Chirp Reconstruction Algorithm for Generalized Second-Order Reed-Muller Frames

Renaud-Alexandre Pitaval and Yi Qin
Huawei Technologies Sweden AB, Stockholm, Sweden
Emails: {renaud.alexandre.pitaval, qinyi4}@huawei.com

***Abstract*—We consider low-complexity decoding of generalized second-order Reed-Muller frames. Second-order Reed-Muller frames are highly non-coherent, highly-structured, sets of 2^m-dimensional complex vectors with fourth root-of-unity alphabet, that comes by design with a low-complexity chirp reconstruction algorithm (ChirpRA). In this paper, we extend ChirpRA to expanded frames in 2^m-dimension with same alphabet, and we also generalized it to Reed-Muller frames in other dimensions constructed from different alphabets.**

***Index Terms*—Reed-Muller frame, chirp reconstruction algorithm, massive random access.**

I. Introduction

This work is primarily motivated by two applications: non-coherent communication with a multi-dimensional constellation currently considered in 5G standardization for sending uplink control information [1]; and unsourced random access [2] of multiple user signatures which is an emerging paradigm for 6G massive machine-type communications. In both applications, we consider that each user sends a complex vector from a predefined set whose maximum pairwise correlation is low. The set is commonly referred as a frame, codebook, or multi-dimensional constellation; and its elements as codewords, sequences, or Grassmannian lines, ect.

Of particular interest for these practical applications are the second-order Reed-Muller frames [3], [4] which maps finite-field Reed-Muller codes to the complex field with a fourth-root of unity alphabet. Besides their versatility, nested structure, and low maximum coherence, the 2nd-order Reed-Muller frames enable a specific low-complexity detection.

In 2^m-dimension, maximum likelihood (ML) detection of a 2nd-order Reed-Muller frame does not require any complex multiplications as only a QPSK alphabet is used. Meanwhile, for applications using very large frames in very large dimensions, a low-complexity chirp reconstruction algorithm (ChirpRA) specific to such frames was introduced in [5]. ChirpRA is notably the main building block of the CHIRRUP algorithm [6] devised for unsourced massive random access. This algorithm renders the detection complexity independent of the frame size (up to $2^{m(m+3)/2}$ vectors), reducing the number of additions needed at the cost of introducing a number of multiplications which is typically much less than with ML.

In [7], we considered expansion of the 2^m-dimensional Reed-Muller frames as well generalization to other dimensions based on other root-of-unity alphabets for the purpose of accommodating more practical resource allocations. However, the benefit of a multiplication-free detection does not extend to the generalized Reed-Muller frames using other alphabets, and in addition no low-detection algorithm was provided. So from this point-of-view, the frames of [7] could be of limited practical value. Therefore, the objective of this paper is to provide a generalization of ChirpRA enabling a low-complexity detection for the generalized frames of [7] as well.

The original ChirpRA is based on the frame-specific property that the conjugate of a vector element-wise multiplied by a permuted version of itself is always a column of a Hadamard matrix, and as a result the decoding can be performed using the Walsh-Hadamard transform (WHT). Unfortunately, this property does not hold anymore to new vectors in the enlarged construction of [7]. To circumvent this, we identify and decompose the enlarged construction as multiple covered versions of the original Reed-Muller frame, and decode it using ChirpRA under different cover hypotheses.

For the generalized constructions using different alphabets, we are here able to show that a similar permute-and-multiply property holds for frames defined from block diagonal chirp matrices. In this case, one gets a column of a generalized Hadamard matrix and decoding can be performed by a generalized Hadamard transform which can be implemented as a cascade of WHTs and discrete Fourier transforms (DFTs). Then, larger frames using more general chirp matrices are decoded, in a similar fashion as in the 2^m-dimensional enlarged construction, by treating the off-diagonal elements as different cover hypothesis over the block-diagonal constructions.

Finally, simulations relevant to unsourced random access are provided. In a single-user and small-dimensional setting, the devised algorithms are shown to perform close to ML detection while decreasing the complexity by two orders of magnitude. In a multi-user and high-dimensional setting, by integrating the devised algorithms in an orthogonal matching pursuit routine, we verify feasibility of a reliable decoding of superposed generalized Reed-Muller sequences.

Notations: $\mathbb{Z}_n = \{0, \dots, n-1\}$ is the ring of n integers. A $N \times M$ matrix is represented with a uppercase boldface symbol and as a collection of ordered elements written as $\mathbf{M} = \{m_{i,j}\}_{i \in \mathbb{Z}_N, j \in \mathbb{Z}_M}$. Similarly, a column vectors is represented by lowercase boldface symbol and as a collection of ordered elements written as $\mathbf{c} = \{c_i\}_{i \in \mathbb{Z}_N}$. The (i,j)th entry of a matrix $\mathbf{M}$ or the ith entry of a vector $\mathbf{c}$ are written as $[\mathbf{M}]_{i,j}$ and $[\mathbf{c}]_i$, respectively. The superscripts $(\cdot)^*$, $(\cdot)^{\mathrm{T}}$, and $(\cdot)^{\mathrm{H}}$ denote complex conjugate, transpose, and conjugate transpose, respectively. The imaginary number is denoted by $\mathrm{i} = \sqrt{-1}$, $\delta_{i,j}$ is the Kronecker delta function, $\odot$ is the Hadamard product, and $\otimes$ is the Kronecker product.

II. 2nd-Order Reed-Muller Frames

We now discuss the 2nd-order Reed-Muller frames for dimension $D = 2^m$ [3], [4] with its low-complexity detection by the chirp reconstruction algorithm (ChirpRA) [5].

