Deterministic Matrices with a Restricted Isometry Property for Partially Structured Sparse Signals

Alihan Kaplan, Volker Pohl, Holger Boche

Chair of Theoretical Information Technology, Technical University of Munich, 80 333 München, Germany

Abstract—**Compressive sampling has become an important tool in diverse applications. One of its main challenges, the construction of deterministic sensing matrices with restricted isometry property (RIP) in the optimal sparsity regime, is still an open problem, despite being of crucial importance for practical system designs. The only known work constructing deterministic RIP matrices beyond the square root bottleneck is due to Bourgain et al. The aim of this paper is to construct sensing matrices consisting of two orthogonal bases and to analyse their RIP properties based on the flat-RIP. Using a known estimation on exponential sums due to Karatsuba, we deduce an RIP result for signals which are restricted to a certain sparse structure. Without any assumption on the sparsity structure, we end up facing a known open problem from number theory regarding exponential sums.**

Index Terms—**deterministic compressive sampling, flat restricted isometry property, structured sparsity**

I. INTRODUCTION

Compressive Sampling (CS) is a modern signal processing framework which became popular recently. The main idea is that a sparse signal can be recovered from fewer measurements then its ambient dimension [1], [2] and so, CS has found its way into various engineering applications [3]–[6]. The usual model is that of an underdetermined system of linear equations $\mathbf{y} = \mathbf{\Phi}\mathbf{x}$ with $\mathbf{y} \in \mathbb{C}^m$, $\mathbf{x} \in \mathbb{C}^N$, $m \ll N$ and $|\text{supp}(\mathbf{x})| \leq s$. We denote the set of s-sparse vectors in $\mathbb{C}^N$ by Σ_s^N, and we call $\mathbf{\Phi}$ the sensing (or measurement) matrix. The main result of CS states that when s is sufficiently small then $\mathbf{x}$ can be uniquely recovered from $\mathbf{y}$ provided $\mathbf{\Phi}$ satisfies some sufficient conditions. One such sufficient condition is the *restricted isometry property* (RIP) which was introduced in [7]. The following definition of the RIP is taken from [2].

Definition 1: *A matrix $\mathbf{\Phi} \in \mathbb{C}^{m \times N}$ has the (s, δ)-restricted isometry property if*

$$(1 - \delta)\|\mathbf{x}\|_2^2 \leq \|\mathbf{\Phi}\mathbf{x}\|_2^2 \leq (1 + \delta)\|\mathbf{x}\|_2^2$$

for every s-sparse vector $\mathbf{x} \in \mathbb{C}^N$. The smallest δ for which $\mathbf{\Phi}$ has (s, δ)-RIP is the restricted isometry constant (RIC) δ_s. Equivalently

$$\delta_s = \max_{\substack{\mathcal{I} \subset \{0,1,\dots,N-1\} \\ |\mathcal{I}| \leq s}} \sigma_{\max}\left(\mathbf{\Phi}_\mathcal{I}^* \mathbf{\Phi}_\mathcal{I} - \mathbf{I}_s\right). \tag{1}$$

Based on RIP, recovery guarantees with high probability were proven for random constructions of the sensing matrix $\mathbf{\Phi}$ and for sparsity levels $s < c\frac{m}{\log(N/s)}$ with a certain positive constant c [1], [2], [8]. Deterministic constructions of matrices with RIP in the optimal sparsity regime are not known. To the best of our knowledge, the only construction of a deterministic RIP matrix beyond the quadratic bottleneck is given in [9]. Despite being a mathematical breakthrough the improvement made on the sparsity level is negligible from a practical point of view [10]. Therefore the search for deterministic RIP matrices remains an interesting question from a practical and theoretical perspective.

This paper investigates a family of sensing matrices which are concatenations of two orthogonal matrices. We prove an RIP result beyond the quadratic bottleneck for sparse signals with a certain support pattern, following the ideas of flat-RIP introduced in [9]. More precisely, we use the flat-*restricted orthogonality* (RO) given in [11] as an alternative description of the flat-RIP. Our main result may be summarized as follows: For all signals having a certain sparsity pattern $\mathbf{x} \in \Lambda \subset \Sigma_s^N \subset \mathbb{C}^N$ the constructed sensing matrices satisfy $(s, \delta_{\Lambda,s})$-RIP with $s \leq m^{\frac{29}{40}+\kappa}$ and $\delta_{\Lambda,s} = 300 c_0 m^{-0.002+\kappa} \log(m)$ for any $\kappa < 0.002$. Here $\frac{9}{40} + \kappa > 0$ reflects the improvement over the quadratic bottleneck.

