$. Thus, for each $\hat{c} \in \mathbb{F}_2^2$, three of $W_{\mathsf{Q}|_{0,0}}(\hat{c}), W_{\mathsf{Q}|_{1,0}}(\hat{c}), W_{\mathsf{Q}|_{0,1}}(\hat{c}), W_{\mathsf{Q}|_{1,1}}(\hat{c})$ are equal to zero and the remaining one is equal to $\pm 2^{\frac{n}{2}}$. Without loss of generality, for a point $c \in \mathbb{F}_2^n$, we assume $W_{\mathsf{Q}|_{0,0}}(\hat{c}) = W_{\mathsf{Q}|_{1,0}}(\hat{c}) = W_{\mathsf{Q}|_{1,1}}(\hat{c}) = 0$, and $W_Q(c) = (-1)^{c_j} W_{\mathsf{Q}|_{0,1}}(\hat{c}) = \pm 2^{\frac{n}{2}}$. Then, according to (13), for the given point c, it follows that

$$\begin{bmatrix} W_Q(c) \\ W_Q(c+e_i) \\ W_Q(c+e_j) \\ W_Q(c+e_i+e_j) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ (-1)^{c_j} W_{\mathsf{Q}|_{0,1}}(\hat{c}) \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} \cdot (-1)^{c_j} W_{\mathsf{Q}|_{0,1}}(\hat{c}),$$

which implies

$$\prod_{\alpha,\beta\in\mathbb{F}_2} W_Q(c+\alpha e_i+\beta e_j) = \left((-1)^{c_j} W_{\mathsf{Q}|_{0,1}(\hat{c})}\right)^4 = 2^{2n}.$$

When $n \geq 4$ and $\mathsf{Q}|_{u,v}(\hat{x})$ is a quadratic function on $\mathbb{F}_2^{n-2}$ for any $u, v \in \mathbb{F}_2$, it is easily seen that $\mathsf{Q}|_{u,v}(\hat{x})$ for all $u, v \in \mathbb{F}_2^n$ have the same quadratic terms. Let r be the rank of $\mathsf{Q}|_{u,v}(\hat{x})$. Note that r is even since it is equal to the rank of the symplectic matrix of $\mathsf{Q}|_{u,v}(\hat{x})$ that is skew symmetric. It follows from (1) that $W_{\mathsf{Q}|_{u,v}}(\hat{c}) \in \{0, \pm 2^{(n-2)-\frac{r}{2}}\}$. Furthermore, the derivative $Q(x+a)+Q(x)$ for any nonzero $a \in \mathbb{F}_2^n$ is linear, thus balanced, that is, it takes the values 0 and 1 equally often. According to [3, Theorem V.4, Equality (33)], we have

$$W^2_{\mathsf{Q}|_{0,0}}(\hat{c}) + W^2_{\mathsf{Q}|_{0,1}}(\hat{c}) + W^2_{\mathsf{Q}|_{1,0}}(\hat{c}) + W^2_{\mathsf{Q}|_{1,1}}(\hat{c}) = 2^n. \tag{14}$$

This together with (12) implies that the rank r can be either $n-4$ or $n-2$. Moreover, when $r = n-4$, three of $W_{\mathsf{Q}|_{u,v}}(\hat{c})$ for $u, v \in \mathbb{F}_2$ are zero and the remaining one equals $\pm 2^{\frac{n}{2}}$; when $r = n-2$, for $u, v \in \mathbb{F}_2$ all $(-1)^{c_i u + c_j v} W_{\mathsf{Q}|_{u,v}}(\hat{c}) = \pm 2^{\frac{n-2}{2}}$, where three of them have the same sign and the remaining one has the opposite sign (otherwise it contradicts (12)).

When $r = n-4$, similarly to the discussion for the case where $\mathsf{Q}|_{u,v}(\hat{x})$ has algebraic degree one for $n = 4$, one can assume that given $c \in \mathbb{F}_2^n$, $W_{\mathsf{Q}|_{u,v}(\hat{c})} = \pm 2^{\frac{n}{2}}$ for a certain pair $(u, v) \in \mathbb{F}_2^2$, we can then apply (13) to obtain

$$\prod_{\alpha,\beta \in \mathbb{F}_2} W_Q(c + \alpha e_i + \beta e_j) = \left((-1)^{c_j} W_{\mathsf{Q}|_{u,v}(\hat{c})}\right)^4 = 2^{2n}.$$

This proves the first claim and implication in Case (i).

When $r = n-2$, again by (13), we have

$$\sum_{\alpha,\beta \in \mathbb{F}_2} W_Q(c + \alpha e_i + \beta e_j) = 4 W_{\mathsf{Q}|_{0,0}}(\hat{c}) = \pm 2^{\frac{n+2}{2}}.$$

Since $W_Q(c + \alpha e_i + \beta e_j) = \pm 2^{\frac{n}{2}}$ for all $\alpha, \beta \in \mathbb{F}_2$, it follows that three of them have the same sign and the remaining one has the opposite sign, which implies

$$\prod_{\alpha,\beta \in \mathbb{F}_2} W_Q(c + \alpha e_i + \beta e_j) = \left((-1)^{c_j} W_{\mathsf{Q}|_{u,v}(\hat{c})}\right)^4 = -2^{2n}.$$

This proves the first claim and implication in Case (ii).

The equivalence follows from the fact that only the first claim in i) and ii) are possible; therefore, the Walsh-Hadamard condition implies the first claim in (i), and the corresponding negated condition implies the first claim in (ii). □

As shown in Proposition 3.4, a quadratic bent function $Q(x)$ satisfies the WHC on (i, j), where $1 \le i < j \le n$, if and only if the decomposition functions $\mathsf{Q}|_{u,v}(\hat{y})$ satisfy the properties in Case (i).

Now we are ready to present the first main theorem below.

Theorem 3.5 *Let $n, m \ge 4$ be even, and let $\pi \in IS_n$, $\rho \in IS_m$ and define $f(x) = Q_\pi(x) + Q_{I_n}(x)$, $g(y) = Q_\rho(y) + Q_{I_m}(y)$, respectively. Then the permutation $\pi\rho^R$ is compatible with I_{n+m} if and only if one of the following conditions holds:*

(i) $(\pi(n) - n)(\rho(1) - 1) = 0$*; or*

(ii) $(\pi(n) - n)(\rho(1) - 1) \neq 0$ *and at least one of $f(x)$ and $g(y)$ satisfy the WHC on $(\pi(n), n)$, $(1, \rho(1))$, respectively.*

Proof For the permutation $\pi\rho^R \in S_{n+m}$, we denote a Boolean function $h(x, y) = Q_{\pi\rho^R}(x, y) + Q_{I_{n+m}}(x, y)$ on $\mathbb{F}_2^n \times \mathbb{F}_2^m$. From the definition of $\pi\rho^R$, it follows directly

that

$$\begin{aligned} h(x,y) &= \sum_{i=1}^{n-1}(x_{\pi(i)}x_{\pi(i+1)} + x_i x_{i+1}) + x_{\pi(n)}y_{\rho(1)} + x_n y_1 \\ &\quad + \sum_{j=1}^{m-1}(y_{\rho(j)}y_{\rho(j+1)} + y_j y_{j+1}) \\ &= f(x) + g(y) + (x_{\pi(n)}y_{\rho(1)} + x_n y_1). \end{aligned} \tag{15}$$

The Walsh-Hadamard transform of $h(x,y)$ at a point $(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ is given by

$$W_h(a,b) = \sum_{(x,y)\in\mathbb{F}_2^{n+m}} (-1)^{f(x)+g(y)+L_a(x)+L_b(y)+(x_{\pi(n)}y_{\rho(1)}+x_n y_1)}. \tag{16}$$

Below we shall investigate the condition such that $|W_h(a,b)| = 2^{\frac{n+m}{2}}$, for all $(a,b) \in \mathbb{F}_2^{n\times m}$ according to the values of $\rho(1)$ and $\pi(n)$.

For Case (i), we consider three subcases, namely, $\pi(n) = n$ and $\rho(1) = 1$; $\pi(n) \neq n$ and $\rho(1) = 1$; $\pi(n) = n$ and $\rho(1) \neq 1$.

Subcase 1. $\pi(n) = n$ *and* $\rho(1) = 1$*:* In this subcase, we have $h(x,y) = f(x)+g(y)$. It follows from (16) that

$$W_h(a,b) = \sum_{(x,y)\in\mathbb{F}_2^{n+m}} (-1)^{f(x)+g(y)+L_a(x)+L_b(y)} = W_f(a)W_g(b) \in \{\pm 2^{\frac{n+m}{2}}\},$$

which implies $h(x,y)$ is bent, and then $\pi\rho^R \bowtie I_{n+m}$.

