# On the codebook design for NOMA schemes from bent functions

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

[1] Department of Informatics, University of Bergen,
5020 Bergen, Norway; {chunlei.li,palash.sarkar}@uib.no

[2] Department of Computer Science, Electrical Engineering and Mathematical Sciences,
Western Norway University of Applied Sciences, 5020 Bergen, Norway; csr@hvl.no

[3] Applied Mathematics Department, Naval Postgraduate School,
Monterey, CA 93943, USA; pstanica@nps.edu

**Abstract**

In the design of codebook for non-orthogonal multiple access (NOMA) schemes in machine-type communications, a fundamental problem asks to construct a large set of special quadratic bent functions in which the difference of any two is required to be bent or near-bent. In this work we proposed a theoretical construction of such sets by applying a recursive approach on sets in smaller dimensions.

## 1 Preliminaries

Golay complementary pairs are pairs of sequences $\mathbf{a}, \mathbf{b}$ of identical length which have zero aperiodic autocorrelation sum. With the zero autocorrelation sum, the sum of peak-to-average power ratios (PAPsR) of $\mathbf{a}$ and $\mathbf{b}$ equals to 2, indicating that each GDJ-sequence has a low PAPR upper bounded by 2. This nice property makes Golay complementary pairs desirable objects in a variety of applications in communication systems. Davis and Jedwab [1] established an important connection between Golay complementary pairs of length $2^n$ and generalized Boolean functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_{2^h}$.

*Lemma* 1. Let $n$ be a positive integer, $\pi$ a permutation of $\{1, 2, \ldots, n\}$ and define an $n$-variable generalized Boolean function

$$f_\pi^c(x) := 2^{h-1} \sum_{k=1}^{n-1} x_{\pi(k)} x_{\pi(k+1)} + \sum_{k=1}^{n} c_k x_k = Q_\pi(x) + L_c(x),$$

where $c = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_2^n$, $Q_\pi$ and $L_c$ denote the quadratic terms and linear terms in $f_\pi^c$, respectively. Then the sequences $\mathbf{a} = [(-1)^{a(i)}]_{0 \le i < 2^n}, \mathbf{b} = [-1^{b(i)}]_{0 \le i < 2^n}$ from the truth tables of the functions $a(x) = f_\pi^c(x) + \epsilon$ and $b(x) = f_\pi^c(x) + x_{\pi(1)} + \epsilon'$, respectively, form a $2^h$-ary Golay complementary pair of length $2^n$ for any $c \in \mathbb{F}_2^n$, $\epsilon, \epsilon' \in \mathbb{Z}_{2^h}$.

The Golay complementary pair $(\mathbf{a}, \mathbf{b})$ in Lemma 1 has been also termed a Golay-Davis-Jedwab (GDJ) pair, and each of the sequences $\mathbf{a}, \mathbf{b}$ is a GDJ sequence. The work of Davis and Jedwab has stimulated many research works on complementary sequences sets with low PAPR and zero-correlation zone sequences in the last two decades. Recently Yu [3] proposed a framework of designing uplink grant-free non-orthogonal multiple access (NOMA) scheme based on binary GDJ sequences, which promised to have low PAPR and low coherence for multi-carrier transmission. Here we recall some basics of the framework in [3]. Given a permutation $\pi$, the set $S_\pi := \{Q_\pi(x) + L_c(x) + \epsilon \mid c \in \mathbb{F}_2^n, \epsilon \in \mathbb{F}_2\}$ is a coset of the first-order Reed-Muller code $\mathcal{R}(1, n)$, with representative $Q_\pi(x)$, within the second-order Reed-Muller code $\mathcal{R}(2, n)$. When we associate the functions in this coset with binary GDJ sequences and arrange them in a matrix column by column, we obtain a $2^n \times 2^n$ matrix whose columns are mutually orthogonal since the difference between any two functions in $S_\pi$ is a nonzero linear function. By adopting more permutations of $\{1, 2, \ldots, n\}$, Yu proposed the following framework for uplink grant-free NOMA schemes.