We want to point out that our analysis is similar to [12]. Although we follow a different path the underlying core estimation idea in both approaches is the same.

II. PRELIMINARIES AND RELEVANT RESULTS

We consider vectors $\mathbf{g}$ in the m-dimensional Euclidean vector space $\mathbb{C}^m$. Entries in these vectors are indexed by the m-element cyclic group $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, i.e. $\mathbf{g} = (\mathbf{g}(0), \mathbf{g}(1), \dots, \mathbf{g}(m-1))^\mathrm{T}$. The identity matrix in $\mathbb{C}^m$ is denoted by $\mathbf{I}_m$ and $\mathbf{F}$ stands for the discrete Fourier transform (DFT) matrix in $\mathbb{C}^m$, given by

$$\mathbf{F} = [\mathbf{f}_0\ \mathbf{f}_1\ \dots\ \mathbf{f}_{m-1}] \quad \text{with columns} \quad \mathbf{f}_l(j) = \tfrac{1}{\sqrt{m}}\,\omega^{lj} \tag{2}$$

wherein $\omega = \exp\{i\frac{2\pi}{m}\}$. Let $\mathbf{A} = \{a_{l,j}\}_{l,j \in \{0,\dots,m-1\}} \in \mathbb{C}^{m \times m}$ be a matrix with entry $a_{l,j}$ in l-th row and j-th column. If $\mathcal{I}, \mathcal{J} \subset \{0, 1, \dots, m-1\}$ are two index sets, then the submatrix $\mathbf{A}_{\mathcal{I},\mathcal{J}}$ of $\mathbf{A}$ is given by $\mathbf{A}_{\mathcal{I},\mathcal{J}} = \{a_{l,j}\}_{l \in \mathcal{I}, j \in \mathcal{J}}$. If $\mathcal{I} = \mathcal{J}$ then $\mathbf{A}_{\mathcal{I},\mathcal{I}}$ is called a *principal submatrix* of $\mathbf{A}$. Moreover, the eigenvalue of $\mathbf{A}$ with the largest magnitude is denoted by $\lambda_{\max}(\mathbf{A})$ and $\sigma_{\max}(\mathbf{A})$ stands for the largest singular value. Similarly, given a sensing matrix $\mathbf{\Phi} \in \mathbb{C}^{m \times N}$ and an index set $\mathcal{I}$ with $|\mathcal{I}| = s$, we denote the submatrix of $\mathbf{\Phi}$ consisting of the columns of $\mathbf{\Phi}$ indexed by $\mathcal{I}$ as $\mathbf{\Phi}_\mathcal{I} \in \mathbb{C}^{m \times s}$.

Characters in finite fields: For an arbitrary prime number p, $\mathbb{F}_p$ stands for the finite field of order p. Let α be a fixed primitive element of $\mathbb{F}_p$. The multiplicative characters in $\mathbb{F}_p$ are given by

$$\chi_{\alpha^l}\left(\alpha^k\right) = \exp\left\{i\frac{2\pi}{p-1}kl\right\} \quad \text{for} \ l, k \in \{0, 1, \dots, p-2\} \tag{3}$$

$$\text{and} \quad \chi_{\alpha^l}(0) = 0 \ \text{for} \ l \in \{0, 1, \dots, p-2\}\,.$$

Legendre symbol and exponential sums: The quadratic residues of a finite field will play an important role in the upcoming analysis. Assume p to be a prime number and define the set of quadratic residues in the finite field $\mathbb{F}_p$ as

$$\mathcal{QR} = \left\{x^2 \,:\, x \in \mathbb{F}_p\,, x \neq 0\right\},$$

and the corresponding *Legendre symbol* is defined as follows

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \in \mathcal{QR} \\ -1 & \text{if } a \notin \mathcal{QR} \ \text{and } a \neq 0 \\ 0 & \text{if } a \equiv 0 \mod p \end{cases} . \tag{4}$$

It will be important to note that the Legendre symbol is just a particular multiplicative character (3) on $\mathbb{F}_p$ obtained by setting $l = (p-1)/2$ in (3), i.e. one has

$$\left(\frac{\alpha^k}{p}\right) = \chi_{\alpha^{(p-1)/2}}(\alpha^k) = \exp(i\pi k) =: \chi_L(\alpha^k) \tag{5}$$
$$\text{and} \quad \chi_L(0) = 0 \, .$$

Later we will also need the following well-known result on quadratic Gauss sum, see [13].