A. 2nd-Order Reed-Muller Grassmannian Frames

With $D = 2^m$, the frame is a set of column vectors

$$\mathcal{C} = \{\mathbf{f}_{\mathbf{S},\mathbf{k}}\}_{\mathbf{k}\in\mathbb{F}_2^m,\mathbf{S}\in\mathcal{S}} \tag{1}$$

indexed by an $m \times m$ binary symmetric matrix $\mathbf{S}$ belonging to a predefined set $\mathcal{S}$ and binary vector $\mathbf{k} \in \mathbb{F}_2^m$; and wherein the entries of each symbol are also indexed by a binary vector $\mathbf{l} \in \mathbb{F}_2^m$ such that $\mathbf{l}$th-entry is defined by

$$[\mathbf{f}_{\mathbf{S},\mathbf{k}}]_{\mathbf{l}} = \mathrm{i}^{\mathbf{l}^{\mathrm{T}}\mathbf{S}\mathbf{l}+2\mathbf{k}^{\mathrm{T}}\mathbf{l}}. \tag{2}$$

Given $\mathbf{S}$ and $\mathbf{k}$, the vector $\{\mathbf{l}^{\mathrm{T}}\mathbf{S}\mathbf{l} + 2\mathbf{k}^{\mathrm{T}}\mathbf{l}\}_{\mathbf{l}\in\mathbb{F}_2^m}$ (modulo 4) is a 2nd-order multivariate polynomial and thus a codeword in the quaternary 2nd-order Reed-Muller code.

Writing $[\mathbf{f}_{\mathbf{S},\mathbf{k}}]_{\mathbf{l}} = \mathrm{i}^{\mathbf{l}^{\mathrm{T}}\mathbf{S}\mathbf{l}} \times (-1)^{\mathbf{k}^{\mathrm{T}}\mathbf{l}}$, this is the element-wise product of the $\mathbf{k}$th column of the Hadamard matrix,

$$\mathbf{H}_D = \{(-1)^{\mathbf{k}^{\mathrm{T}}\mathbf{l}}\}_{\mathbf{k},\mathbf{l}\in\mathbb{F}_2^m}, \tag{3}$$

with a sequence which is the exponentiation of the imaginary number by a quadratic form defined by $\mathbf{S}$, and thus, as pointed out in [5], has an analogy with chirp modulation.

We denote the set of all binary $m \times m$ symmetric matrices by S_m which is of size $2^{m(m+1)/2}$. Thus, by selecting $\mathcal{S} = \mathrm{S}_m$ one gets a frame of size $N_{\mathrm{c}} = 2^{m(m+3)/2}$ whose maximum coherence is $2^{-1/2}$ [3].

B. Chirp Reconstruction Algorithm (ChirpRA)

ChirpRA is summarized in Algorithm 1. The algorithm is based on the frame-specific property that the conjugate of a symbol vector element-wise multiplied by a permuted version of itself is a column of the Hadamard matrix [5] as

$$[\mathbf{f}^*_{\mathbf{S},\mathbf{k}}]_{\mathbf{l}}[\mathbf{f}_{\mathbf{S},\mathbf{k}}]_{\mathbf{l}+\mathbf{e}} = K(-1)^{(\mathbf{S}\mathbf{e})^{\mathrm{T}}\mathbf{l}} \tag{4}$$

for some constant K. We will write the permutation of a vector $\mathbf{x}$ according to the index shift $\mathbf{l}+\mathbf{e}$ by $\mathbf{x}^{(\mathbf{e})}$. Accordingly, the vector $\mathbf{f}^*_{\mathbf{S},\mathbf{k}} \odot \mathbf{f}^{(\mathbf{e})}_{\mathbf{S},\mathbf{k}}$ is colinear to the $(\mathbf{S}\mathbf{e})$-th column of $\mathbf{H}_D$ while being orthogonal to the others.

Based on this property, ChirpRA takes a received vector $\mathbf{y}$, computes $\mathbf{y}^* \odot \mathbf{y}^{(\mathbf{e})}$ and quantizes it with the closest column of $\mathbf{H}_D$ whose index provides an estimate of $\mathbf{S}\mathbf{e}$. By taking a canonical shift $[\mathbf{e}_i]_j = \delta_{i,j}$, this directly returns $\mathbf{S}\mathbf{e}_i = \mathbf{s}_i$ the ith column of $\mathbf{S} = \{\mathbf{s}_1, \cdots, \mathbf{s}_m\}$, so that the matrix $\mathbf{S}$ can be discovered column by column. The linear coefficient $\mathbf{k}$ is then detected by *dechirping*, i.e., by removing by conjugation the estimated 2nd-order term component $\hat{\mathbf{S}}$, and then correlating again with the columns of $\mathbf{H}_D$.

An important aspect is that the inner product with the columns of the Hadamard matrix can be performed efficiently with the Walsh-Hadamard transform (WHT) which requires only $D \log_2 D$ additions, so ChirpRA uses a total of $\mathcal{O}(D \log_2^2 D)$ additions. Meanwhile, ChirpRA will take $D/2(3\log_2 D + 1)$ complex multiplications, i.e., scaling at $\mathcal{O}(D \log_2 D)$ which is typically much less than ML.