Subcase 2. $\pi(n) \neq n$ *and* $\rho(1) = 1$*:* In this subcase, we have $h(x,y) = f(x) + g(y) + y_1(x_{\pi(n)} + x_n)$. Then,

$$\begin{aligned} &W_h(a,b) \\ &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+L_a(x)} \left[\sum_{\substack{y\in\mathbb{F}_2^m \\ y_1=0}} (-1)^{g(y)+L_b(y)} + (-1)^{x_n+x_{\pi(n)}} \sum_{\substack{y\in\mathbb{F}_2^m \\ y_1=1}} (-1)^{g(y)+L_b(y)} \right]. \end{aligned}$$

For simplicity, we denote

$$G_0(b) = \sum_{\substack{y\in\mathbb{F}_2^m \\ y_1=0}} (-1)^{g(y)+L_b(y)}, \quad G_1(b) = \sum_{\substack{y\in\mathbb{F}_2^m \\ y_1=1}} (-1)^{g(y)+L_b(y)}.$$

Then we have

$$W_h(a,b) = W_f(a)G_0(b) + W_f(a + e_n + e_{\pi(n)})G_1(b) \tag{17}$$

and

$$G_0(b) + G_1(b) = W_g(b) = \pm 2^{\frac{m}{2}}.$$

Since the Boolean functions $g(y) + L_b(y)$ for $y_1 = 0$ and $y_1 = 1$ have the same quadratic terms, it follows from (1) that $G_0(b), G_1(b) \in \{0, \pm 2^{m-1-\frac{r}{2}}\}$ for an even integer r with $0 \leq r \leq (m-1)$. By the equality $G_0(b) + G_1(b) = \pm 2^{\frac{m}{2}}$, it is clear that the product of $G_0(b)$ and $G_1(b)$ must be zero, i.e., $(G_0(b), G_1(b)) \in \{(0, \pm 2^{\frac{m}{2}}), (\pm 2^{\frac{m}{2}}, 0)\}$, since if $|G_0(b)| = |G_1(b)| = 2^{\frac{m}{2}-1}$, then $r = m$, which is not

possible for functions on $m-1$ variables, and the other possibilities sum to zero. Each of these cases implies that $W_h(a,b) \in \{\pm 2^{\frac{n+m}{2}}\}$ and then $\pi\rho^R \bowtie I_{n+m}$.

Subcase 3. $\pi(n) = n$ *and* $\rho(1) \neq 1$*:* In this subcase, we have $h(x,y) = f(x) + g(y) + x_n(y_1 + y_{\rho(1)})$. As in the case where $\pi(n) \neq n$, $\rho(1) = 1$, letting

$$F_0(a) = \sum_{\substack{x\in\mathbb{F}_2^n \\ x_n=0}} (-1)^{f(x)+L_a(x)}, \quad F_1(a) = \sum_{\substack{x\in\mathbb{F}_2^n \\ x_n=1}} (-1)^{f(x)+L_a(x)},$$

one has

$$W_h(a,b) = W_g(b)F_0(a) + W_g(b + e_1 + e_{\rho(1)})F_1(a).$$

Following similar arguments as in the previous subcase, we have $(F_0(a), F_1(a)) \in \{(0, \pm 2^{\frac{n}{2}}), (\pm 2^{\frac{n}{2}}, 0)\}$, which implies $|W_h(a,b)| = 2^{\frac{n+m}{2}}$ and then $\pi\rho^R \bowtie I_{n+m}$.

Case (ii). For $(\pi(n)-n)(\rho(1)-1) \neq 0$, we have $h(x,y) = f(x)+g(y)+(x_{\pi(n)}y_{\rho(1)}+x_ny_1)$. In this case, we need to investigate $W_h(a,b)$ by explicit evaluations on $y_1, y_{\rho(1)}$ or on $x_n, x_{\pi(n)}$.

Considering the explicit values of $y_1, y_{\rho(1)}$ in the calculation of $W_g(b)$, we have, for any $u, v \in \mathbb{F}_2$,

$$\begin{aligned}\sum_{\substack{y_{\rho(1)}=u \\ y_1=v}} (-1)^{g(y)+L_b(y)} &= (-1)^{b_{\rho(1)}u+b_1v} \sum_{\hat{y}\in\mathbb{F}_2^{m-2}} (-1)^{g_{u,v}(\hat{y})+L_{\hat{b}}(\hat{y})} \\ &= (-1)^{b_{\rho(1)}u+b_1v} W_{g_{u,v}}(\hat{b}),\end{aligned}$$

where $g_{u,v}(\hat{y})$ is the restriction of $g(y)$ on $\Omega_{u,v} = \{y \in \mathbb{F}_2^m : y_1 = u, y_{\rho(1)} = v\}$, and $\hat{y}, \hat{b}$ are the vectors obtained by removing the 1-st and $\rho(1)$-th entries of y and b in $\mathbb{F}_2^m$, respectively. For simplicity, denote $G_{u,v}(b) = (-1)^{b_{\rho(1)}u+b_1v} W_{g_{u,v}}(\hat{b})$ and $\widetilde{F_{u,v}}(a) = W_f(a + ue_{\pi(n)} + ve_n)$ for $u, v \in \mathbb{F}_2$, where $e_{\pi(n)}, e_n$ are the $\pi(n)$-th, respectively, the n-th row of the dimension-n identity matrix.

Then

$$W_g(b) = G_{0,0}(b) + G_{0,1}(b) + G_{1,0}(b) + G_{1,1}(b) = \pm 2^{\frac{m}{2}} \tag{18}$$

and

$$\begin{aligned}&W_h(a,b) \\ &= \sum_{(x,y)\in\mathbb{F}_2^{n+m}} (-1)^{f(x)+g(y)+L_a(x)+L_b(y)+(x_{\pi(n)}y_{\rho(1)}+x_ny_1)} \\ &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+L_a(x)} \sum_{y\in\mathbb{F}_2^m} (-1)^{g(y)+L_b(y)+(x_{\pi(n)}y_{\rho(1)}+x_ny_1)} \\ &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+L_a(x)} \big[G_{0,0}(b) + (-1)^{x_n} G_{0,1}(b) \\ &\qquad\qquad + (-1)^{x_{\pi(n)}} G_{1,0}(b) + (-1)^{x_{\pi(n)}+x_n} G_{1,1}(b)\big] \\ &= G_{0,0}(b)\widetilde{F_{0,0}}(a) + G_{0,1}(b)\widetilde{F_{0,1}}(a) + G_{1,0}(b)\widetilde{F_{1,0}}(a) + G_{1,1}(b)\widetilde{F_{1,1}}(a).\end{aligned} \tag{19}$$

Similarly, for $(a,b) \in \mathbb{F}_2^{n+m}$ and $u, v \in \mathbb{F}_2$, define

$$\widetilde{G_{u,v}}(b) = W_g(b + u\varepsilon_1 + v\varepsilon_{\rho(1)}) \text{ and } F_{u,v}(a) = (-1)^{a_{\pi(n)}u+a_nv} W_{f_{u,v}}(\hat{a}),$$

where $\varepsilon_1, \varepsilon_{\rho(1)}$ are the first and $\rho(1)$-th row of the $m \times m$ identity matrix over $\mathbb{F}_2$. By the symmetry of $f(x)$ and $g(y)$ in $h(x, y)$, we have

$$W_h(a,b) = F_{0,0}(a)\widetilde{G_{0,0}}(b) + F_{0,1}(a)\widetilde{G_{0,1}}(b) + F_{1,0}(a)\widetilde{G_{1,0}}(b) + F_{1,1}(a)\widetilde{G_{1,1}}(b).$$

Below we investigate the necessary and sufficient condition to have $|W_h(a,b)| = 2^{\frac{n+m}{2}}$, for all $(a,b) \in \mathbb{F}_2^{n+m}$.

According to Proposition 3.4, for even $m \geq 4$, the values of $G_{u,v}(b)$ as b ranges through $\mathbb{F}_2^m$ can be divided into two subcases: three of $G_{u,v}(b)$ are zero and the remaining one is $\pm 2^{\frac{m}{2}}$, which is equivalent to the fact that $g(y)$ satisfies the WHC on $(1, \rho(1))$; all $G_{u,v}(b)$ are equal to $\pm 2^{\frac{m-2}{2}}$ with three of them having the same sign and the fourth one having the opposite sign.

For the first subcase, it is easily seen that

$$G_{0,0}(b)\widetilde{F_{0,0}}(a) + G_{0,1}(b)\widetilde{F_{0,1}}(a) + G_{1,0}(b)\widetilde{F_{1,0}}(a) + G_{1,1}(b)\widetilde{F_{1,1}}(a) = \pm 2^{\frac{n+m}{2}}$$

since only one term in the sum is nonzero.

For the second subcase, for any $u, v \in \mathbb{F}_2$ and $(a,b) \in \mathbb{F}_2^{n+m}$, we have

$$|G_{u,v}(b)| = 2^{\frac{m-2}{2}} \text{ and } |G_{u,v}(b)\widetilde{F_{u,v}}(a)| = 2^{\frac{n+m-2}{2}}.$$

Denote $\eta_{u,v}(a,b) = G_{u,v}(b)\widetilde{F_{u,v}}(a)/2^{\frac{n+m-2}{2}}$ for $u, v \in \mathbb{F}_2$. Then

$$G_{0,0}(b)\widetilde{F_{0,0}}(a) + G_{0,1}(b)\widetilde{F_{0,1}}(a) + G_{1,0}(b)\widetilde{F_{1,0}}(a) + G_{1,1}(b)\widetilde{F_{1,1}}(a) = \pm 2^{\frac{m+n}{2}}$$

if and only if for any $(a,b) \in \mathbb{F}_2^n$, $(\eta_{0,0}(a,b), \eta_{0,1}(a,b), \eta_{1,0}(a,b), \eta_{1,1}(a,b)) \in \{\pm(1,1,1,-1), \pm(1,1,-1,1), \pm(1,-1,1,1), \pm(-1,1,1,1)\}$. That is to say, for any $(a,b) \in \mathbb{F}_2^n$, three of the $\eta_{0,0}(a,b), \eta_{0,1}(a,b), \eta_{1,0}(a,b), \eta_{1,1}(a,b)$ have the same sign, and the fourth one has the opposite sign. Therefore, $W_h(a,b) = \pm 2^{\frac{m+n}{2}}$ if only if

$$\prod_{u,v \in \mathbb{F}_2} G_{u,v}(b) W_f(a + ue_{\pi(n)} + ve_n) = -2^{2n+2m-4}, \tag{20}$$

which, by the fact that $\prod_{u,v \in \mathbb{F}_2} G_{u,v}(b) = -2^{2(m-2)}$, is equivalent to

$$\prod_{u,v \in \mathbb{F}_2} W_f(a + ue_{\pi(n)} + ve_n) = 2^{2n}, \text{ for any } a \in \mathbb{F}_2^n,$$

i.e., $f(x)$ satisfies the WHC on $(1, \rho(1))$.