Theorem 1: *For all odd integers $n \geq 3$, one has*

$$\sum_{x=0}^{n-1} \exp\left\{i\frac{2\pi}{n}x^2\right\} = \begin{cases} \sqrt{n} & \text{if } n \equiv 1 \mod 4 \\ i\sqrt{n} & \text{if } n \equiv 3 \mod 4 \end{cases} \, .$$

Our analysis will use an estimate on character sums due to Karatsuba. The following theorem can be found in this form in [15], for more details see [16] and [17].

Theorem 2: *Let χ be a non-trivial multiplicative character of $\mathbb{F}_p$ and $\mathcal{I}, \mathcal{J} \subset \mathbb{F}_p$. If $|\mathcal{I}| > p^{0.5+\gamma}$ and $|\mathcal{J}| > p^\gamma$, where $0 < \gamma < 0.5$, then*

$$\left| \sum_{a \in \mathcal{I}} \sum_{b \in \mathcal{J}} \chi(a+b) \right| \leq cp^{-0.05\gamma^2} |\mathcal{I}| |\mathcal{J}|$$

holds for some constant $c > 0$.

Flat restricted orthogonality: The flat restricted orthogonality as given in [11] is going to play a key role in our analysis. Here we briefly discuss some known results and the connections between RIP, RO and flat-RO which will be used in the upcoming sections. Restricted orthogonality is a property which is closely related to the RIP [2] and defined as follows.

Definition 2: *The (k,l)-restricted orthogonality constant (ROC) $\theta_{k,l}$ of a matrix $\mathbf{\Phi}$ is the smallest $\theta \geq 0$ such that*

$$|\langle \mathbf{\Phi}\mathbf{u}, \mathbf{\Phi}\mathbf{v} \rangle| \leq \theta \|\mathbf{u}\|_2 \|\mathbf{v}\|_2$$

for all disjointly supported k-sparse and l-sparse vectors $\mathbf{u}$ and $\mathbf{v}$, respectively. Equivalently it is given by

$$\theta_{k,l} = \max\{\sigma_{\max}(\mathbf{\Phi}_K^*\mathbf{\Phi}_L) \, , \, K \cap L = \emptyset \, , \, |K| \leq k, |L| \leq l\}$$

where $\sigma_{\max}(\mathbf{\Phi}_K^*\mathbf{\Phi}_L)$ is the largest singular value of $\mathbf{\Phi}_K^*\mathbf{\Phi}_L$.

An idea used in [9] is the flat-RIP. An alternative formulation of the flat-RIP is given as flat-RO in [11], which will play a fundamental role subsequently.

Definition 3: *The matrix $\mathbf{\Phi} = [\boldsymbol{\varphi}_1, \boldsymbol{\varphi}_2, ..., \boldsymbol{\varphi}_N]$ has $(s, \hat{\theta})$-flat restricted orthogonality if*

$$\left| \left\langle \sum_{l \in \mathcal{I}} \boldsymbol{\varphi}_l, \sum_{j \in \mathcal{J}} \boldsymbol{\varphi}_j \right\rangle \right| \leq \hat{\theta}\sqrt{|\mathcal{I}||\mathcal{J}|} \tag{6}$$

for each disjoint pair $\mathcal{I}, \mathcal{J} \subseteq \{1, ..., N\}$ with $|\mathcal{I}|, |\mathcal{J}| \leq s$.

The following theorem (Thm. 13 in [11]) gives an estimation of the restricted orthogonality based on the flat restricted orthogonality.

Theorem 3: *A matrix with $(s, \hat{\theta})$-flat restricted orthogonality has a restricted orthogonality constant satisfying $\theta_{s,s} \leq C\hat{\theta} \log s$, and we may take $C = 75$.*

Finally, we need the following auxiliary result which can be found in [2], [10].

