On the codebook design for NOMA schemes from bent functions

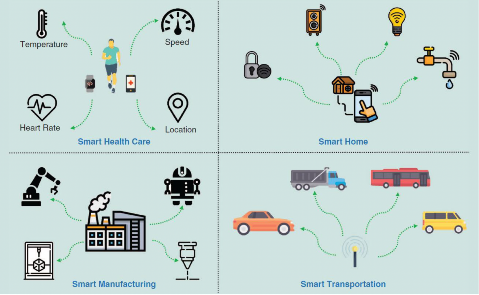
Chunlei Li, **Constanza Riera**, Pantelimon Stănică, Palash Sarkar

The 9th BFA workshop dedicated to the 75th anniversary of Claude Carlet

September, 2024

Background

- Massive Machine-Type Communication (mMTC)



L. Liu, E. G. Larsson, W. Yu, P. Popovski, C. Stefanovic, and E. de Carvalho, "Sparse signal processing for grant-free massive connectivity - A future paradigm for random access protocols in the internet of things," *IEEE Signal Process. Mag.*, pp. 88-99, Sep. 2018.

- Everything, benefiting from being connected, will be connected
  - massive IoT devices, small data, sporadic transmission, etc

- Grant-free random access
  - user-specific sequences assigned to devices
  - each active device attempts to access a base station using its assigned sequence
  - low signaling overhead $\longrightarrow$ low latency in uplink access

Problem Formulation

- Grant-free random access can be formulated by a compressed sensing problem

$$\mathbf{Y} = \mathbf{\Phi} \cdot \mathbf{X} + \mathbf{W}$$

  - $\mathbf{X}$: row-wise sparse matrix due to sparse device activity
  - $\mathbf{\Phi}$: a collection of user-specific, non-orthogonal sequences
  - $\mathbf{W}$: additive white noise

- The coherence of matrix $\mathbf{\Phi} \in \mathbb{C}^{N \times M}$ given by

$$\mu(\mathbf{\Phi}) := \max_{1 \le i < j \le N} \frac{|\langle \mathbf{\Phi}_i, \mathbf{\Phi}_j \rangle|}{\| \mathbf{\Phi}_i \| \cdot \| \mathbf{\Phi}_j \|}$$

  where $\langle \cdot \rangle$ denotes the inner product

- low coherence $\longrightarrow$ more reliable data recovery at base station

An interesting construction of $\boldsymbol{\Phi}$

- Golay spreading sequences
  - a binary Golay sequence $\mathbf{a} = [a_0, a_1, \ldots, a_{N-1}]$ has

$$\mathrm{PAPR}(\mathbf{a}) := \max_{t \in [0,1)} \frac{|\sum_{j=0}^{N-1} (-1)^{a_j} e^{2\pi i \cdot jt}|^2}{N} \leq 2$$

  - low PAPR is desired for low power consumption
  - a binary sequence of length 2^n can be seen as the truth table of the following Boolean function

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n-1} x_{\pi(i)} x_{\pi(i+1)} + \sum_{i=1}^{n} c_i x_i$$

where π is a permutation of $\{1, 2, \ldots, n\}$ and $c_i \in \mathbb{F}_2$

An interesting construction of $\mathbf{\Phi}$ (II)

Assume $\mathbf{\Phi} \in \mathbb{C}^{N \times M}$ with $N = 2^n$ has its columns given by some $(-1)^{f(x)}$ with [1]

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n-1} x_{\pi(i)} x_{\pi(i+1)} + \sum_{i=1}^{n} c_i x_i,$$

where $(c_1, \ldots, c_n) \in \mathbb{F}_2^n$, and different permutations π will be chosen when $M > N$.

- each column of $\mathbf{\Phi}$ will be used as a device sequence
- each sequence has PAPR ≤ 2
- larger M indicates more devices can be accommodated
- loading factor $L = M/N$ is desirable to be large

[1] N. Yu, Binary Golay Spreading Sequences and Reed-Muller Codes for Uplink Grant-Free NOMA. IEEE Trans. Commun. 69(1): 276-290 (2021)

- $\| \mathbf{\Phi}_i \|^2 = 2^n$ for $0 \le i \le M-1$
- for $0 \le i < j < M$,

$$\langle \mathbf{\Phi}_i, \mathbf{\Phi}_j \rangle = \sum_{x \in \mathbb{F}_2^n} (-1)^{f_i(x)+f_j(x)}$$