*Definition* 2. Consider $L$ distinct permutations $\pi_1, \cdots, \pi_L$ of $\{1, \cdots, n\}$. For each $\pi_l$, let $\mathbf{a}_{\pi_l}^{(c)}$ be the GDJ sequence of length $N = 2^n$ associated with the function $f_{\pi_l}^c(x)$ as in Lemma 1. With $L$ permutations, we construct an $N \times LN$ non-orthogonal spreading matrix as follows:

$$\mathbf{\Phi} = \frac{1}{\sqrt{M}} \left[\mathbf{\Phi}_1, \cdots, \mathbf{\Phi}_L\right], \tag{1}$$

where $\mathbf{\Phi}_l = \left[\mathbf{a}_{\pi_l}^{(0)}, \mathbf{a}_{\pi_l}^{(1)}, \cdots, \mathbf{a}_{\pi_l}^{(N-1)}\right]_{N \times N}$ is an orthogonal matrix for $1 \le l \le L$.

It is well known [2] that a quadratic form $Q(x)$ over $\mathbb{F}_2^n$ can be characterized by its corresponding symplectic matrix $\mathbf{B}$, which is an $n \times n$ binary matrix such that for $1 \le i, j \le n$, the entry $\mathbf{B}(i, j) = 1$ iff $Q(x)$ contains the term $x_i x_j$. The rank of quadratic function $Q(x)$ is identical to the rank of the corresponding symplectic matrix $\mathbf{B}$ and the weight distribution of the coset with representative $Q_\pi$ in $\mathcal{R}(2, n)$ is uniquely determined by the rank of $\mathbf{B}$. Based on this fact, the coherence of the above spreading matrix was characterized in [3, Th. 1] as follows.

*Lemma* 3. Let $\mathbf{\Phi}$ be an $N \times LN$ spreading matrix $\mathbf{\Phi}$ defined as in (1). Let $\mathbf{B}_{l_1,l_2}$ be the binary simplectic matrix of the quadratic function $Q_{l_1,l_2}(x) = Q_{\pi_{l_1}}(x) + Q_{\pi_{l_2}}(x)$, namely, for $1 \le i, j \le n$, $\mathbf{B}_{l_1,l_2}(i, j) = 1$ iff $Q_{l_1,l_2}(x)$ has the term $x_i x_j$. Then the coherence of the spreading matrix is given by

$$\mu(\mathbf{\Phi}) = \frac{1}{\sqrt{2^{r_{\min}}}}, \text{ where } r_{\min} = \min_{1 \le l_1 \ne l_2 \le L} \operatorname{rank}\left(\mathbf{B}_{l_1,l_2}\right). \tag{2}$$

From the above result, it is easy to see that the coherence $\mu(\mathbf{\Phi})$ has the following lower bounds

$$\mu(\mathbf{\Phi}) \ge \begin{cases} \frac{1}{\sqrt{2^n}} \text{ for even } n, \\ \frac{1}{\sqrt{2^{n-1}}} \text{ for odd } n. \end{cases} \tag{3}$$

In the application for uplink grant-free NOMA, the above design of the spreading matrix $\mathbf{\Phi}$ has several advantages: each column of $\mathbf{\Phi}$ as a spreading sequence has low

PAPR upper bounded by 2, the coherence of $\mathbf{\Phi}$ can achieve the lowest possible value when the symplectic matrix $\mathbf{B}_{l_1,l_2}$ for any $1 \le l_1 \ne l_2 \le L$ has full rank $n$ for even $n$ or almost full rank $n-1$ for odd $n$. In order to accommodate more devices, it is desirable to have as large $L$ as possible. Here natural but challenging problems arise.

**Main Problem 1.** Let $\mathbf{\Phi}$ be the $N \times LN$ spreading matrix defined in (1) satisfying the following two conditions: (i) each column of $\mathbf{\Phi}$ is a binary GDJ sequence with PAPR $\le 2$; (ii) $\mathbf{\Phi}$ has the lowest coherence as in (3). How can this spreading matrix be theoretically constructed for any $n$?