Combining the above two subcases, we see that in the case of$(\pi(n) - n)(\rho(1) - 1) \neq 0$, if one of $f(x)$ and $g(y)$ satisfies the WHC, then $h(x,y)$ is bent on $\mathbb{F}_2^{n+m}$. In addition, when none of them satisfies the WHC, according to Proposition 3.4 (ii), the decompositions of $f(x)$ and $g(y)$ are all bent functions. In this case, since $\prod_{u,v \in \mathbb{F}_2} G_{u,v}(b) = -2^{2(m-2)}$ and $\prod_{u,v \in \mathbb{F}_2} F_{u,v}(a) = -2^{2(n-2)}$, it is easy to verify that $h(x,y)$ cannot be bent. The desired claims in Case (ii) thus follow. □

Below we provide a theorem for $n, m \geq 4$, odd n and even m, about the extension. Since the proof is rather similar to the prior one, we omit it.

Theorem 3.6 *For integers $n, m \geq 4$ with odd n and even m, let $\pi \in IS_n$, $\rho \in IS_m$ and define $f(x) = Q_\pi(x) + Q_{I_n}(x)$ and $g(y) = Q_\rho(y) + Q_{I_m}(y)$. Then $\pi\rho^R$ is compatible with I_{n+m} if one of the following conditions holds:*

(i) $\rho(1) = 1$*; or*

(ii) $(\rho(1) - 1)(\pi(n) - n) \neq 0$ *and for any* $(a, b) \in \mathbb{F}_2^{n+m}$,

$$\prod_{u,v \in \mathbb{F}_2} W_{g_{u,v}}(\hat{b}) W_f(a + ue_{\pi(n)} + ve_n) \in \left\{0, -2^{2n+2m-6}\right\},$$

where $\hat{b}$ *is the dimension-*$(m-2)$ *vector derived from* b *by removing its first and* $\rho(1)$*-th entries.*

In the following subsection we conduct a comprehensive analysis of compatible sets for $n = 4$. The analysis discusses relations and properties of all permutations in IS_4 and lists all maximal compatible sets in dimension 4. These results are useful for the recursive construction in Subsection 3.3.

3.2 Compatible sets for $n = 4$

When $n = 4$, by an exhaustive search we obtain all the permutations that are compatible with the identity permutation I_4 as below:

$$\begin{aligned}
&\rho_1 = [3,2,4,1], \quad \rho_2 = [2,4,1,3], \quad \rho_3 = [3,4,1,2], \quad \rho_4 = [2,4,3,1],\\
&\rho_5 = [3,1,4,2], \quad \rho_6 = [1,3,4,2], \quad \rho_7 = [4,2,1,3], \quad \rho_8 = [2,1,4,3],\\
&\rho_9 = [4,1,3,2], \ \rho_{10} = [2,3,1,4], \ \rho_{11} = [1,4,2,3], \ \rho_{12} = [3,1,2,4].
\end{aligned}$$

Among these permutations, it is easily seen that

$$\rho_{11} = \widetilde{\rho_1}, \ \rho_5 = \widetilde{\rho_2}, \ \rho_8 = \widetilde{\rho_3}, \ \rho_6 = \widetilde{\rho_4}, \ \rho_{12} = \widetilde{\rho_7}, \rho_{10} = \widetilde{\rho_9} \tag{21}$$

and

$$\begin{aligned}
&\rho_5 = \rho_2^{-1}, \ \rho_3^{-1} = \rho_3, \ \rho_8 = \rho_8^{-1},\\
&\rho_7 = \rho_1^{-1} = \rho_1^2, \ \rho_9 = \rho_4^{-1} = \rho_4^2, \rho_{11} = \rho_6^{-1} = \rho_6^2, \ \rho_{12} = \rho_{10}^{-1} = \rho_{10}^2.
\end{aligned} \tag{22}$$

By Lemma 3.2 (i)-(ii) and Equations (21)–(22), the following three chains of permutations are compatible with I_4:

$$\begin{aligned}
&\rho_1 \overset{\text{rev}}{\longleftrightarrow} \rho_{11} \overset{\text{inv}}{\longleftrightarrow} \rho_6 \overset{\text{rev}}{\longleftrightarrow} \rho_4 \overset{\text{inv}}{\longleftrightarrow} \rho_9 \overset{\text{rev}}{\longleftrightarrow} \rho_{10} \overset{\text{inv}}{\longleftrightarrow} \rho_{12} \overset{\text{rev}}{\longleftrightarrow} \rho_7 \overset{\text{inv}}{\longleftrightarrow} \rho_1,\\
&\rho_2 \overset{\text{rev}}{\longleftrightarrow} \rho_5 \overset{\text{inv}}{\longleftrightarrow} \rho_2,\\
&\rho_3 \overset{\text{rev}}{\longleftrightarrow} \rho_8 \overset{\text{inv}}{\longleftrightarrow} \rho_8 \overset{\text{rev}}{\longleftrightarrow} \rho_3.
\end{aligned}$$

By Lemma 3.2 (iii), $\pi \bowtie \pi^{-1}$ if and only if $I_n \bowtie \pi^2$, where $\pi^2 = \pi \circ \pi$. Then, by Equation (22), $\rho_1 \bowtie \rho_7, \rho_4 \bowtie \rho_9, \rho_6 \bowtie \rho_{11}, \rho_{10} \bowtie \rho_{12}$, creating four examples of compatible sets of size 3. More work is needed to get a compatible set of larger

size in which any two permutations are compatible. Starting from each of these pairs, one needs to find a new permutation compatible with the existing ones from the remaining permutations, and repeat this process to obtain maximal compatible sets for $n = 4$.

For instance, starting from ρ_1, ρ_7, one can first add ρ_3 since the permutations $\rho_1^{-1} \circ \rho_3 = \rho_7 \circ \rho_3 = \rho_6$ and $\rho_7^{-1} \circ \rho_3 = \rho_1 \circ \rho_3 = \rho_9$ are compatible with I_4. This gives us a compatible set $\{I_4, \rho_1, \rho_3, \rho_7\}$. To add a new permutation, say ρ, we need to choose $\rho \in IS_4$ and check whether it is compatible with the existing permutations ρ_1, ρ_3, ρ_7.

To facilitate the calculation, we provide Table 1 to look up $\rho_i^{-1} \circ \rho_j$ for $1 \le i, j \le 12$, where "0" indicates $\rho_i^{-1} \circ \rho_j = I_4$, "–" indicates $\rho_i^{-1} \circ \rho_j \notin \{\rho_1, \rho_2, \ldots, \rho_{12}\}$ (i.e., $\rho_i^{-1} \circ \rho_j$ is not compatible with I_4), and k in the entry of the i-th row and j-th column in Table 1 indicates $\rho_i^{-1} \circ \rho_j = \rho_k$. Since $(\rho_i^{-1} \circ \rho_j)^{-1} = \rho_j^{-1} \circ \rho_i$, Table 1 gives all information about the compatibility between permutations in IS_4. From Table 1, for any ρ_i, ρ_j, one can easily verify whether $\rho_i^{-1} \circ \rho_j$ belongs to IS_4. It is readily seen that the two permutations ρ_2, ρ_5 are not compatible with any permutation in IS_4. Furthermore, since $Q_\pi(x) = Q_{\widetilde{\pi}}(x)$, no permutation π can be compatible with its reverse $\widetilde{\pi}$.

Continuing with the compatible set $\{I_4, \rho_1, \rho_3, \rho_7\}$, we see that ρ_6 is compatible with the existing permutations in this set since $\rho_6^{-1} \circ \rho_1 = \rho_4$, $\rho_6^{-1} \circ \rho_3 = \rho_{10}$ and $\rho_6^{-1} \circ \rho_7 = \rho_3$, yielding a compatible set $\{I_4, \rho_1, \rho_3, \rho_7, \rho_6\}$. For the remaining permutations $\rho_2, \rho_4, \rho_5, \rho_8, \rho_9, \rho_{10}, \rho_{11}, \rho_{12}$, from Table 1 we see that ρ_2, ρ_5 should be excluded instantly, and that, due to mutual incompatibility, ρ_1 excludes ρ_{11}, ρ_3 excludes ρ_8, ρ_6 excludes ρ_4, and ρ_7 excludes ρ_{12}. Hence, we can further add ρ_9 or ρ_{10} to the compatible set, leading to $\{I_4, \rho_1, \rho_3, \rho_7, \rho_6, \rho_9\}$ or $\{I_4, \rho_1, \rho_3, \rho_7, \rho_6, \rho_{10}\}$ (as the first two in Table 2). Since ρ_9 is incompatible with ρ_{10}, no more permutations can be added to these two compatible sets. As a matter of fact, according to the upper bound (8) by Paterson [20], they are maximal compatible sets for $n = 4$.