  - equals 0 if f_i, f_j have the same π
  - otherwise, reduces to

$$W_Q(\lambda) = \sum_{x \in \mathbb{F}_2^n} (-1)^{Q(x)+\lambda \cdot x}$$

where

$$Q = \sum_{i=1}^{n-1} x_{\pi(i)} x_{\pi(i+1)} + \sum_{i=1}^{n-1} x_{\pi'(i)} x_{\pi'(i+1)}$$

and $\lambda = c + c'$

Coherence of $\mathbf{\Phi}$

The coherence of previously defined $\mathbf{\Phi}$ satisfies

$$|\mu(\mathbf{\Phi})| = \max_{1\le i<j\le N} \frac{|\langle \mathbf{\Phi}_i, \mathbf{\Phi}_j \rangle|}{2^n} \ge \begin{cases} 2^{\frac{n}{2}}, & \text{for even } n, \\ 2^{\frac{n+1}{2}}, & \text{for odd } n. \end{cases}$$

where the equalities are achieved when

- Q is bent for even n;
- Q is semibent for odd n

Design Goal

We need the matrix $\mathbf{\Phi}$ with

- low PAPR, low coherence, and large loading factor $L = M/N$

Essential Problem

Construct **a large set** of permutations $\pi_1, \ldots, \pi_L$ of $\{1, \ldots, n\}$ such that for any $1 \le l_1 < l_2 \le L$, the quadratic function

$$\begin{aligned} Q_{l_1,l_2}(x) &= Q_{\pi_{l_1}}(x) + Q_{\pi_{l_2}}(x) \\ &= \sum_{k=1}^{n-1} x_{\pi_{l_1}(k)} x_{\pi_{l_1}(k+1)} + \sum_{k=1}^{n-1} x_{\pi_{l_2}(k)} x_{\pi_{l_2}(k+1)}, \end{aligned}$$

are bent for even n and semibent for odd n (we call then π_1 and π_2 compatible).

Note that $Q_\pi(x)$ for any π is bent or semibent

Notation

- A subset of the permutation group 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 and I_n the identity permutation

Goal: obtain as large as possible a compatible subset of S_n

Basic results on *compatible* permutations

Lemma

For any two permutations $\pi, \sigma \in S_n$, we have

1. *I_n and π are compatible iff I_n and the reverse π^R of π are compatible;*
2. *I_n and π are compatible iff I_n and the inverse π^{-1} of π are compatible;*
3. *π and σ 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.*

Small example $n = 4$

Computationally, we found that all the permutations compatible with I_4 are:

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

It is easily seen that

- $\rho_5 = \rho_2^R$, $\rho_6 = \rho_4^R$, $\rho_8 = \rho_3^R$, $\rho_{10} = \rho_9^R$, $\rho_{11} = \rho_1^R$, $\rho_{12} = \rho_7^R$,
- $\rho_7 = \rho_1^{-1} = \rho_1^2$, $\rho_5 = \rho_2^{-1}$, $\rho_3^{-1} = \rho_3$, $\rho_9 = \rho_4^{-1} = \rho_4^2$, $\rho_{11} = \rho_6^{-1} = \rho_6^2$, $\rho_8 = \rho_8^{-1}$ and $\rho_{12} = \rho_{10}^{-1} = \rho_{10}^2$.

Checking mutual compatibility among these permutations give in total 32 compatible sets of maximal size, e.g.,

$$\Pi = \{I_4, \rho_1, \rho_4, \rho_5, \rho_8, \rho_{10}\}$$

- When we take the permutations in S_n as vertices and draw edges between any two vertices if the corresponding permutations are 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 $6, 13, 9, 13$, respectively.
- Exhaustive search for compatible sets becomes infeasible quickly as n increases.
- In this work we extend compatible sets by recursion.

Theorem

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

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

- It might appear that one can easily extend a compatible permutation from dimension n to $n+4$.
- But 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 the properties of these 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 $a \in \mathbb{F}_2^n$.
- 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 π extended by ρ on the right. Then we get the following result.

Theorem

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

Extending pairs by repetition

Lemma

$\rho \in \{\rho_1, \rho_3, \rho_7, \rho_8, \rho_{10}, \rho_{12}\}$ *all satisfy the WHC condition.*

Corollary

$\rho\overline{\rho}$ *is compatible with the identity for any* $\rho \in \{\rho_1, \rho_3, \rho_4, \rho_6, \rho_7, \rho_8, \rho_9, \rho_{10}, \rho_{11}, \rho_{12}\}$. *Recursively applying this fact gives permutations compatible with the identity in any dimension* $4m$ *for* $m \geq 1$.

Extending sets

- We are interested in those compatible sets with as large size as possible (maximal set).
- Recall that, 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:

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

Extending by repetition

Theorem

Given any maximal set Π in dimension 4, the set $\{\pi\overline{\pi} \mid \pi \in \Pi\}$ is a compatible set in S_8. Recursively applying this fact gives a compatible set of size 6 in any dimension $4m$ for $m \geq 1$.

- This is not the only possible way to extend a maximal set, by our methods.
- However, the conditions are more restrictive, since even if π and σ satisfy WHC, we do not necessarily have that $\sigma\pi^{-1}$ satisfies WHC.

Conclusion and future work

- Our method extends compatible pairs in any dimension n (odd or even), to a dimension $n+4m$, $m \geq 1$.
- By repetition, we can also find compatible sets of size 6 (current record size) in any dimension $4m$ for $m \geq 1$.
- We want to create algorithms that can extend any sets of size $\ell > 2$ in dimension 4 by other than repetition.
- For $n > 4$, 6 is not the maximal size (by inspection on small dimensions): it is our objective to extend the size of the sets in dimensions $4m$, $m > 1$.
- We also want to also investigate the properties of the permutations compatible with the identity for small dimensions $n \neq 4$ and find similar extension results.