Lemma 4: *If $\mathbf{\Phi}$ has (s, δ)-RIP, then $\mathbf{\Phi}$ has $(ns, 2n\delta)$-RIP for all $n \geq 1$.*

It gives an estimate on the restricted isometry property for larger sparsity if the RIP is already known for a small values of sparsity.

III. CONSTRUCTION OF THE SENSING MATRIX

This section describes the construction of the sensing matrices $\mathbf{\Phi}$ and gives some insight into their structure. To this end, we define for an odd prime number m the vector $\boldsymbol{\phi} \in \mathbb{C}^m$ by

$$\phi(x) = \begin{cases} \left(\frac{x}{m}\right) & \text{if } x \in \{1, ..., m-1\} \\ -1 & \text{if } x = 0 \end{cases}$$

and therewith the diagonal matrix $\mathbf{D}_\phi = \text{diag}(\boldsymbol{\phi})$. Then we set

$$\mathbf{C} = \mathbf{D}_\phi \mathbf{F}$$

wherein $\mathbf{F}$ is the unitary DFT-matrix defined in (2). Now we consider the $m \times 2m$ sensing matrix $\mathbf{\Phi} = [\mathbf{C} \mid \mathbf{F}]$ and investigate its Gram matrix

$$\mathbf{G} = \mathbf{\Phi}^*\mathbf{\Phi} = \begin{bmatrix} \mathbf{C}^*\mathbf{C} & \mathbf{C}^*\mathbf{F} \\ \mathbf{F}^*\mathbf{C} & \mathbf{F}^*\mathbf{F} \end{bmatrix} = \begin{bmatrix} \mathbf{I}_m & \mathbf{U} \\ \mathbf{U}^* & \mathbf{I}_m \end{bmatrix} \tag{7}$$

with $\mathbf{U} = \mathbf{C}^*\mathbf{F} = \mathbf{F}^*\mathbf{D}_\phi\mathbf{F}$. We note that $\mathbf{U}$ is unitary, self-adjoint, and because $\mathbf{U}$ is diagonalized by the DFT matrix, it is circulant. In fact $\mathbf{U}$ has only three different entries because each entry can be written by means of a quadratic Gaussian sum as expressed in Theorem 1. Indeed, using some elementary relations from number theory on quadratic congruences (see, e.g., [13]) and Theorem 1, one obtains for the entries $u_{l,j} = \langle \mathbf{c}_l, \mathbf{f}_j \rangle$ of $\mathbf{U}$, the values

$$\langle \mathbf{c}_l, \mathbf{f}_j \rangle = \langle \mathbf{f}_l, \mathbf{D}_\phi \mathbf{f}_j \rangle = \frac{1}{m} \sum_{x \in \mathcal{QR}} \left(\omega^{j-l}\right)^x - \frac{1}{m} \sum_{x \in \mathcal{QR}^c} \left(\omega^{j-l}\right)^x$$
$$= \begin{cases} \frac{1}{m}\left(-1 + \left(\frac{j-l}{m}\right)\sqrt{m}\right) & \text{if } m \equiv 1 \mod 4 \\ \frac{1}{m}\left(-1 - i\left(\frac{j-l}{m}\right)\sqrt{m}\right) & \text{if } m \equiv 3 \mod 4 \end{cases} \tag{8}$$

with $\omega = \exp\left\{i\frac{2\pi}{m}\right\}$, and where $\mathbf{c}_l$ is the l-th column of $\mathbf{C}$.

An obvious question is what can we say about the RIP in our two-ortho case $\mathbf{\Phi} = [\mathbf{C} \mid \mathbf{F}]$ from the Gram matrix $\mathbf{G}$ given in (7)? In fact, one can upper bound the restricted isometry constant δ of our sensing matrix for any sparsity as follows.

Proposition 1: *The restricted isometry constant of $\mathbf{\Phi} = [\mathbf{C}|\mathbf{F}]$ satisfies $\delta_s \leq 1$ for any sparsity $s \leq m$.*

The proof of this statement follows easily from the following well known lemma.