Algorithm 1 Chirp Reconstruction Algorithm (ChirpRA) [5]

```
Inputs: Received signal $\mathbf{y}$
  for $i = 1$ to $m$ do
    $\mathbf{y}^{(\mathbf{e}_i)} = \{[\mathbf{y}]_{\mathbf{l}+\mathbf{e}_i}\}_{\mathbf{l}\in\mathbb{Z}_2^m}$
    $\mathbf{z} = \mathbf{y}^* \odot \mathbf{y}^{(\mathbf{e}_i)}$
    $\hat{\mathbf{s}}_i = \arg\max_{\mathbf{l}\in\mathbb{Z}_2^m} |\, [\mathbf{H}_D\mathbf{z}]_{\mathbf{l}} \,|$
  end for
  $\hat{\mathbf{S}} = \{\hat{\mathbf{s}}_1, \cdots, \hat{\mathbf{s}}_m\}$
  $\mathbf{c} = \{\mathrm{i}^{-\mathbf{l}^{\mathrm{T}}\hat{\mathbf{S}}\mathbf{l}}\}_{\mathbf{l}\in\mathbb{Z}_2^m}$
  $\mathbf{x} = \mathbf{c} \odot \mathbf{y}$
  $\hat{\mathbf{k}} = \arg\max_{\mathbf{l}\in\mathbb{Z}_2^m} |[\mathbf{H}_D\mathbf{x}]_{\mathbf{l}}|$
Output: $\hat{\mathbf{S}}$ and $\hat{\mathbf{k}}$
```

III. Extension of ChirpRA to Generalized Frames

The original chirp reconstruction algorithm described in the previous section is designed for frames in dimension $D = 2^m$ of maximum size $2^{m(m+3)/2}$. In this section, we show how one can extend ChirpRA to the expanded or generalized Reed-Muller frames introduced in [7].

A. ChirpRA for Expanded Frames in $D = 2^m$

1) Expanded Frame Construction S^+_m: In [7], we observed that the Reed-Muller frame is based on an exponentiation by almost all possible second-order polynomials defined over the ring of integers modulo 4 with binary multidimensional variable $\mathbf{l}$; and accordingly, we proposed to enlarge the frame by considering the complete set of second-order polynomials by taking also symmetric matrices with 1/2 and 3/2 in their off-diagonal entries. This extended set of symmetric matrix S^+_m has size 2^{m^2} and thus leads to a frame of size $2^{m(m+1)}$.

2) Discussion: ChirpRA detects each column of $\mathbf{S}$ as any possible binary vector, so one may think it may potentially decode up to 2^{m^2} binary, not necessarily symmetric, $m \times m$ matrices $\mathbf{S}$, and thus directly decode larger frames using non-symmetric $\mathbf{S}$. In the meantime, some new vectors in the enlarged construction of [7] may be defined using a non-symmetric binary matrix, for example using $\mathbf{S} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ leads to the same polynomial phase than with $\mathbf{S} = \begin{bmatrix} 1 & 1/2 \\ 1/2 & 0 \end{bmatrix}$ from S^+_m. However, using non-symmetric matrices to define additional vectors would lead to ambiguities: here in our example $\mathbf{S} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ leads also to the same polynomial.

Another difficulty for generalizing ChirpRA to the enlarged construction of [7] is that by using matrices in S^+_m which are not necessarily binary and symmetric, the vector $\{\mathrm{i}^{(\mathbf{l}+\mathbf{e}_i)^{\mathrm{T}}\mathbf{S}(\mathbf{l}+\mathbf{e}_i)+2\mathbf{k}^{\mathrm{T}}(\mathbf{l}+\mathbf{e}_i)}\}_{\mathbf{l}\in\mathbb{F}_2^m}$ is not necessarily a permutation of $\mathbf{f}_{\mathbf{S},\mathbf{k}}$ as in general $(\mathbf{l}+\mathbf{e}_i)$ is computed in modulo-4 arithmetic. So we are not anymore able to benefit of a similar property as (4) from which ChirpRA is built on.

3) Cover Decomposition: To circumvent these issues, we remark that a frame constructed from S^+_m is actually made of multiple covered copies of the original frame constructed from S_m. Namely, any $\mathbf{S} \in \mathrm{S}_m^+$ can be written as

$$\mathbf{S} = \bar{\mathbf{S}} + \frac{1}{2}\widetilde{\mathbf{S}} \tag{5}$$

where $\bar{\mathbf{S}} \in \mathrm{S}_m$ and $\widetilde{\mathbf{S}}$ is a binary symmetric matrices with zeros on the main diagonal. We denote the set of cover matrices $\widetilde{\mathbf{S}}$ in the construction of $\mathcal{S}$ by $\widetilde{\mathcal{S}}$ (including the trivial cover $\widetilde{\mathbf{S}}_0 = \mathbf{0}$), whose size is at most $|\widetilde{\mathcal{S}}| \leq 2^{\frac{m(m-1)}{2}}$.Therefore the resulting frame can be written as

$$\begin{aligned} \mathcal{C} &= \{\mathbf{f}_{\mathbf{S},\mathbf{k}}\}_{\mathbf{k}\in\mathbb{F}_2^m, \mathbf{S}\in\mathrm{S}_m^+} & (6)\\ &= \bigcup_{a=0}^{|\widetilde{\mathcal{S}}|-1} \{\mathbf{c}_a \odot \mathbf{f}_{\bar{\mathbf{S}},\mathbf{k}}\}_{\mathbf{k}\in\mathbb{F}_2^m, \bar{\mathbf{S}}\in\mathrm{S}_m} & (7)\end{aligned}$$

where

$$[\mathbf{c}_a]_{\mathbf{l}} = \mathrm{i}^{\frac{1}{2}\mathbf{l}^T \widetilde{\mathbf{S}}_a \mathbf{l}} \tag{8}$$

is the covering sequence.