For $1 \le l_1 \ne l_2 \le L$, the quadratic function $Q_{l_1,l_2}(x)$ as in Lemma 3 with rank $r$ has the Walsh spectrum $\{0, \pm 2^{n-\frac{r}{2}}\}$. Let $W_Q(c)$ be the Walsh-Hadamard transform of $Q(x)$ at a point $c \in \mathbb{F}_2^n$ and

$$W(\mathbf{\Phi}) := \max_{1 \le l_1 \ne l_2 \le L} \max_{c \in \mathbb{F}_2^n} |W_{Q_{l_1,l_2}}(c)| = \frac{2^n}{\sqrt{2^{r_{\min}}}} \tag{4}$$

where $r_{\min} = \min_{1 \le l_1 \ne l_2 \le L} \operatorname{rank}(\mathbf{Q}_{l_1,l_2})$. Combining (2) and (4), we obtain the following relation $W(\mathbf{\Phi}) = 2^n \mu(\mathbf{\Phi})$. Therefore, for even $n$ the lower bound in (3) is achieved when the quadratic function $Q_{\pi_{l_1},\pi_{l_2}}(x)$ for any $1 \le l_1 \ne l_2 \le L$ is a bent function; and for odd $n$ the lower bound is achieved when $Q_{\pi_{l_1},\pi_{l_2}}(x)$ for any $1 \le l_1 \ne l_2 \le L$ is a near-bent function. With this relation, the main problem can be restated in an alternative way.

**Main Problem 1'.** How to construct a large set of permutations $\pi_1, \ldots, \pi_L$ of $\{1, \ldots, n\}$ such that the quadratic functions $Q_{l_1,l_2}(x) = Q_{\pi_{l_1}}(x) + Q_{\pi_{l_2}}(x) = \sum_{k=1}^{n-1} x_{\pi_{l_1}(k)} x_{\pi_{l_1}(k+1)} + \sum_{k=1}^{n-1} x_{\pi_{l_2}(k)} x_{\pi_{l_2}(k+1)}$ for any $1 \le l_1 < l_2 \le L$ are bent for even $n$ and near bent for odd $n$?

## 2 Theoretical Constructions

In this section we will be concerned with theoretical constructions of a set of permutations of $\{1, 2, \ldots, n\}$, for $n$ even, satisfying the conditions in the main problem. We denote by $I_n$ the identity permutation and $S_n$ the set of all permutations of $\{1, 2, \ldots, n\}$. For convenience of presentation, two permutations $\pi_1$, $\pi_2$ in $S_n$ are said to **compatible** if the corresponding quadratic function $Q_{\pi_1}(x) + Q_{\pi_2}(x)$ is bent. Furthermore, a set of permutations in $S_n$ is said to be compatible if any two permutations in the set are compatible. As customary, we write a permutation $\pi = [i_1, i_2, \ldots]$, or (when there is no danger of confusion) as the concatenation $\pi = i_1 i_2 \ldots$ to mean $\pi(1) = i_1, \pi(2) = i_2$, etc. Throughout the paper, the proofs are omitted due to page limitations.

We first provide some basic properties on compatible permutations.

*Lemma* 4. For any two permutations $\pi$, $\sigma \in S_n$, we have

1. $I_n$ and $\pi$ are compatible iff $I_n$ and the reverse $\pi^R$ of $\pi$ are compatible;
2. $I_n$ and $\pi$ are compatible iff $I_n$ and the inverse $\pi^{-1}$ of $\pi$ are compatible;
3. $\pi$ and $\sigma$ are compatible iff $I_n$ is compatible with the permutations $\pi \circ \sigma^{-1}, \sigma^{-1} \circ \pi$, $\pi^{-1} \circ \sigma$, $\sigma \circ \pi^{-1}$, where $\circ$ denotes the mapping composition.

In the case of $n = 4$, by exhaustive search all the permutations that are compatible with the identity permutations are listed below.