As shown in Table 1, the two permutations ρ_2, ρ_5 are not compatible with any permutations in IS_4. For each permutation $\rho_i \bowtie I_4$, either ρ_i or its reverse $\widetilde{\rho_i}$ can be included in a compatible set. Therefore, there are in total 32 compatible sets for $n = 4$, which are listed in Table 2. They have the maximum size due to the upper bound in (8). Note that all these maximal compatible sets give the same spreading matrix $\mathbf{\Phi}$ defined in (3) (under a permutation of $\mathbf{\Phi}_l$ in $\mathbf{\Phi}$) since for each permutation $\rho \in IS_4$ taken from a compatible set, the spreading sequences $\mathbf{a}_\rho^j$ and $\mathbf{a}_{\widetilde{\rho}}^j$ are identical due to the fact that $Q_\rho(x) = Q_{\widetilde{\rho}}(x)$.

At the end of this section, we discuss the difficulty of the Main Problem 1.

	1	2	3	4	5	6	7	8	9	10	11	12
1	0	-	6	10	-	9	1	4	3	8	-	11
2	-	0	-	-	-	-	-	-	-	-	-	-
3	11	-	0	7	-	12	4	-	10	9	1	6
4	12	-	1	0	-	-	8	11	4	6	7	3
5	-	-	-	-	0	-	-	-	-	-	-	-
6	4	-	10	-	-	0	3	9	12	7	6	8
7	7	-	9	8	-	3	0	10	6	4	12	-
8	9	-	-	6	-	4	12	0	1	11	10	7
9	3	-	12	9	-	10	11	7	0	-	8	1
10	8	-	4	11	-	1	9	6	-	0	3	10
11	-	-	7	1	-	11	10	12	8	3	0	9
12	6	-	11	3	-	8	-	1	7	12	4	0

Table 1: Compositions $\rho_i^{-1} \circ \rho_j$ for $1 \leq i, j \leq 12$

$\{I_4, \rho_1, \rho_3, \rho_6, \rho_7, \rho_9\}$	$\{I_4, \rho_1, \rho_3, \rho_6, \rho_7, \rho_{10}\}$	$\{I_4, \rho_4, \rho_7, \rho_8, \rho_{10}, \rho_{11}\}$
$\{I_4, \rho_3, \rho_4, \rho_7, \rho_{10}, \rho_{11}\}$	$\{I_4, \rho_6, \rho_8, \rho_9, \rho_{11}, \rho_{12}\}$	$\{I_4, \rho_3, \rho_6, \rho_9, \rho_{11}, \rho_{12}\}$
$\{I_4, \rho_1, \rho_6, \rho_8, \rho_{10}, \rho_{12}\}$	$\{I_4, \rho_1, \rho_3, \rho_6, \rho_{10}, \rho_{12}\}$	$\{I_4, \rho_1, \rho_6, \rho_7, \rho_8, \rho_{10}\}$
$\{I_4, \rho_3, \rho_4, \rho_{10}, \rho_{11}, \rho_{12}\}$	$\{I_4, \rho_4, \rho_8, \rho_{10}, \rho_{11}, \rho_{12}\}$	$\{I_4, \rho_1, \rho_3, \rho_4, \rho_{10}, \rho_{12}\}$
$\{I_4, \rho_6, \rho_8, \rho_{10}, \rho_{11}, \rho_{12}\}$	$\{I_4, \rho_6, \rho_7, \rho_8, \rho_9, \rho_{11}\}$	$\{I_4, \rho_4, \rho_7, \rho_8, \rho_9, \rho_{11}\}$
$\{I_4, \rho_3, \rho_6, \rho_7, \rho_9, \rho_{11}\}$	$\{I_4, \rho_1, \rho_4, \rho_8, \rho_9, \rho_{12}\}$	$\{I_4, \rho_1, \rho_3, \rho_4, \rho_9, \rho_{12}\}$
$\{I_4, \rho_3, \rho_4, \rho_9, \rho_{11}, \rho_{12}\}$	$\{I_4, \rho_3, \rho_4, \rho_7, \rho_9, \rho_{11}\}$	$\{I_4, \rho_3, \rho_6, \rho_{10}, \rho_{11}, \rho_{12}\}$
$\{I_4, \rho_4, \rho_8, \rho_9, \rho_{11}, \rho_{12}\}$	$\{I_4, \rho_1, \rho_4, \rho_7, \rho_8, \rho_9\}$	$\{I_4, \rho_1, \rho_3, \rho_4, \rho_7, \rho_9\}$
$\{I_4, \rho_1, \rho_3, \rho_4, \rho_7, \rho_{10}\}$	$\{I_4, \rho_6, \rho_7, \rho_8, \rho_{10}, \rho_{11}\}$	$\{I_4, \rho_3, \rho_6, \rho_7, \rho_{10}, \rho_{11}\}$
$\{I_4, \rho_1, \rho_4, \rho_7, \rho_8, \rho_{10}\}$	$\{I_4, \rho_1, \rho_4, \rho_8, \rho_{10}, \rho_{12}\}$	$\{I_4, \rho_1, \rho_6, \rho_7, \rho_8, \rho_9\}$
$\{I_4, \rho_1, \rho_3, \rho_6, \rho_9, \rho_{12}\}$	$\{I_4, \rho_1, \rho_6, \rho_8, \rho_9, \rho_{12}\}$	

Table 2: All the 32 maximal compatible sets for $n = 4$.

Remark 3.7. *The Main Problem 1 can be reformulated as a clique problem. Define a graph G_n such that a vertex in G_n denotes a permutation in S_n and an edge between two vertices in G_n represents that the corresponding two permutations in S_n are compatible. Recall from Lemma 3.2 (iii) that $\pi \bowtie \sigma$ if and only if $I_n \bowtie (\pi^{-1} \circ \sigma)$. Hence the graph G_n is an undirected regular graph with $n!$ vertices (where each vertex has the same number of neighbours). In practice, edges in G_n can be created by first calculating IS_n and then drawing an edge between two vertices π and ρ if $\pi^{-1} \circ \sigma \in IS_n$ (as done for $n = 4$ in this section). In essence, the Main Problem 1 asks to determine or approximate the size of the maximum clique in the regular graph G_n and to find an L-clique in G_n with L as large as possible.*

Note that determining the size of the maximum clique in an arbitrarily given graph is NP-hard, and that there does not even exist any polynomial-time $N^{1-\epsilon}$-approximation algorithm (which, upon the input of a graph G of N vertices, outputs a clique of size that is always at least the maximum clique size of

G divided by $N^{1-\epsilon}$) for any constant ϵ [13]. Similarly for regular graphs, it was shown in [1] *that there exists no polynomial-time algorithm that approximates the maximum size of cliques in a regular graph within a factor of $N^{1/2-\epsilon}$ for any constant ϵ. In the theory of computational complexity, existing results show that determining or even approximating the maximum clique size of a regular graph is NP-hard. Computationally, the Bron-Kerbosch algorithm, which is one of the most efficient algorithms that lists all maximal cliques in a graph G of N vertices, has worst-case running time $O(3^{N/3})$* [2].

For the specific regular graph G_n derived from S_n, with the rapid growth of $N = n!$ as n increases, we believe that the Main Problem 1 is computationally intractable for relatively small integers n larger than 10. *For instance, for $n = 7$, the regular graph G has in total* 5040 *vertices with degree* 3857 *for each vertex. The authors of* [14] *included search results for $4 \leq n \leq 9$ with the Bron-Kerbosch algorithm, where they provided only partial search results for $n = 7, 8, 9$.*

3.3 Extending compatible sets from $n = 4$ to $n = 4m$

In this subsection we shall recursively construct compatible sets in dimension $4m$ for any positive integer $m \geq 2$. We first consider extending a permutation $\pi \in IS_n$ with a permutation ρ taken from $IS_4 = \{\rho_1, \rho_2, \ldots, \rho_{12}\}$, based on the conditions in Theorems 3.5 and 3.6.