Lemma 5 (Thm. 4.3.15 in [14]): *Let $\mathbf{A}$ be a Hermitian matrix, let s be an integer with $1 \leq s \leq m$, and let $\mathbf{A}_s$ be an arbitrary s-by-s principal submatrix of $\mathbf{A}$. Then*

$$\lambda_k(\mathbf{A}) \leq \lambda_k(\mathbf{A}_s) \leq \lambda_{k+m-s}(\mathbf{A}) \qquad \text{for all } 1 \leq k \leq s \, .$$

Therein $\lambda_k(\mathbf{A})$ stands for the k-th eigenvalue of $\mathbf{A}$ sorted in increasing order.

Proof (Proposition 1): Recall the definition of the s-th restricted isometry constant,

$$\delta_s = \max_{\substack{\mathcal{I} \subseteq \{0,1,...,N-1\} \\ |\mathcal{I}|=s}} \lambda_{\max}\left((\mathbf{\Phi}_\mathcal{I}^*\mathbf{\Phi}_\mathcal{I}) - \mathbf{I}_s\right)$$

and note that $\mathbf{\Phi}_\mathcal{I}^*\mathbf{\Phi}_\mathcal{I}$ is a principal submatrix of the Gram matrix $\mathbf{G} = \mathbf{\Phi}^*\mathbf{\Phi}$. In fact $\mathbf{\Phi}_\mathcal{I}^*\mathbf{\Phi}_\mathcal{I} - \mathbf{I}_s$ is a principal submatrix of $\mathbf{G} - \mathbf{I}_{2m}$. It is easy to verify that $\mathbf{G} - \mathbf{I}_{2m}$ is unitary and has only the eigenvalues 1 and -1. Lemma 5 implies that the eigenvalues of any principal submatrix of $\mathbf{G} - \mathbf{I}_{2m}$ lie in the interval $[-1, 1]$, which then implies that $\delta_s \in [0, 1]$ for all $s \leq m$. ∎

The standard approach with the Gershgorin circles (which results in the well known quadratic bottleneck for the sparsity) would give

sparsity results proportional to $\sqrt{m}$, because the coherence of the sensing matrices is $\mu(\mathbf{\Phi}) = \frac{\sqrt{m+1}}{m}$. In contrast to this, Proposition 1 asserts that the RIC is upper bounded by 1 indicating that our constructed matrices are suitable sensing matrices.

IV. AN RIP RESULT FOR STRUCTURED SPARSITY

After these preparations we are able to present our main result. It shows that the $m \times 2m$ matrices $\mathbf{\Phi}$ introduced in Section III have RIP for structured sparse vectors in $\mathbb{C}^{2m}$.

The sparsity structure is characterized by the support set $\mathrm{supp}(\mathbf{x})$ of the vectors $\mathbf{x} \in \Sigma_s^{2m}$. We assume that $\mathrm{supp}(\mathbf{x})$ belongs to the set Γ with $|\mathrm{supp}(\mathbf{x})| \leq s$ and where every $S \in \Gamma$ has the following sparsity structure:

$$S = A \cup B \quad \text{with} \quad \begin{array}{l} A \subset \{0, ..., m-1\} \\ B \subset \{m, ..., 2m-1\} \end{array}$$

where

$$m^{\gamma_-} < |A| < m^{0.5-\gamma_+} \quad \text{and} \quad m^{0.5+\gamma_-} < |B| < m^{0.5+\gamma_+} \quad (9)$$

with $0 < \gamma_- < \gamma_+$ and $\gamma_-, \gamma_+ \in \left(0, \frac{1}{4}\right]$ For instance a valid choice for these parameters is $\gamma_- = \frac{1}{5}$ and $\gamma_+ = \frac{1}{4}$.

Then

$$\Lambda = \left\{ \mathbf{x} \in \Sigma_s^{2m} \ : \ \mathrm{supp}(\mathbf{x}) \in \Gamma \right\}$$

is the set of all s-sparse vectors in $\mathbb{C}^{2m}$ with this particular sparsity pattern.

For structured s-sparse vectors in Λ, we can prove now the following result.