Based on this structure, we compute for each cover hypothesis $\mathbf{c}_a$ a corresponding uncovered received signal

$$\tilde{\mathbf{y}}_a = \mathbf{c}_a^* \odot \mathbf{y} \tag{9}$$

from which we can apply ChirpRA to return an estimated uncovered chirp matrix $\hat{\bar{\mathbf{S}}}_a = \{\hat{\bar{\mathbf{s}}}_{a,1}, \cdots, \hat{\bar{\mathbf{s}}}_{a,m}\} \in \mathrm{S}_m$.

In order to select the cover, we use as a likelihood measure for each $\hat{\bar{\mathbf{S}}}_a$ the sum of the coherences outputted by the WHTs for selecting its columns. Namely, for cover index a, columns of $\hat{\bar{\mathbf{S}}}_a$ are sequentially detected as in Algorithm 1, i.e., by first computing $\mathbf{z} = \tilde{\mathbf{y}}_a^* \odot \tilde{\mathbf{y}}_a^{(\mathbf{e}_i)}$ with permuted uncovered received vector $\tilde{\mathbf{y}}_a^{(\mathbf{e}_i)} = \{[\tilde{\mathbf{y}}_a]_{\mathbf{l}+\mathbf{e}_i}\}_{\mathbf{l}\in\mathbb{Z}_2^m}$, to finally get by WHT $\hat{\bar{\mathbf{s}}}_{a,i} = \arg\max_{\mathbf{l}\in\mathbb{Z}_2^m} |\,[\mathbf{H}_D\mathbf{z}]_{\mathbf{l}}\,|$. This leads to the estimated chirp matrix $\hat{\mathbf{S}}_a = \hat{\bar{\mathbf{S}}}_a + \frac{1}{2}\hat{\widetilde{\mathbf{S}}}_a$ to which we attach the soft value

$$\mu_a = \sum_{i=1}^{m} |\,[\mathbf{H}_D\mathbf{z}]_{\hat{\bar{\mathbf{s}}}_{a,i}}\,|. \tag{10}$$

The final chirp matrix $\hat{\mathbf{S}}_{\hat{a}}$ is selected as $\hat{a} = \arg\max_a \mu_a$.

Overall, the same steps are applied as in ChirpRA for each of the $|\widetilde{\mathcal{S}}| = N_\mathrm{c}|\mathrm{S}_m|^{-1}$ covers which mainly account to scale the number of operations by $|\widetilde{\mathcal{S}}|$. Note the trivial case $\tilde{\mathbf{y}}_0 = \mathbf{y}$, and also that uncovering the received signal in general does not cost any additional complex multiplications as the entries of $\mathbf{c}_a$ are QPSK symbols. Therefore, the number of additions will scale as $O(|\widetilde{\mathcal{S}}|D\log_2^2 D)$, and number of complex multiplications becomes $D/2(3|\widetilde{\mathcal{S}}|\log_2 D+1)$ which scales as $O(|\widetilde{\mathcal{S}}|D\log_2 D)$.

B. ChirpRA for Generalized Reed-Muller Frames

Now we look at the generalization to any dimension in [7].

1) Generalized Frame Constructions: The generalized construction is based on the prime factorization of the dimension

$$D = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n} \tag{11}$$

where $p_1 < \cdots < p_n$ are the n unique prime factors, each of order $m_1, \ldots, m_n$. There is a total of $m = \sum_{k=1}^n m_k$ primes, and the product of the unique prime factors is $q = \prod_{k=1}^n p_k$. We define $\lambda = 2$ for D even and $\lambda = 1$ otherwise, and we denote the q-root of unity by $w_q = e^{\frac{2\pi \mathrm{i}}{q}}$.

For indexing entries of a D-dimensional vector, we use a one-to-one mapping from the ring of integers $\mathbb{Z}_D$ to the Cartesian product of the Galois fields that follows from (11)

$$\mathbb{Z}_D \mapsto \mathbb{F}_{p_1}^{m_1} \times \mathbb{F}_{p_2}^{m_2} \times \cdots \times \mathbb{F}_{p_n}^{m_n}. \tag{12}$$

Consistently, elements in $\mathbb{Z}_D$ are represented by m-dimensional vectors. For example, any $x \in \mathbb{Z}_{12}$ can be written as $[b_2, b_1, t] \in \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_3$ where $x = t \times 2^0 \cdot 2^0 \cdot 3^0 + b_1 \times 2^0 \cdot 2^0 \cdot 3^1 + b_2 \times 2^0 \cdot 2^1 \cdot 3^1$, such that e.g. $8 \to [1, 0, 2]^\mathrm{T}$.

Using this, vectors are constructed as

$$[\mathbf{f}_{\mathbf{S},\mathbf{k}}]_{\mathbf{l}} = w_q^{\mathbf{l}^\mathrm{T}\mathbf{S}\mathbf{l} + \mathbf{k}^\mathrm{T}\mathbf{D}\mathbf{l}} \tag{13}$$

where $\mathbf{l}, \mathbf{k} \in \mathbb{Z}_D$, $\mathbf{S}$ is a $m \times m$ symmetric matrix from a predefined set $\mathcal{S}$, and

$$\mathbf{D} = \mathrm{blkdiag}\left(\frac{q}{p_1}\mathbf{I}_{m_1}, \frac{q}{p_2}\mathbf{I}_{m_2}, \ldots, \frac{q}{p_n}\mathbf{I}_{m_n}\right) \tag{14}$$

is a diagonal matrix where $\mathbf{I}_n$ is an $n \times n$ identity matrix and $\mathrm{blkdiag}(\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_n)$ defines a block diagonal matrix with matrices $(\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_n)$ along its diagonal.