Proposition 3.8. *Let π be a permutation in IS_n. Then the permutation $\pi\rho^R$ is compatible with I_{n+4} for any ρ in the set $\{\rho_3, \rho_4, \rho_6, \rho_8, \rho_9, \rho_{11}\} = \{[3,4,1,2], [2,4,3,1], [1,3,4,2], [2,1,4,3], [4,1,3,2], [1,4,2,3]\}$.*

Proof By Theorems 3.5 and 3.6 Case (i), it is readily seen that $\pi\rho^R \bowtie I_{n+4}$ for $\rho = \rho_6, \rho_{11}$ since $\rho_6(1) = \rho_{11}(1) = 1$. For the other permutations, we have

$$\begin{aligned}
Q_{\rho_3}(y) + Q_{I_4}(y) &= y_2y_3 + y_4y_1,\\
Q_{\rho_4}(y) + Q_{I_4}(y) &= y_1y_2 + y_2y_3 + y_2y_4 + y_3y_1,\\
Q_{\rho_8}(y) + Q_{I_4}(y) &= y_2y_3 + y_1y_4,\\
Q_{\rho_9}(y) + Q_{I_4}(y) &= y_1y_2 + y_3y_4 + y_4y_1 + y_1y_3.
\end{aligned}$$

For each permutation $\rho \in \{\rho_3, \rho_4, \rho_8, \rho_9\}$, it can be easily verified that the function $g(y) = Q_\rho(y) + Q_{I_4}(y)$ restricted on $y_{\rho(1)} = i, y_1 = j$ for any $i, j \in \mathbb{F}_2$ is a linear function on $\mathbb{F}_2^2$, implying that the condition in Theorems 3.5 and 3.6 Case (ii) is satisfied. It thus follows that $\pi\rho^R \bowtie I_{n+4}$. □

We now focus on the case of even n, and we study the extensions on the right with the remaining permutations $\rho_1, \rho_2, \rho_5, \rho_7, \rho_{10}, \rho_{12}$ in IS_4. For this case, the following conditions will be needed.

Proposition 3.9. *Let $\pi \in IS_n$ with $\pi(n) \neq n$. Then for a permutation $\rho \in \{\rho_1, \rho_2, \rho_5, \rho_7, \rho_{10}, \rho_{12}\}$, the permutation $\pi\rho^R$ is compatible with I_{n+4} if and only if $f(x) = Q_\pi(x) + Q_{I_n}(x)$ fulfills the WHC on $(\pi(n), n)$.*

Proof Note that for $\rho \in \{\rho_1, \rho_2, \rho_5, \rho_7, \rho_{10}, \rho_{12}\}$, the quadratic functions $Q_\rho(y) + Q_{I_4}(y)$ are given as follows:

$$\begin{aligned}
Q_{\rho_1}(y) + Q_{I_4}(y) &= y_1y_2 + y_1y_4 + y_2y_4 + y_3y_4,\\
Q_{\rho_2}(y) + Q_{I_4}(y) &= y_1y_2 + y_1y_3 + y_1y_4 + y_2y_3 + y_2y_4 + y_3y_4,\\
Q_{\rho_5}(y) + Q_{I_4}(y) &= y_1y_2 + y_1y_3 + y_1y_4 + y_2y_3 + y_2y_4 + y_3y_4,\\
Q_{\rho_7}(y) + Q_{I_4}(y) &= y_1y_3 + y_2y_3 + y_2y_4 + y_3y_4,\\
Q_{\rho_{10}}(y) + Q_{I_4}(y) &= y_1y_2 + y_1y_3 + y_1y_4 + y_3y_4,\\
Q_{\rho_{12}}(y) + Q_{I_4}(y) &= y_1y_3 + y_2y_3 + y_2y_4 + y_3y_4.
\end{aligned}$$

The calculations for all ρ in the set are similar, and we will take $\rho = \rho_1 = [3, 2, 4, 1]$ as an instance. In this case, letting $\pi' = \pi\rho^R$, $f(x) = Q_{I_n}(x) + Q_\pi(x)$, and $g(y) = Q_{\rho_1}(y) + Q_{I_4}(y)$, we have

$$\begin{aligned}
h(x,y) &= Q_{I_{n+4}}(x,y) + Q_{\pi'}(x,y) = f(x_1,\ldots,x_n) + g(y_1,y_2,y_3,y_4) + x_{\pi(n)}y_3 + x_ny_1\\
&= f(x_1,\ldots,x_n) + y_1y_2 + y_1y_4 + y_2y_4 + y_3y_4 + x_{\pi(n)}y_3 + x_ny_1.
\end{aligned}$$

For $g(y) = y_1y_2 + y_3y_4 + y_2y_4 + y_4y_1$, the function $g_{i,j}(\hat{y}) = g|_{y_3=i,y_1=j} = y_2y_4 + j(y_2 + y_4) + iy_4$ contains the quadratic term y_2y_4 for any $(i,j) \in \mathbb{F}_2^2$. Since $\pi(n) \neq n$, the permutation π' is compatible with I_{n+4} if and only if the condition in Theorem 3.5 (ii) is satisfied. Below we investigate the explicit value of the product in Theorem 3.5 (ii).

Denote

$$W_{h_y}(a,b) = \sum_{x\in\mathbb{F}_2^n} (-1)^{h(x,y)+L_a(x)+L_b(y)} = (-1)^{L_b(y)} \sum_{x\in\mathbb{F}_2^n} (-1)^{h(x,y)+L_a(x)}.$$

Table 3 lists the values of W_{h_y}, for all $y \in (y_1,y_2,y_3,y_4) \in \mathbb{F}_2^4$, where $\alpha = (-1)^{b_1}$, $\beta = (-1)^{b_2}$, $\gamma = (-1)^{b_3}$, and $\delta = (-1)^{b_4}$.

From Table 3, the Walsh-Hadamard transform of h at (a,b) can be expressed as follows:

$$\begin{aligned}
W_h(a,b) &= \sum_{y\in\mathbb{F}_2^4} W_{h_y}(a,b)\\
&= W_f(a)(1+\delta+\beta(1-\delta)) + W_f(a+e_{\pi(n)})\gamma(1-\delta+\beta(1+\delta))\\
&\quad + W_f(a+e_n)\alpha(1-\delta-\beta(1+\delta))\\
&\quad + W_f(a+e_n+e_{\pi(n)})\alpha\gamma(1+\delta-\beta(1-\delta)).
\end{aligned}$$

y_1	y_2	y_3	y_4	$W_{h_y}(a,b)$
0	0	0	0	$W_f(a)$
0	0	0	1	$W_f(a)\delta$
0	0	1	0	$W_f(a+e_{\pi(n)})\gamma$
0	0	1	1	$W_f(a+e_{\pi(n)})\gamma\delta(-1)$
0	1	0	0	$W_f(a)\beta$
0	1	0	1	$W_f(a)\beta\delta(-1)$
0	1	1	0	$W_f(a+e_{\pi(n)})\beta\gamma$
0	1	1	1	$W_f(a+e_{\pi(n)})\beta\gamma\delta$
1	0	0	0	$W_f(a+e_n)\alpha$
1	0	0	1	$W_f(a+e_n)\alpha\delta(-1)$
1	0	1	0	$W_f(a+e_n+e_{\pi(n)})\alpha\gamma$
1	0	1	1	$W_f(a+e_n+e_{\pi(n)})\alpha\gamma\delta$
1	1	0	0	$W_f(a+e_n)\alpha\beta(-1)$
1	1	0	1	$W_f(a+e_n)(-1)\alpha\beta\delta$
1	1	1	0	$W_f(a+e_n+e_{\pi(n)}(-1)\alpha\beta\gamma$
1	1	1	1	$W_f(a+e_n+e_{\pi(n)})\alpha\beta\gamma\delta$

Table 3: The Walsh-Hadamard transform of h

Recalling the expression of $W_h(a,b)$ from (19) as below,

$$W_h(a,b) = G_{0,0}(b)\widetilde{F_{0,0}}(a) + G_{0,1}(b)\widetilde{F_{0,1}}(a) + G_{1,0}(b)\widetilde{F_{1,0}}(a) + G_{1,1}(b)\widetilde{F_{1,1}}(a),$$

where $\widetilde{F_{i,j}}(a) = W_f(a + ie_{\pi(n)} + je_n)$ for $i,j \in \mathbb{F}_2$, we see that

$$\begin{aligned} G_{0,0}(b) &= (1+\delta+\beta(1-\delta)), \quad G_{1,0}(b) = \gamma(1-\delta+\beta(1+\delta)), \\ G_{0,1}(b) &= \alpha(1-\delta-\beta(1+\delta)), \; G_{1,1}(b) = \alpha\gamma(1+\delta-\beta(1-\delta)). \end{aligned}$$

Notice that

$$\begin{aligned} \prod_{i,j\in\{0,1\}} G_{i,j}(b) &= \alpha^2\gamma^2((1+\delta)^2 - \beta^2(1-\delta)^2)((1-\delta)^2 - \beta^2(1+\delta)^2) \\ &= -((1+\delta)^2 - (1-\delta)^2)^2 = -2^4. \end{aligned}$$

Thus, it follows from Theorem 3.5 (ii) that $h(x,y)$ is bent if and only if $f(x)$ satisfies the WHC

$$\prod_{i,j\in\{0,1\}} \widetilde{F_{i,j}}(a) = 2^{2n}.$$

Similarly as $\rho = \rho_1$, the functions $g_{i,j}(\hat{y})$ for $i,j \in \mathbb{F}_2$ are all bent. Hence for $\rho \in \{\rho_2, \rho_5, \rho_7, \rho_{10}, \rho_{12}\}$, $\pi\rho^R \bowtie I_{n+4}$ if and only if $f(x)$ satisfies the WHC. □

For even n, Theorem 3.5, Proposition 3.8 and Proposition 3.9 characterize the required properties of $\pi \in S_n$ when it is extended with $\rho_i \in IS_4$ on the right side. For odd n, we have Theorem 3.6 and Proposition 3.8. Below we shall investigate how one can obtain permutations in S_{4m} for $m \geq 2$ that are compatible with I_{4m}, when π is picked from IS_4.