Theorem 6: *Let $\mathbf{\Phi} \in \mathbb{C}^{m \times 2m}$ be the matrix as defined in Section III. Then one has for every $\mathbf{x} \in \Lambda \subset \Sigma_s^{2m}$*

$$(1 - \delta_{\Lambda, s}) \|\mathbf{x}\|_2^2 \leq \|\mathbf{\Phi}\mathbf{x}\|_2^2 \leq (1 + \delta_{\Lambda, s}) \|\mathbf{x}\|_2^2$$

with $|\mathrm{supp}(\mathbf{x})| \leq m^{\frac{29}{40}+\kappa}$ and $\delta_{\Lambda, s} = 300 c_0 m^{-0.002+\kappa} \log(m)$, for all $\kappa < 0.002$ and with an appropriate constant $c_0 > 0$.

Remark: Theorem 6 holds only for support patterns as defined in (9), i.e. for supports $\mathrm{supp}(\mathbf{x}) = A \cup B$ such that $|A| \leq m^{\frac{29}{40}+\kappa}$ is satisfied by one part of the support, and $|B| \leq m^{\frac{9}{20}+\kappa}$ holds for the other part of the support. So Theorem 6 holds for signals whose support is known to be highly concentrated on either A or B.

Proof: We start by deriving an estimate for the flat restricted orthogonality of $\mathbf{\Phi}$ as given in Def. 3. To this end, we note that $\mathbf{\Phi}$ was defined by $\mathbf{\Phi} = [\mathbf{C} \mid \mathbf{F}]$ and that the support pattern S of vectors $\mathbf{x} \in \Sigma_s^{2m}$ are in Γ, i.e. they have the structure (9) with disjoint sets A, B. Consequently the expression on the left hand side of (6) is equal to the sum of the entries of the matrix $\mathbf{\Phi}_A^* \mathbf{\Phi}_B = \mathbf{C}_A^* \mathbf{F}_B = \mathbf{U}_{A,B}$. For the calculation, it is assumed that $|A| \leq m^\epsilon$ and $|B| \leq m^{0.5+\epsilon}$. Using the particular structure of $\mathbf{U}$, as discussed in Sec. III, and in particular (8), one gets

$$\left| \sum_{a \in A} \sum_{b \in B} \langle \mathbf{c}_a, \mathbf{f}_b \rangle \right| \leq \frac{1}{m} |A||B| + \frac{1}{\sqrt{m}} \left| \sum_{a \in A} \sum_{b \in B} \left(\frac{a-b}{m} \right) \right| \quad (10)$$

wherein $\mathbf{c}_a$ and $\mathbf{f}_b$ stands for the a-th and b-th column of the matrix $\mathbf{C}$ and $\mathbf{F}$, respectively. Our next step is to upper bound the sum on the right hand side of (10), we recall that the Legendre symbol is just a particular multiplicative character on $\mathbb{F}_m$ (cf. (5)). Consequently, Theorem 2 holds in particular for the character χ_L corresponding to the Legendre symbol. Then our support sets $S \in \Lambda$ satisfy the conditions of Theorem 2 which provides us with an upper bound on

the sum on the right hand side of (10) with an appropriately choosen ϵ, $\gamma_- < \epsilon < \gamma_+$. So overall, we get

$$\left| \sum_{a \in A} \sum_{b \in B} \langle \mathbf{c}_a, \mathbf{f}_b \rangle \right| \leq \left(\frac{1}{\sqrt{m}} + cm^{-0.05\gamma_-^2} \right) \sqrt{|A||B|}$$
$$\leq 2cm^{-0.05\gamma_-^2} \sqrt{|A||B|}. \quad (11)$$

In order to demonstrate that $\mathbf{\Phi}$ has $(m^{0.5+\epsilon}, \hat{\theta})$-flat restricted orthogonality with $\hat{\theta} = 2cm^{-0.05\gamma_-^2}$ and for signals with support set in Γ, we need to prove that (11) establishes an upper bound for all partial sums of the expression on the left hand side of (11).