Each frame vector is then the element-wise product of a "chirp sequence" $\{w_q^{\mathbf{l}^\mathrm{T}\mathbf{S}\mathbf{l}}\}_{\mathbf{l}\in\mathbb{Z}_D}$, and a column of a generalized Hadamard matrix

$$\mathbf{H}_D = \{w_q^{\mathbf{k}^\mathrm{T}\mathbf{D}\mathbf{l}}\}_{\mathbf{l},\mathbf{k}\in\mathbb{Z}_D}. \tag{15}$$

In [7], frames are constructed by restricting the symmetric matrices $\mathbf{S}$ to be of the form

$$\mathbf{S} = \bar{\mathbf{S}} + \widetilde{\mathbf{S}} \tag{16}$$

where $\bar{\mathbf{S}}$ is block-diagonal as

$$\bar{\mathbf{S}} = \mathrm{blkdiag}\left(\frac{q}{\lambda p_1}\mathbf{P}_1, \frac{q}{p_2}\mathbf{P}_2, \ldots, \frac{q}{p_n}\mathbf{P}_n\right) \tag{17}$$

with $\mathbf{P}_k$ being a symmetric matrix of size $m_k \times m_k$ with entries in $\mathbb{Z}_{p_k}$; and $\widetilde{\mathbf{S}}$ is a symmetric matrix with entries in $\mathbb{Z}_q$ being zero on the diagonal blocks of $\bar{\mathbf{S}}$. We denote the set of all $\bar{\mathbf{S}}$ and $\widetilde{\mathbf{S}}$ used in the frame construction by $\bar{\mathcal{S}}$ and $\widetilde{\mathcal{S}}$, receptively. Hence, the total number of symmetric matrices used is $|\mathcal{S}| = |\bar{\mathcal{S}}||\widetilde{\mathcal{S}}|$. If selecting $\widetilde{\mathcal{S}} = \{\mathbf{0}\}$, the maximum frame size is $N_\mathrm{c} = \prod_i p_i^{m_i(m_i+3)/2}$ with maximum coherence $p_1^{-1/2}$.

The frame can be expanded with a set of cover matrices, sometimes without even increasing its coherence by selecting carefully the entries of $\widetilde{\mathbf{S}}$ [7]. For example, one can observe this by starting from the largest frame obtained from block-diagonal chirps as described above and extending it with cover matrices that have their (i, j) off-diagonal-block entries restricted to $\frac{q}{p'_i}\mathbb{Z}_{p'_i}$ or $\frac{q}{p'_j}\mathbb{Z}_{p'_j}$ (divided by two if p'_j or $p'_i = 2$) where $p'_1 \leq \cdots \leq p'_m$ are the sorted non-unique prime factors of $D = \prod_{i=1}^m p'_i$. Another example arises starting from a smaller frame where $p = 2$ and $\mathbf{P}_1$ is restricted to a Delsarte-Goethals set, the frame size can be expanded without increasing the coherence by selecting cover matrices as in the previous example except that the (i,j) entries should also not be in $\frac{q}{4}\mathbb{Z}_2$. In both examples, it is preferable to take elements in the largest possible ring to maximize the frame size, i.e., the (i,j) entries of the cover are taken in $\frac{q}{\max(p'_i,p'_j)}\mathbb{Z}_{\max(p'_i,p'_j)}$.

2) Generalized Chirp Reconstruction Algorithm: In the original ChirpRA, the index shift performed in $\mathbf{f}^{(\mathbf{e}_i)}_{\mathbf{S},\mathbf{k}}$ is equivalent to a permutation of the entries. However, with the generalization (13), this is only true if $\widetilde{\mathbf{S}} = \mathbf{0}$. So in order to reuse this shifting property, as previously done we will first try to remove the off-diagonal component $\widetilde{\mathbf{S}}$ by element-wise multiplication of the received data $\mathbf{y}$ with $\left\{w_q^{-\mathbf{l}^T\widetilde{\mathbf{S}}\mathbf{l}}\right\}_{\mathbf{l}\in\mathbb{Z}_D}$ for all known $\widetilde{\mathbf{S}}$ hypotheses.

Additionally, ChirpRA is originally made to detect columns of $\mathbf{S}$ by identifying them with label indexes in $\mathbb{F}_2^m$, while here columns of $\mathbf{S}$ are not necessarily in $\mathbb{Z}_D \cong \prod_i \mathbb{F}_{p_i}^{m_i}$. To obtain something similar, we write

$$\bar{\mathbf{S}} = \mathbf{D}_\lambda \mathbf{P} \tag{18}$$

where $\mathbf{D}_\lambda = \text{blkdiag}\left(\frac{q}{\lambda p_1}\mathbf{I}_{m_1}, \frac{q}{p_2}\mathbf{I}_{m_2}, \ldots, \frac{q}{p_n}\mathbf{I}_{m_n}\right)$ and $\mathbf{P} = \text{blkdiag}\left(\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_n\right)$. In this form, the column of $\mathbf{P} = \{\mathbf{p}_1, \ldots \mathbf{p}_m\}$ are always in $\mathbb{Z}_D \cong \prod_i \mathbb{F}_{p_i}^{m_i}$ and we will be able to detect them accordingly. Now, we can verify a similar property as we had for the original ChirpRA:

$$\begin{aligned} [\mathbf{f}^*_{\bar{\mathbf{S}},\mathbf{k}}]_{\mathbf{l}}[\mathbf{f}_{\bar{\mathbf{S}},\mathbf{k}}]_{\mathbf{l}+\mathbf{e}_i} &= K w_q^{2(\bar{\mathbf{S}}\mathbf{e}_i)^{\mathrm{T}}\mathbf{l}} && (19)\\ &= K w_q^{2(\mathbf{D}_\lambda\mathbf{P}\mathbf{e}_i)^{\mathrm{T}}\mathbf{l}} && (20)\\ &= K w_q^{2\mathbf{p}_i^{\mathrm{T}}\mathbf{D}_\lambda\mathbf{l}} && (21)\end{aligned}$$

for some constant K. From (21), we see one can detect the ith column of $\mathbf{P}$ by correlating $\mathbf{z} = \tilde{\mathbf{y}}^* \odot \tilde{\mathbf{y}}^{(\mathbf{e}_i)}$ with the columns of a slightly modified generalized Hadamard matrix

$$\widetilde{\mathbf{H}}_D = \{w_q^{2\mathbf{k}^{\mathrm{T}}\mathbf{D}_\lambda\mathbf{l}}\}_{\mathbf{l},\mathbf{k}\in\mathbb{Z}_D}. \tag{22}$$