We start with the case of $m = 2$. For the 12 permutations in IS_4, by a routine calculation, the sets of ρ_i for $1 \le i \le 12$ such that $f(x) = Q_{I_4}(x) + Q_{\rho_i}(x)$ satisfies the WHC are given as follows,

$$S_{WHC} = \{\rho_1, \rho_3, \rho_8, \rho_9, \rho_{10}, \rho_{12}\}.$$

Below we shall recursively extend the permutations in IS_4 except for ρ_2, ρ_5 (which cannot be extended multiple times), thereby obtaining permutations in $IS_{4(m+1)}$ for $m = 1, 2, 3, \ldots$. Denote by

$$\pi\rho^{R_m} = \pi\overbrace{\rho^R \cdots \rho^R}^{m}$$

the right extension on π with ρ by m times. When $\pi = \rho$, we denote $\pi\rho^{R_m}$ as $\rho^{R_{m+1}}$. We have the following result.

Theorem 3.10 *Let $IS_4 = \{\rho_1, \rho_2, \ldots, \rho_{12}\}$. Then, for any $\rho_i \in IS_4 \setminus \{\rho_2, \rho_5\}$ and any integer $m \ge 2$, the permutation $\rho_i^{R_m}$ is compatible with I_{4m}.*

Proof By Proposition 3.8, if $\rho_i \in \{\rho_3, \rho_4, \rho_6, \rho_8, \rho_9, \rho_{11}\}$, then $\rho_i^{R_{m-1}} \bowtie I_{4(m-1)}$ immediately implies $\rho_i^{R_m} \bowtie I_{4m}$. For the permutations ρ_{10}, ρ_{12}, since $\rho_{10}(4) = \rho_{12}(4) = 4$, it follows from Theorem 3.5 (i) that the permutations $\rho_{10}^{R_m} = \rho_{10}(\rho_{10}^{R_{m-1}})^R$ and $\rho_{12}^{R_m} = \rho_{12}(\rho_{12}^{R_{m-1}})^R$ are compatible with I_{4m}.

We will prove the statement for the remaining permutations ρ_1, ρ_7, by induction on m. We start with the discussion for ρ_1.

For $m = 2$, it is clear that

$$\rho_1^{R_2} = \rho_1\rho_1^R \bowtie I_8.$$

Suppose $\rho_1^{R_k}$ is compatible with I_{4k} for an integer k with $2 \le k < m$. Then we need to show that $\rho_i^{R_{k+1}}$ is compatible with $I_{4(k+1)}$. By Proposition 3.9, the assumption $\rho_1^{R_k} \bowtie I_{4k}$ implies that the bent function

$$f_k(x) = Q_{\rho_1^{R_k}}(x) + Q_{I_{4k}}(x)$$

satisfies the WHC on $(\pi(4k), 4k)$, where $\pi = \rho_1^{R_k}$. This implies that for any $a \in \mathbb{F}_2^{4k}$,

$$\frac{W_{f_k}(a + e_{4k} + e_{\pi(4k)})}{W_{f_k}(a)} = \frac{W_{f_k}(a + e_{4k})}{W_{f_k}(a + e_{\pi(4k)})}. \tag{23}$$

Below we shall show that the bent function

$$f_{k+1}(x) = Q_{\rho_1^{R_{k+1}}}(x) + Q_{I_{4(k+1)}}(x)$$

satisfies the WHC on $(\pi'(4(k+1)), 4(k+1))$, where $\pi' = \pi\rho_1^R = \rho_1^{R_{k+1}}$. Note that for integers $j = 1, 2, \ldots, 4k$, $\pi'(j) = \pi(j)$.

Recall from the proof of Proposition 3.9 that

$$\begin{aligned}
W_{f_{k+1}}(\overline{a}) &= (1+\delta)\Big(W_{f_k}(a) + \alpha\gamma W_{f_k}(a+e_{4k}+e_{\pi(4k)}) \\
&\qquad +\beta(\gamma W_{f_k}(a+e_{\pi(4k)}) - \alpha W_{f_k}(a+e_{4k}))\Big) \\
&\quad + (1-\delta)\Big(\beta(W_{f_k}(a) - \alpha\gamma W_{f_k}(a+e_{4k}+e_{\pi(4k)})) \\
&\qquad +\gamma W_{f_k}(a+e_{\pi(4k)}) + \alpha W_{f_k}(a+e_{4k})\Big) \\
&= (1+\delta)\Big(W_{f_k}(a)(1+\epsilon\alpha\gamma) + \beta W_{f_k}(a+e_{\pi(4k)})(\gamma-\epsilon\alpha)\Big) \\
&\quad + (1-\delta)\Big(\beta W_{f_k}(a)(1-\epsilon\alpha\gamma) + W_{f_k}(a+e_{\pi(4k)})(\gamma+\epsilon\alpha)\Big),
\end{aligned}$$

where $\overline{a} = (a_1, a_2, \ldots, a_{4k+4})$, $a = (a_1, a_2, \ldots, a_{4k})$, $\alpha = (-1)^{a_{4k+1}}, \beta = (-1)^{a_{4k+2}}, \gamma = (-1)^{a_{4k+3}}$, $\delta = (-1)^{a_{4k+4}}$, and ϵ denotes the division in (23) and takes the values ± 1. Therefore,

$$\begin{aligned}
&W_{f_{k+1}}(\overline{a} + e_{4(k+1)} + e_{\pi'(4(k+1))}) \\
&= (1-\delta)\Big(W_{f_k}(a)(1-\epsilon\alpha\gamma) + \beta W_{f_k}(a+e_{\pi(4k)})(\gamma+\epsilon\alpha)\Big) \\
&\quad + (1+\delta)\Big(\beta W_{f_k}(a)(1+\epsilon\alpha\gamma) + W_{f_k}(a+e_{\pi(4k)})(\gamma-\epsilon\alpha)\Big).
\end{aligned}$$

From here, it is clear that $W_{f_{k+1}}(\overline{a} + e_{4(k+1)} + e_{\pi'(4(k+1))}) = \beta W_{f_{k+1}}(\overline{a})$. In the same way,

$$\begin{aligned}
W_{f_{k+1}}(\overline{a} + e_{\pi'(4(k+1))}) &= (1+\delta)\Big(W_{f_k}(a)(1-\epsilon\alpha\gamma) + \beta W_{f_k}(a+e_{\pi(4k)})(\gamma+\epsilon\alpha)\Big) \\
&\quad + (1-\delta)\Big(\beta W_{f_k}(a)(1+\epsilon\alpha\gamma) + W_{f_k}(a+e_{\pi(4k)})(\gamma-\epsilon\alpha)\Big),
\end{aligned}$$

while

$$\begin{aligned}
W_{f_{k+1}}(\overline{a} + e_{4(k+1)})) &= (1-\delta)\Big(W_{f_k}(a)(1+\epsilon\alpha\gamma) + \beta W_{f_k}(a+e_{\pi(4k)})(\gamma-\epsilon\alpha)\Big) \\
&\quad + (1+\delta)\Big(\beta W_{f_k}(a)(1-\epsilon\alpha\gamma) + W_{f_k}(a+e_{\pi(4k)})(\gamma+\epsilon\alpha)\Big).
\end{aligned}$$

It follows, therefore, that $W_{f_{k+1}}(\overline{a} + e_{\pi'(4(k+1))}) = \beta W_{f_{k+1}}(\overline{a} + e_{4(k+1)})$. This implies that $f_{k+1}(x)$ fulfills the WHC on $(\pi'(4(k+1)), 4(k+1))$. Therefore, $\rho_1^{R_{k+1}}$ is compatible with $I_{4(k+1)}$.

As for the permutation ρ_7, we have $\rho_7^{-1} = \rho_1$. According to (11), it follows that $(\rho_7\rho_7^R)^{-1} = (\rho_7^{-1})(\rho_7^{-1})^R = \rho_1\rho_1^R$ and recursively, $(\rho_7^{R_m})^{-1} = \rho_1^{R_m}$. Thus it follows from Lemma 3.2 (*ii*) that $\rho_7^{R_m} \bowtie I_{4m}$. □

In the following, we present a way to extend a maximal compatible set in dimension 4 (which has size 6) to a size-6 set in any dimension $4m$ for $m > 1$, by recursively adding a shift of itself.

Theorem 3.11 *Given any maximal compatible set* Π *in dimension* 4*, the set* $\{\rho^{R_m} : \rho \in \Pi\}$ *is a compatible set in dimension* $4m$ *for any integer* $m \geq 2$.

Proof Let $\pi, \sigma \in \Pi$. We know that $\pi \bowtie \sigma$ and $\pi, \sigma \notin \{\rho_2, \rho_5\}$. We shall show π^{R_m} is compatible with σ^{R_m}, equivalently, $(\pi^{R_m})^{-1} \circ \sigma^{R_m} \bowtie I_{4m}$.