Consider subsets $P_A \subset A$ and $P_B \subset B$. If $|P_A| > m^{\gamma_-}$ and $|P_B| > m^{0.5+\gamma_-}$ then one can still use the estimate of Theorem 2 and (11) remains an upper bound since $|P_A| \leq |A|$ and $|P_B| \leq |B|$. If however $|P_A| \leq m^{\gamma_-}$ or $|P_B| \leq m^{0.5+\gamma_-}$ then by setting $\gamma_- = \frac{1}{5}$ and $\gamma_+ = \frac{1}{4}$ and using the triangular inequality we get

$$\frac{1}{m}|P_A||P_B| + \frac{1}{\sqrt{m}} \left| \sum_{a \in P_A} \sum_{b \in P_B} \left(\frac{a-b}{m} \right) \right|$$
$$\leq \frac{1}{m}|P_A||P_B| + \frac{1}{\sqrt{m}} |P_A||P_B|$$
$$\leq 2m^{-\frac{1}{4}+\frac{\gamma_+}{2}+\frac{\gamma_-}{2}} \sqrt{|P_A||P_B|}$$
$$= 2m^{-0.025} \sqrt{|P_A||P_B|} \leq 2cm^{-0.002} \sqrt{|P_A||P_B|} \quad (12)$$

for sufficiently large m. The bounds (11) and (12) together show that $\mathbf{\Phi}$ satisfies $(m^{0.5+\epsilon}, \hat{\theta})$-flat restricted orthogonality with $\hat{\theta} = 2cm^{-0.05\gamma_-^2}$ with $\gamma_- < \epsilon < \gamma_+$ for signals with support set Γ.

Theorem 3 implies therefore that the restricted orthogonality constant of $\mathbf{\Phi}$ satiesfies $\theta_{m^\epsilon, m^{0.5+\epsilon}} \leq 150 c_0 m^{-0.05\gamma_-^2} \log(m)$, with $c_0 = c\left(\frac{1}{2}+\epsilon\right)$.

Now this gives an estimate for $\delta_{\Lambda, m^{0.5+\epsilon}} = \sigma_{\max}(\mathbf{U}_{A,B}) \leq 150 c_0 m^{-0.05\gamma_-^2} \log(m)$. Next using Lemma 4 we can generalize the scaling of $\delta_{\Lambda, s}$ to higher sparsity levels. Assume $s = m^{0.5+\epsilon+\kappa}$ for some $\kappa < 0.05\gamma_-^2$ then we can deduce $\delta_{\Lambda, s} \leq 300 c_0 m^{-0.05\gamma_-^2+\kappa} \log(m)$. Finally choosing $\gamma_- = \frac{1}{5}$, $\gamma_+ = \frac{1}{4}$ and $\epsilon = \frac{9}{40}$ establishes our assertion and finishes the proof. ∎

V. APPLICATION: TIME-DIVISION MULTIPLE-ACCESS

Theorem 6 holds only for signal with a particular sparsity structure (cf. Remark following Theorem 6). In the following, we sketch a very simple application where signals with such a sparsity structure may appear and Theorem 6 might be applied. Because of space constraints, the example might be somewhat oversimplified but we focus on describing the relation to Theorem 6.

Time-Division Multiple-Access (TDMA) is a widely used multiple access technique especially in wireless and vehicular communication system applications [18], [19]. In a standard TDMA scenario multiple users share the same carrier frequency to communicate with a base station. Each user is assigned a time slot during which it is allowed to transmit messages. However, due to multipath propagation, signals in consecutive time slot may interfere (cf. Figure 1). Therefore, a guard interval may be insert between consecutive time slots. However, if the transmitted signals are sparse, also the following approach might be applied to overcome this interference problem. Assume the transmitted signal of User 2 is $\tilde{u}(t) = \sum_{k=0}^{m-1} \tilde{s}(k) \delta\left(t - k\frac{T}{m}\right)$ for $t \in [T, 2T]$, where $\tilde{\mathbf{s}} = \mathbf{U}\mathbf{s}$ is the linear transformation of the actual
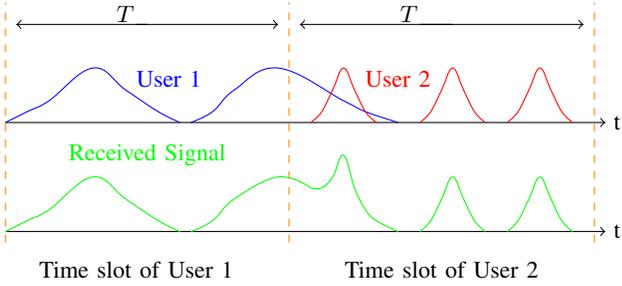
Fig. 1. The original signals of two users and the signal received by the base station. The received signal illustrates the interference of the signal of the second user by the transmission of the signal of the first user.