The index of the column of $\widetilde{\mathbf{H}}_D$ returning the largest absolute correlation with $\mathbf{z}$ will then return an estimate of $\mathbf{p}_i$. Furthermore, because each diagonal block $\mathbf{P}_k$ of $\mathbf{P}$ is actually restricted to have only entries in $\mathbb{Z}_{p_k}$, we can further restrict the selection of the $\mathbf{p}_i$ in a feasible set $\mathcal{P}_i$ corresponding to an embedding of $\mathbb{Z}_{p_k}^{m_k}$ in $\mathbb{Z}_D$ according to the block $\mathbf{P}_k$ to which $\mathbf{p}_i$ is overlapping with.

Then, from a block diagonal chirp matrix estimate $\hat{\mathbf{P}}$, we get the chirp matrix estimate $\hat{\mathbf{S}} = \mathbf{D}_\lambda\hat{\mathbf{P}} + \hat{\widetilde{\mathbf{S}}}$ with cover hypothesis $\hat{\widetilde{\mathbf{S}}}$. As previously discussed, we attach this estimated chirp matrix with a soft value which is the sum of coherences w.r.t. to correlations made with the generalized Hadamard matrix, and final chirp matrix detection is performed by maximizing this soft value under all cover hypotheses.

Finally, "dechirping" is done as before by computing

$$\mathbf{x} = \{[w_q^{-\mathbf{l}^{\mathrm{T}}\hat{\mathbf{S}}\mathbf{l}}]_{\mathbf{l}}[\mathbf{y}]_{\mathbf{l}}\}_{\mathbf{l}\in\mathbb{Z}_D} \tag{23}$$

and an estimation of $\mathbf{k}$ is obtained by correlating $\mathbf{x}$ with the columns of $\mathbf{H}_D$.

Algorithm 2 ChirpRA – Generalized

```
Inputs: Received signal: $\mathbf{y}$
        Set of cover matrices: $\widetilde{\mathcal{S}} = \{\widetilde{\mathbf{S}}_a\}_0^{|\widetilde{\mathcal{S}}|-1}$
        Sets of feasible columns of $\mathbf{P}$: $\{\mathcal{P}_i\}_{i=1}^m$
Initialization: $\bar{\mu} = 0$, $\{\mu_a = 0\}_a$
  for $a = 0$ to $|\widetilde{\mathcal{S}}| - 1$ do
    $\mathbf{c}_a = \left\{w_q^{-\mathbf{l}^T\widetilde{\mathbf{S}}_a\mathbf{l}}\right\}_{\mathbf{l}\in\mathbb{Z}_D}$
    $\tilde{\mathbf{y}}_a = \mathbf{c}_a \odot \mathbf{y}$
    for $i = 1$ to $m$ do
      $\tilde{\mathbf{y}}_a^{(\mathbf{e}_i)} = \{[\tilde{\mathbf{y}}_a]_{\mathbf{l}+\mathbf{e}_i}\}_{\mathbf{l}\in\mathbb{Z}_D}$
      $\mathbf{z}_a = \tilde{\mathbf{y}}^*_{\underset{\sim}{a}} \odot \tilde{\mathbf{y}}_a^{(\mathbf{e}_i)}$
      $\mathbf{h}_{a,i} = \mathbf{H}^*_D\mathbf{z}_a$
      $\mathbf{p}_{a,i} = \arg\max_{\mathbf{l}\in\mathcal{P}_i}|[\mathbf{h}_{a,i}]_{\mathbf{l}}|$
      $\mu_a \leftarrow \mu_a + \max_{\mathbf{l}\in\mathcal{P}_i}|[\mathbf{h}_{a,i}]_{\mathbf{l}}|$
    end for
    if $\mu_a > \bar{\mu}$ then
      $\hat{\mathbf{P}} \leftarrow \{\mathbf{p}_{a,i}, \ldots, \mathbf{p}_{a,m}\}$
      $\hat{a} \leftarrow a$, $\bar{\mu} \leftarrow \mu_a$
    end if
  end for
  $\hat{\mathbf{S}} = \mathbf{D}_\lambda\hat{\mathbf{P}} + \widetilde{\mathbf{S}}_{\hat{a}}$
  $\mathbf{c} = \{w_q^{-\mathbf{l}^{\mathrm{T}}\hat{\mathbf{S}}\mathbf{l}}\}_{\mathbf{l}\in\mathbb{Z}_D}$
  $\mathbf{x} = \mathbf{c} \odot \mathbf{y}$
  $\hat{\mathbf{k}} = \arg\max_{\mathbf{l}\in\mathbb{Z}_D}|[\mathbf{H}^*_D\mathbf{x}]_{\mathbf{l}}|$
Output: $\hat{\mathbf{S}}$ and $\hat{\mathbf{k}}$
```

An implementation of this generalized ChirpRA is summarized in Algorithm 2. Alternatively, one could also do a joint estimation of the columns of $\mathbf{P}$ to guarantee in addition that we always satisfy $\mathbf{D}_\lambda\mathbf{P} \in \bar{\mathcal{S}}$, limiting further the probability of error. This may improve the performance when $\bar{\mathcal{S}}$ is very small, otherwise for a large set $\bar{\mathcal{S}}$ performance gain is unnoticeable while requiring much more computer memory.