From $\pi \bowtie \sigma$, we know $\pi^{-1} \circ \sigma \bowtie I_4$ and $\sigma^{-1} \circ \pi \bowtie I_4$. Without loss of generality, we may assume $\pi^{-1} \circ \sigma \bowtie I_4$. According to (11) and (10), we have

$$\begin{aligned}
(\pi^{R_m})^{-1} \circ \sigma^{R_m} &= (\pi^{R_{m-1}}\pi^R)^{-1} \circ \sigma^{R_m} \\
&= ((\pi^{R_{m-1}})^{-1}(\pi^{-1})^R) \circ \sigma^{R_m} \\
&= ((\pi^{R_{m-1}})^{-1}(\pi^{-1})^R) \circ (\sigma^{R_{m-1}}\sigma^R) \\
&= ((\pi^{R_{m-1}})^{-1} \circ \sigma^{R_{m-1}})(\pi^{-1} \circ \sigma)^R \\
&= ((\pi^{R_{m-2}})^{-1} \circ \sigma^{R_{m-2}})(\pi^{-1} \circ \sigma)^{R_2} \\
&= \dots \\
&= (\pi^{-1} \circ \sigma)^{R_m},
\end{aligned}$$

where the second equality follows from (11) and the fourth equation follows from (10). Notice that $\pi^{-1} \circ \sigma$ is compatible with I_4, $\pi^{-1} \circ \sigma$ is neither ρ_2 nor ρ_5 (as shown in Table 1). It follows from Theorem 3.10 that $(\pi^{-1} \circ \sigma)^{R_m}$ is compatible with I_{4m}, implying $(\pi^{R_m})^{-1} \circ \sigma^{R_m} \bowtie I_{4m}$, and then $\pi^{R_m} \bowtie \sigma^{R_m}$. Since π, σ are freely chosen from Π, one can easily see that the set $\{\rho^{R_m} : \rho \in \Pi\}$ is a compatible set. □

According to Table 2, Theorem 3.11 yields 32 compatible sets each consisting of 6 permutations in S_{4m} for all integers $m \geq 2$.

Remark 3.12. *For dimension $4m$, it is possible to consider other types of extension. For other extensions than repetition, to ensure newly extended permutations are still compatible, one needs to check the required condition as in Lemma 3.3. Specifically, when $\pi \bowtie \sigma$ and they are extendable by ρ_i, ρ_j, respectively, if both $\rho_j^{-1} \circ \rho_i$ and $\rho_i^{-1} \circ \rho_j$ require the WHC, then $\pi^{-1} \circ \sigma$ or $\sigma^{-1} \circ \pi$ must satisfy the corresponding WHC. Depending on the choice of permutations, additional checks may be required in the recursive extension. Some examples are given in Tables 8 and 9 in Appendix A.*

In Appendix A, we present several examples of compatible sets comprising six permutations in dimension $4m$ for $m = 2, 3, 4$.

4 Conclusion

In this paper, we propose a recursive construction of a codebook for uplink grant-free NOMA using GDJ sequences. The contributions are twofold: we establish the necessary and sufficient condition for a permutation of type $\pi\rho^R$ to be compatible with I_{n+m} when π is compatible with I_n, and ρ is compatible with I_m, respectively; and we recursively extend compatible sets of

4-dimensional permutations to compatible sets of $4m$-dimensional permutations. As a result, any compatible set in dimension 4 can be extended to a compatible set of the same size in dimension $4m$. The proposed approach allows for constructing many NOMA codebooks of $6N$ GDJ sequences of length $N = 2^{4m}$ and the lowest possible coherence $1/\sqrt{N}$ for integers $m \geq 1$. Our results complement the work of [15] regarding the construction of NOMA codebooks with large overloading factors, whereas the problem of improving the general upper bound remains open.

List of Abbreviations

NOMA	Non-Orthogonal Multiple Access
PAPR	Peak-to-Average Power Ratio
OFDM	Orthogonal Frequency-Division Multiplexing
RM	Reed-Muller
GDJ	Golay-Davis-Jedwab
WHC	Walsh-Hadamard Condition

Declarations

Availability of data and material

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Funding

The work of Chunlei Li, Constanza Riera, and Palash Sarkar was supported by the Research Council of Norway under Grant 311646/O70. The work of Chunlei Li was also supported in part by the UK Engineering and Physical Sciences Research Council under an international collaboration grant EP/Y000986/1 ('SORT'). The work of Pantelimon Stănică was partially sponsored by DoD.

Authors' contributions

All authors contributed equally to this work. All authors read and approved the final manuscript.

Acknowledgements

The authors would like to thank the editors for efficiently handling our paper and the reviewers for their careful reading, beneficial comments, and constructive suggestions. We thank Prof. Dibyendu Roy for his valuable input on our SageMath implementation. The fourth-named author worked on this problem during a visit to the Selmer Center at the University of Bergen. He thanks the center for the hospitality, support, and excellent working conditions.

References

[1] Brandes, U., Holm, E., Karrenbauer, A.: Cliques in regular graphs and the Core-Periphery problem in social networks. Combinatorial Optimization and Applications, Editors: Chan, TH., Li, M., Wang, L. **10043**, 175–186 (2016) https://doi.org/10.1007/978-3-319-48749-6_13

[2] Bron, C., Kerbosch, J.: Algorithm 457: finding all cliques of an undirected graph. Communications of the ACM **16**(9), 575–577 (1973) https://doi.org/10.1145/362342.362367

[3] Canteaut, A., Carlet, C., Charpin, P., Fontaine, C.: On cryptographic properties of the cosets of $RM(1, m)$, IEEE Trans. Inf. Theory **47**(4), 1494–1513 (2001) https://doi.org/10.1109/18.923730

[4] Dai, L., Wang, B., Ding, Z., Wang, Z., Chen, S., Hanzo, L.: A survey of non-orthogonal multiple access for 5G. IEEE Commun. Surveys and Tut. **20**(3), 2294–2323 (2018) https://doi.org/10.1109/COMST.2018.2835558

[5] Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge, 2021.

[6] Cusick, T. W., Stănică, P.: Cryptographic Boolean Functions and Applications (Ed. 2). Academic Press, San Diego, CA, 2017.

[7] Dai, L., Wang, B., Yuan, Y., Han, S., Chih-lin, I., Wang, Z.: Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends. IEEE Commun. Mag. **53**(9), 74–81 (2015) https://doi.org/10.1109/MCOM.2015.7263349

[8] Davis, J.A., Jedwab, J.: Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes. IEEE Trans. Inf. Theory **45**(7), 2397–2417 (1999) https://doi.org/10.1109/18.796380

[9] Ding, C.: Complex codebooks from combinatorial designs. IEEE Trans. Inf. Theory **52**(9), 4229–4235 (2006) https://doi.org/10.1109/TIT.2006.880058

[10] Ding, C., Feng, T.: A generic construction of complex codebooks meeting the Welch bound. IEEE Trans. Inf. Theory **53**(11), 4245–4250 (2007) https://doi.org/10.1109/TIT.2007.907343

[11] Garey, M., Johnson, D.S.: Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman and Company, 1979.

[12] Golay, M.J.E.: Multi-slit spectrometry∗. J. Opt. Soc. Am. **39**(6), 437–444 (1949) https://doi.org/10.1364/JOSA.39.000437

[13] Håstad, J.: Clique is hard to approximate within $n^{1-\epsilon}$. Acta Mathematica **182**, 105–142 (1999) https://doi.org/10.1007/BF02392825

[14] Liu, K., Zhou, Z., Adhikary, A.R., Luo, R.: New sets of non-orthogonal spreading sequences with low correlation and low PAPR using extended Boolean functions. Des. Codes Cryptogr. **91**, 3115–3139 (2023) https://doi.org/10.1109/LCOMM.2022.3194158

[15] Liu, K., Zhou, Z., Adhikary, A.R., Tang, C.: Large sets of binary spreading sequences with low correlation and low PAPR via Gold functions. IEEE Trans. Inf. Theory **70**(7), 5309–5322 (2024) https://doi.org/10.1109/TIT.2024.3379514

[16] Luo, G., Cao, X.: Two constructions of asymptotically optimal codebooks via the hyper Eisenstein sum. IEEE Trans. Inf. Theory **64**(10), 6498–6505 (2018) https://doi.org/10.1109/TIT.2017.2777492

[17] MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, 1977.

[18] Mesnager, S.: Bent Functions: Fundamentals and Results. Springer, 2016.

[19] Taleb, T., Kunz, A.: Machine type communications in 3GPP networks: potential, challenges, and solutions. IEEE Commun. Mag. **50**(3), 178–184 (2012) https://doi.org/10.1109/MCOM.2012.6163599

[20] Paterson, K.: Sequences for OFDM and Multi-Code CDMA: two problems in algebraic coding theory. Proceedings of Sequences and their Applications, ed. Helleseth, T, Kumar, P.V. and Yang, K. 46–71 (2002)

https://doi.org/10.1007/978-1-4471-0673-9_4

[21] Sustik, M., Tropp, J., Dhillon, I., Heath, R.: On the existence of equiangular tight frames. Linear Algebra and its Applications **426**(2-3), 619–635 (2007) https://doi.org/10.1016/j.laa.2007.05.043

[22] Tian, L., Liu, T., Li, Y.: New constructions of binary Golay spreading sequences for uplink grant-free NOMA. IEEE Commun. Lett. **26**(10), 2480–2484 (2022) https://doi.org/10.1109/LCOMM.2022.3194158

[23] Welch, L., Lower bounds on correlation of sequences. IEEE Trans. Inf. Theory **20**(3), 397–399 (1974) https://doi.org/10.1109/tit.1974.1055219

[24] Yu, N.Y.: Binary Golay spreading sequences and Reed-Muller codes for uplink grant-free NOMA. IEEE Trans. Commun. **69**(1), 276–290 (2021) https://doi.org/10.1109/TCOMM.2020.3031613

A Explicit examples of compatible sets for generating NOMA codebooks

The examples presented in this appendix were generated and verified using a computational script in SageMath. The script implements the exhaustive search for the base case of $n = 4$ and the recursive self-extension method described in Theorem 3.11 as well as mixed-extension methods.