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

It's easily seen that $\rho_5 = \rho_2^R$, $\rho_6 = \rho_4^R$, $\rho_8 = \rho_3^R$, $\rho_{10} = \rho_9^R$, $\rho_{11} = \rho_1^R$, $\rho_{12} = \rho_7^R$, and that $\rho_7 = \rho_1^{-1} = \rho_1^2$, $\rho_5 = \rho_2^{-1}$, $\rho_3^{-1} = \rho_3$, $\rho_9 = \rho_4^{-1} = \rho_4^2$, $\rho_{11} = \rho_6^{-1} = \rho_6^2$, $\rho_8 = \rho_8^{-1}$ and $\rho_{12} = \rho_{10}^{-1} = \rho_{10}^2$. By Lemma 4 the pairs $(\rho_1, \rho_7), (\rho_4, \rho_9), (\rho_6, \rho_{11}), (\rho_{10}, \rho_{12})$ are compatible. Furthermore, checking mutual compatibility among these permutations give in total 32 compatible sets, e.g., $\Pi = \{I_4, \rho_1, \rho_4, \rho_5, \rho_8, \rho_{10}\}$. When we denote the permutations in $S_n$ as vertices and draw edges between any two vertices if the corresponding permutations when compatible, the main problem is essentially to find the maximum clique of a graph composed of $n!$ vertices, which is known to be an NP-complete problem. By an exhaustive search on $n = 4, 5, 6, 7$, the maximum sizes of compatible sets in $n$ variables are $6, 13, 9, 15$, respectively. However, exhaustive search for compatible sets becomes infeasible quickly as $n$ increases.

### 2.1 Extending compatible pairs from $S_n$ to $S_{n+4}$

This subsection summarizes different ways of extending a permutation in $S_n$ compatible with $I_n$ to a permutation in $S_{n+4}$ compatible with $I_{n+4}$. The results are derived from detailed investigations of the bentness of relevant quadratic functions.

**Theorem 5.** *Suppose $\pi \in S_n$ is compatible with $I_n$. The following permutations in $S_{n+4}$ are all compatible with $I_{n+4}$ :*

| | |
|---|---|
| $(n+4)(n+1)\pi(n+3)(n+2)$ | $(n+2)(n+3)\pi(n+1)(n+4)$ |
| $(n+2)(n+3)(n+1)\pi(n+4)$ | $(n+4)\pi(n+3)(n+2)(n+1)$ |
| $(n+3)(n+2)(n+4)\pi(n+1)$ | $(n+1)\pi(n+4)(n+2)(n+3)$ |
| $(n+3)(n+4)(n+1)\pi(n+2)$ | $(n+2)\pi(n+1)(n+4)(n+3)$ |
| $(n+1)(n+3)(n+4)(n+2)\pi$ | $\pi(n+2)(n+4)(n+3)(n+1)$ |
| $(n+2)(n+4)(n+3)(n+1)\pi$ | $\pi(n+1)(n+3)(n+4)(n+2)$ |
| $(n+3)(n+2)(n+4)(n+1)\pi$ | $\pi(n+1)(n+4)(n+2)(n+3)$ |
| $(n+2)(n+1)(n+4)(n+3)\pi$ | $\pi(n+3)(n+4)(n+1)(n+2)$ |
| $(n+3)(n+4)(n+1)(n+2)\pi$ | $\pi(n+2)(n+1)(n+4)(n+3)$ |
| $(n+2)(n+3)(n+1)(n+4)\pi$ | $\pi(n+4)(n+1)(n+3)(n+2)$ |

From Theorem 5 it might appear that one can easily extend a compatible permutation from dimension $n$ to $n+4$. On the other hand, considering the total 120 possible combinations of $\pi, (n+1), (n+2), (n+3), (n+4)$, the portion is relatively small. Moreover, when considering the mutual compatibility among them, the calculation of the Walsh transform of relevant functions becomes more challenging and the size of a compatible set drops quickly. Here we need to further investigate properties of permutations. Given a permutation $\pi \in S_n$, it will be said to satisfy the Walsh-Hadamard Condition (WHC)