3) The Generalized Hadarmard Transform (GHT): In Algorithm 2 we need several times to correlate vectors with the columns of $\mathbf{H}_D$ or $\widetilde{\mathbf{H}}_D$, which we will refer to as the generalized Hadarmard transform (GHT).

First, we remark that $\widetilde{\mathbf{H}}_D$ is a column permutation of $\mathbf{H}_D$ and thus essentially the same operator. Moreover, in the cases $D = 2^{m_1}\cdot 3^{m_2}$, as $2x = -x \mod 3$ and $x = -x \mod 2$, it can be verified that $w_q^{2\mathbf{k}^{\mathrm{T}}\mathbf{D}_\lambda\mathbf{l}} = w_q^{-\mathbf{k}^{\mathrm{T}}\mathbf{D}\mathbf{l}}$ and thus $\widetilde{\mathbf{H}}_D = \mathbf{H}^*_D$.

The GHT is a Kronecker product of subdimentional DFT, as

$$\mathbf{H}_D = \bigotimes_{i=1}^{n}\bigotimes_{k=1}^{m_i}\mathbf{F}^*_{p_i} \tag{24}$$

where $\mathbf{F}_{p_i}$ is the p_i-point DFTs. Note that $\mathbf{F}_2 = \mathbf{H}_2$ is the 2×2 Hadamard matrix. The GHT can thus be implemented by a cascade of WHTs and DFTs.

Taking for simplicity the case $D = 2^{m_1}\cdot 3$, which is also related to practical 3GPP resource allocation where one physical resource block (PRB) is made of 12 subcarriers, this corresponds to apply a DFT to each 2^{m_1} segments of 3 entries of the input vector, and then taking each kth entry of each

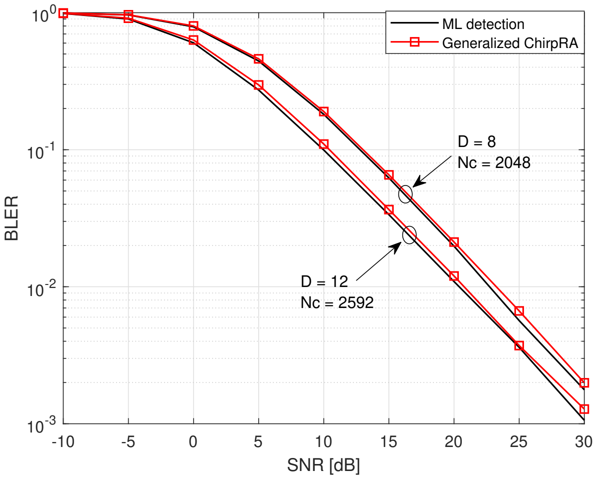

Fig. 1. Error rate of ChirpRA compared to ML decoding for extended frame S_m^{+} in $D = 8$ and generalized frame in composite dimension $D = 12$.

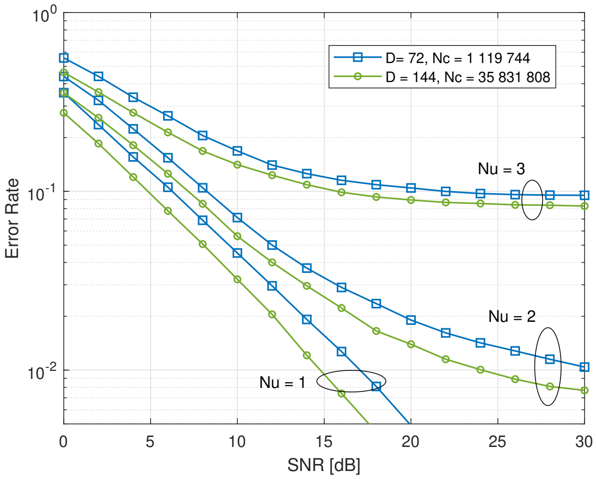

Fig. 2. Error rate of Generalized ChirpRA for multi-user access with $D = 76$ and $D = 144$.

segment together and process them by a WHT. This takes in total 2^{m_1} 3-point DFTs and three 2^{m_1}-point WHTs. As a 3-point DFT can be implemented with 2 complex multiplications (and 8 complex additions), a GHT would take 2^{m_1+1} complex multiplications, i.e., scaling as $\mathcal{O}(D)$, while the number of addition scales as previously as $\mathcal{O}(D\log_2 D)$. Additionally, because the matrix $\mathbf{P}$ is constrained to a block diagonal structure, only few columns of $\widetilde{\mathbf{H}}_D$ with related indexes are relevant. The first m_1 columns of $\mathbf{P}$ corresponds actually to the all-one column of the 3-point DFT in $\widetilde{\mathbf{H}}_D$ and thus correlation with corresponding columns does not require any multiplication. Overall, we need to perform $(|\widetilde{\mathcal{S}}| - 1)D + |\widetilde{\mathcal{S}}|(3/2D(m_1+2) + 2^{m_1+2})$ complex multiplications which is dominated as $\mathcal{O}(m_1 2^{m_1}|\widetilde{\mathcal{S}}|)$.