A.1 Base case: maximal compatible sets for $n = 4$

The recursive construction starts with a maximal compatible set for $n = 4$, containing $L = 6$ permutations by exhaustion. Table 4 lists three such sets, Π_1, Π_2, and Π_3. The set Π_1 corresponds to the first set listed in Table 2, while Π_2 and Π_3 correspond to the fourth set and 27th set, respectively. These sets form the $m = 1$ base case, yielding codebooks of $K = 96$ sequences of length $N = 16$ with optimally low coherence $\mu(\mathbf{\Phi}) = 1/4$.

A.2 Recursive self-extension examples: $n = 4m$

For dimension $n = 4m$, Theorem 3.11 guarantees that the recursive self-extension of any base compatible set Π maintains compatibility. This yields a set of $L = 6$ permutations $\Pi^{R_m} = \{\rho^{R_m} \mid \rho \in \Pi\}$ in S_{4m}. Below we illustrate this with Π_1 for $m = 2, 3, 4$ as in Tables 5-7, respectively. Correspondingly, we obtain a $2^{4m} \times 6 \cdot 2^{4m}$ NOMA codebook of sequences with length 2^{4m} and PAPR upper bouned by 2 and optimally low coherrence $1/2^{2m}$.

Table 4: Example maximal compatible sets for $n = 4$ (base case).

Set	Permutations (1-indexed)
Π_1	$\{[1,2,3,4],[3,2,4,1],[3,4,1,2],$ $[1,3,4,2],[4,2,1,3],[4,1,3,2]\}$
Π_2	$\{[1,2,3,4],[2,3,1,4],[3,4,1,2],$ $[2,4,3,1],[4,2,1,3],[1,4,2,3]\}$
Π_3	$\{[1,2,3,4],[1,3,4,2],[1,4,2,3],$ $[2,3,1,4],[3,4,1,2],[4,2,1,3]\}$

Table 5: Self-recursive extension on Π_1 for $m = 2$.

Base $\pi_k \in \Pi_1$	**Extended** $\pi_k^{R_2} = \pi_k \cdot \pi_k^R$
$[1,2,3,4]$	$[1,2,3,4,5,6,7,8]$
$[3,2,4,1]$	$[3,2,4,1,7,6,8,5]$
$[3,4,1,2]$	$[3,4,1,2,7,8,5,6]$
$[1,3,4,2]$	$[1,3,4,2,5,7,8,6]$
$[4,2,1,3]$	$[4,2,1,3,8,6,5,7]$
$[4,1,3,2]$	$[4,1,3,2,8,5,7,6]$

Table 6: Self-recursive extension on Π_1 for $m = 3$.

Base $\pi_k \in \Pi_1$	**Extended** $\pi_k^{R_3} = \pi_k^{R_2} \cdot \pi_k^R$
$[1,2,3,4]$	$[1,2,3,4,5,6,7,8,9,10,11,12]$
$[3,2,4,1]$	$[3,2,4,1,7,6,8,5,11,10,12,9]$
$[3,4,1,2]$	$[3,4,1,2,7,8,5,6,11,12,9,10]$
$[1,3,4,2]$	$[1,3,4,2,5,7,8,6,9,11,12,10]$
$[4,2,1,3]$	$[4,2,1,3,8,6,5,7,12,10,9,11]$
$[4,1,3,2]$	$[4,1,3,2,8,5,7,6,12,9,11,10]$

Table 7: Self-recursive extension on Π_1 for $m = 4$.

Base $\pi_k \in \Pi_1$	**Extended** $\pi_k^{R_4}$
$[1,2,3,4]$	$[1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16]$
$[3,2,4,1]$	$[3,2,4,1,7,6,8,5,11,10,12,9,15,14,16,13]$
$[3,4,1,2]$	$[3,4,1,2,7,8,5,6,11,12,9,10,15,16,13,14]$
$[1,3,4,2]$	$[1,3,4,2,5,7,8,6,9,11,12,10,13,15,16,14]$
$[4,2,1,3]$	$[4,2,1,3,8,6,5,7,12,10,9,11,16,14,13,15]$
$[4,1,3,2]$	$[4,1,3,2,8,5,7,6,12,9,11,10,16,13,15,14]$

A.3 Recursive mixed-extension examples

Exhaustive search reveals that one can also obtain compatible sets of size 6 by *mixed extension*: extending each permutation in one compatible set on the right with permutations from another compatible set. Suppose Π_A is a compatible set in dimension $4m_1$ and Π_B is another compatible set in dimension $4m_2$. We

start with a candidate set $\Pi_A\Pi_B^R = \{\pi\rho^R : \pi \in \Pi_A, \rho \in \Pi_B\}$, which contains in total $|\Pi_A| \cdot |\Pi_B|$ permutations in dimension $4(m_1+m_2)$. This set is then fed into a function in our implementation, which outputs all maximal compatible sets for the given input. The search is pruned recursively: once a candidate permutation is selected, all remaining permutations incompatible with it are discarded, so one does not enumerate all subsets of the input set. For the input pair $(\Pi_A, \Pi_B) = (\Pi_1, \Pi_3)$, our script finds all maximal compatible sets arising from this mixed-extension input; in dimension 8 this yields four compatible sets of size 6. We include these data only as illustrative examples of the recursive method, not as a classification of all compatible sets in higher dimensions.

Taking $(\Pi_A, \Pi_B) = (\Pi_1, \Pi_3)$ as in Table 4, one can obtain four compatible sets in dimension 8 of size 6. Table 8 gives an example for $m = 2$.

Table 8: An example of mixed extension for $m = 2$.

$\pi \in \Pi_1$	$\rho \in \Pi_3$	**Extended** $\pi\rho^R$
$[1,2,3,4]$	$[1,2,3,4]$	$[1,2,3,4,5,6,7,8]$
$[2,4,3,1]$	$[1,4,2,3]$	$[2,4,3,1,5,8,6,7]$
$[3,2,4,1]$	$[3,4,1,2]$	$[3,2,4,1,7,8,5,6]$
$[3,4,1,2]$	$[2,3,1,4]$	$[3,4,1,2,6,7,5,8]$
$[4,1,3,2]$	$[1,3,4,2]$	$[4,1,3,2,5,7,8,6]$
$[4,2,1,3]$	$[4,2,1,3]$	$[4,2,1,3,8,6,5,7]$

Take Π_A as the compatible set in Table 8 and Π_B as Π_3 again. Similarly, one obtains several compatible sets of size 6. Table 9 gives an example for $m = 3$.

Table 9: An example of mixed extension for $m = 3$.

$\pi \in \Pi_A$	$\rho \in \Pi_3$	**Extended** $\pi\rho^R$
$[1,2,3,4,5,6,7,8]$	$[1,2,3,4]$	$[1,2,3,4,5,6,7,8,9,10,11,12]$
$[2,4,3,1,5,8,6,7]$	$[1,4,2,3]$	$[2,4,3,1,5,8,6,7,9,12,10,11]$
$[3,2,4,1,7,8,5,6]$	$[3,4,1,2]$	$[3,2,4,1,7,8,5,6,11,12,9,10]$
$[3,4,1,2,6,7,5,8]$	$[2,3,1,4]$	$[3,4,1,2,6,7,5,8,10,11,9,12]$
$[4,1,3,2,5,7,8,6]$	$[1,3,4,2]$	$[4,1,3,2,5,7,8,6,9,11,12,10]$
$[4,2,1,3,8,6,5,7]$	$[4,2,1,3]$	$[4,2,1,3,8,6,5,7,12,10,9,11]$

Experimental results demonstrate that the mix-extension method can generate many compatible sets of size 6 in a dimension of $4m$ for $m \geq 2$. It is worth noting that one is not necessarily restricted to extending a compatible set by another compatible set. Instead, one may extend a set of permutations with another set of permutations. Starting from $n = 4$, among all permutations in

IS_4, one can get a candidate set of 169 permutations in dimension 8, which leads to 1936 compatible sets of size 6 in dimension 8. This type of extension can continue with larger m.

The theoretical analysis of the recursive mixed-extension approach appears complicated by using the technique in this paper. We shall further develop new methods for those cases in our future work.

A.4 Summary of recursive construction parameters

The recursive construction generates NOMA codebooks of size $K = 6N$ for all dimensions $n = 4m$, where each sequence has length $N = 2^n$ and PAPR upper bounded by 2.

Table 10: Properties of NOMA codebooks from the recursive construction.

m	Dim. n	Len. N	#Sequences K	Coherence $\mu(\mathbf{\Phi})$	Overloading Factor L
1	4	16	96	1/4	6
2	8	256	1,536	1/16	6
3	12	4,096	24,576	1/64	6
4	16	65,536	393,216	1/256	6

All codebooks achieve the optimal coherence $1/\sqrt{N}$ as shown in (5), and the construction maintains a constant overloading factor $L = 6$ for all dimensions $n = 4m$ with $m \geq 1$.