if the quadratic function $f = Q_{I_n}(x) + Q_\pi(x)$ is bent and $W_{Q_\pi}(a)W_{Q_\pi}(a + e_{\pi(n-2)}) = W_{Q_\pi}(a + e_{n-2})W_{Q_\pi}(a + e_{n-2} + e_{\pi(n-2)})$ holds for all $a \in \mathbb{F}_2^n$. It can be shown that any $\rho_i \in \{\rho_1, \rho_3, \rho_7, \rho_8, \rho_{10}, \rho_{12}\}$ satisfies WHC. The WHC plays an important role in our investigation. Given $\pi \in S_n$ and $\rho \in S_4$, we denote $\pi\overline{\rho} = [\pi(1), \ldots, \pi(n), n + \rho(1), n + \rho(2), n + \rho(3), n + \rho(4)]$, i.e. the permutation $\pi$ extended by $\rho$ on the right. Then we get the following result.

**Theorem 6.** *For a permutation $\pi \in S_n$ compatible with $I_n$, if $\pi$ satisfies the WHC, then the permutation $\pi\overline{\rho}$ in $S_{n+4}$ satisfies WHC for any $\rho \in \{\rho_1, \rho_3, \rho_7, \rho_8, \rho_{10}, \rho_{12}\}$.*

### 2.2 Extending a compatible set from small dimensions

We are interested in those compatible sets with as large size as possible, and a compatible set with maximum possible size for a given dimension $n$ is termed a *maximal set*. For $n = 4$, there are 12 permutations that are compatible with $I_4$. Furthermore, there are in total 32 maximal sets of size 6, some of which are given below:

$$\begin{array}{lll}
\{I_4, \rho_1, \rho_4, \rho_5, \rho_8, \rho_{10}\}, & \{I_4, \rho_4, \rho_5, \rho_8, \rho_{10}, \rho_{11}\}, & \{I_4, \rho_4, \rho_7, \rho_8, \rho_{10}, \rho_{11}\}, \\
\{I_4, \rho_3, \rho_4, \rho_7, \rho_{10}, \rho_{11}\}, & \{I_4, \rho_6, \rho_8, \rho_9, \rho_{11}, \rho_{12}\}, & \{I_4, \rho_3, \rho_6, \rho_9, \rho_{11}, \rho_{12}\}, \\
\{I_4, \rho_1, \rho_3, \rho_6, \rho_{10}, \rho_{12}\}, & \{I_4, \rho_1, \rho_6, \rho_8, \rho_{10}, \rho_{12}\}, & \{I_4, \rho_1, \rho_6, \rho_7, \rho_8, \rho_{10}\}, \\
\{I_4, \rho_3, \rho_4, \rho_{10}, \rho_{11}, \rho_{12}\}, & \{I_4, \rho_1, \rho_3, \rho_6, \rho_7, \rho_{10}\}, & \{I_4, \rho_6, \rho_8, \rho_{10}, \rho_{11}, \rho_{12}\}.
\end{array}$$

By inspecting the patterns of the permutations listed in Theorem 5, we observe that except for $\rho_2$ and $\rho_5$, all the other 10 permutations can be recursively extended. This leads to a recursive construction of compatible sets in $S_{4n}$ for $n \geq 1$.

**Theorem 7.** *Given any maximal set $\Pi$ in dimension 4, the set $\{\pi\overline{\pi} \mid \pi \in \Pi\}$ is a compatible set in $S_{n+4}$. Recursively applying this fact gives a compatible set of size 6 in any dimension $4n$ for $n \geq 1$.*

*Remark* 8. This is not the only possible maximal set extended by our methods. However, the conditions are more restrictive, as even if $\pi$ and $\sigma$ satisfy WHC, we do not necessarily have that $\sigma\pi^{-1}$ satisfy WHC.

## References


[1] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes," IEEE Trans. Inf. Theory, vol. 45, pp. 2397–2417, Nov. 1999.

[2] MacWilliams, F.J. and Sloane, N.J.A. (1977) The Theory of Error-Correcting Codes. Elsevier-North-Holland, Amsterdam.

[3] N. Y. Yu, "Binary Golay Spreading Sequences and Reed-Muller Codes for Uplink Grant-Free NOMA," in IEEE Trans. Commun., vol. 69, no. 1, pp. 276–290, Jan. 2021.