IV. Applications and Simulations

We consider a multiple-access transmission as

$$\mathbf{y} = \sqrt{\mathrm{snr}}\sum_{u=1}^{N_\mathrm{u}} h_u \mathbf{x}_u + \mathbf{n} \tag{25}$$

where $\mathbf{x} \in \mathbb{C}^{D\times 1}$ is the per-user transmitted codeword satisfying $\|\mathbf{x}\|^2 = D$, h_u are independent and identically distributed channel fading components following a standard normal distribution, $\mathbf{n} \in \mathbb{C}^{D\times 1}$ is a zero-mean unit-variance average white Gaussian noise, and $\mathbf{y} \in \mathbb{C}^{D\times 1}$ is the received signal. Each user transmit a codeword from a shared codebook $\mathcal{C}$ of size N_c. The receiver does not have any a-priori knowledge of the channels, however we assume that N_u is known for simplicity.

If $N_\mathrm{u} = 1$, this is referred to as a non-coherent communication scenario. Otherwise, this corresponds to an unsourced random access scenario where the receiver should decode the codewords from a small number of colliding users up to a permutation so without needs for performing any user identification.

a) Non-coherent communications with $N_\mathrm{u} = 1$: Fig. 1 shows the detection performance with $N_\mathrm{u} = 1$ of an expanded frame in $D = 8$ with size $N_\mathrm{c} = 2^{11}$ which is obtained by taking the maximal Reed-Muller frame of size 2^9, and using $|\widetilde{\mathcal{S}}| = 4$ covers where the non-trivial covers are $\widetilde{\mathbf{S}}_1 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$, $\widetilde{\mathbf{S}}_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ and $\widetilde{\mathbf{S}}_3 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$. Fig. 1 shows as well as the performance for a generalized frame in $D = 12$ of size $N_\mathrm{c} = 2^5 \cdot 3^4$ which corresponds to the construction EBD6 in [7].

Comparison is made between an ML detection and a generalized ChirpRA taking the 4 cover hypotheses into account. ML rule is [8] $\hat{\mathbf{x}} = \arg\max_{\mathbf{x}\in\mathcal{C}} \|\mathbf{y}^\mathrm{H}\mathbf{x}\|^2$, requiring $N_\mathrm{c}(D + 1/2)$ complex multiplications and $N_\mathrm{c}(D-1)$ complex additions, both dominated as $\mathcal{O}(N_\mathrm{c}D)$ which thus become prohibitive for large dimensions with large frames. As we can see the generalized ChirpRA performs close to ML detection while it takes only $148 \approx 0.8\%$ complex multiplications compared to the 17408 with ML for $D = 8$, and $888 \approx 2.7\%$ complex multiplications compared of the 32400 with ML for $D = 12$.

b) Unsourced Random Access $N_\mathrm{u} \geq 1$: With multiple-access, we are interested in larger D in order to exploit sparse signal processing techniques. For this, we integrate ChirpRA in an orthogonal matching pursuit procedure as in [6]. Fig. 2 shows the performance obtained for $D = 72 = 2^3 \cdot 3^2$ with $N_\mathrm{c} = 2^9 \cdot 3^7$ and $D = 144 = 2^4 \cdot 3^2$ with $N_\mathrm{c} = 2^{14} \cdot 3^7$. These would correspond from a 3GPP perspective to a resource allocation of 6 PRBs and 12 PRBs, transmitting 20 and 25 bits respectively. The frames are constructed by taking all possible diagonal blocks and 9 covers. The obtained multi-user performance from $N_\mathrm{u} = 1$ to 3 is consistent with the one in [9] for the original Reed-Muller frames and their subspace chirp expansion. Remark that the complexity of performing similar simulations but with an ML decoding would be prohibitive.

V. Conclusion

We generalized the low-complexity chirp reconstruction algorithm to generalized second-order Reed-Muller frames, and demonstrated its feasibility for multiple user detection in a massive unsourced random access setting.

References

[1] Huawei, “R1-2007584: Potential solutions for PUCCH coverage enhancement,” www.3gpp.org, 3GPP TSG RAN WG1, meeting 103-e, Nov. 2020.

[2] Y. Polyanskiy, “A perspective on massive random-access,” in *IEEE Int. Symp. Inf Theory ISIT*, 2017, pp. 2523–2527.

[3] R. Calderbank, S. Howard, and S. Jafarpour, “Construction of a large class of deterministic sensing matrices that satisfy a statistical isometry property,” *IEEE J. Sel. Topics Sig. Proc.*, vol. 4, no. 2, pp. 358–374, Apr. 2010.

[4] R. Calderbank and S. Jafarpour, “Reed Muller sensing matrices and the LASSO,” in *Proc. Int. Conf. Sequences and Their Applications*. Springer, 2010, pp. 442–463.

[5] S. D. Howard, A. R. Calderbank, and S. J. Searle, “A fast reconstruction algorithm for deterministic compressive sensing using second order Reed-Muller codes,” in *Proc. Annual Conf. Inf. Sciences and Systems*, 2008, pp. 11–15.

[6] R. Calderbank and A. Thompson., “CHIRRUP: a practical algorithm for unsourced multiple access,” *Information and Inference: A Journal of the IMA*, no. iaz029, 2019.

[7] R.-A. Pitaval and Y. Qin, “Grassmannian frames in composite dimensions by exponentiating quadratic forms,” in *Proc. IEEE Int. Symp. Inf. Theory*, June 2020, pp. 13–18.

[8] B. M. Hochwald and T. L. Marzetta, “Unitary space-time modulation for multiple-antenna communications in Rayleigh flat fading,” *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 543–564, Mar. 2000.

[9] T. Pllaha, O. Tirkkonen, and R. Calderbank, “Reconstruction of multi-user binary subspace chirps,” in *Proc. IEEE Int. Symp. Inf. Theory*, June 2020, pp. 531–536.