message **s** of User 2 using the matrix **U** from Section III for the linear transformation of **s**. Then the received signal of User 2 is

$$y(t) = \sum_{k=0}^{m-1} \mathbf{n}(k)\,\delta\left(t - k\frac{T}{m}\right) + \sum_{k=0}^{m-1} \tilde{\mathbf{s}}(k)\,\delta\left(t - k\frac{T}{m}\right) \quad (13)$$

where $\sum_{k=0}^{m-1} \mathbf{n}(k)\,\delta\left(t - k\frac{T}{m}\right)$ is the interference caused by the first user. Further, we can assume that **n** is a very sparse vector because we assume that only a small portion of the signal of User 1 is shifted in the time slot of User 2. If $\tilde{\mathbf{s}}$ is also sparse then we can formulate (13) as a standard CS problem

$$\mathbf{y} = [\mathbf{I}_m \mid \mathbf{U}]\,\mathbf{x} \quad (14)$$

where $\mathbf{x} = [\mathbf{n}\ \tilde{\mathbf{s}}]^T$ has a sparsity structure as in Theorem 6 with a support which is highly concentrated on the second half of the signal. Now, one can solve (14) to filter out the interference of User 1 from the message of User 2.

VI. CONCLUSION & OUTLOOK

Our main results holds only for signals with a particular sparsity structure. What happens if we drop this assumption on the structure of the support set of the signals? Note that we used in the proof of Theorem 6 the result by Karatsuba (Theorem 2) to estimate the sum in (10). The restrictions on the size of $\mathcal{I}$ and $\mathcal{J}$ in Theorem 2 is the reason for the constraint on the structure of the support set of our signals. For a general estimate on (10), we need to drop the condition on the size of $A, B \subset \mathbb{F}_p$. Writing the sum with a general non-principal multiplicative character, one ends up with a known problem from number theory, see, for example, [15, Problem 4.3].

Problem 1: *Let p be an odd prime, let $\gamma > 0$ be a real number, and let $A, B \subset \mathbb{F}_p$ be arbitrary sets with $|A|, |B| > p^\gamma$. Prove that there exists a number $\tau = \tau(\gamma)$ such that for any sufficiently large p and all non-trivial multiplicative characters χ the following estimation holds*

$$\left|\sum_{a \in A}\sum_{b \in B}\chi(a+b)\right| < p^{-\tau}|A||B|. \quad (15)$$

If a solution of Problem 1 would exist, we could use (15) to get an upper bound in (10) without any restriction on the support set of the signals.

Although the authors in [12] used a different construction for the sensing matrices, it is still possible in their case to write the inner products as quadratic Gaussian sums. Then they also end up with a sum as in (10) and use the flat-RIP to estimate the RIP. To estimate the sum of Legendre symbols the authors of [12] assume that Conjecture 2.2 from [20] holds and deduce under this condition

an estimate in the following form (cf. [12, Lemma 3.3]). Assume $p \equiv 1 \mod 4$, $\alpha > 0$, and $0 < \beta < 2$, then

$$\left|\sum_{\substack{a \in A\ b \in B}}\left(\frac{a-b}{p}\right)\right| \le p^\tau \sqrt{3\,|A|\,|B|} \quad (16)$$

for any $\tau \ge 2\alpha/(2-\beta)$ with $A, B \subset \mathbb{F}_p$, $|A| \le |B| \le p^{2\tau/(2-\beta)}$ and $A \cap B = \emptyset$.

In fact, if we would have access to an estimate as in (16) then we would not need to require the condition $|A|, |B| \le \sqrt{p}$ in our analysis and we could neglect the structure constraint on the support patterns. As a final remark, we recall the statement of Proposition 1 that the RIC of the sensing matrices constructed in Section III is not blowing up with increasing sparsity. This indicates that there might be some hope to derive better RIP results than what was achieved here.

REFERENCES

[1] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[2] S. Foucart and H. Rauhut, *A Mathematical Introduction to Compressive Sensing*. Birkhäuser Basel, 2013, vol. 1, no. 3.

[3] M. A. Herman and T. Strohmer, "High-resolution radar via compressed sensing," *IEEE Trans. Signal Process.*, vol. 57, no. 6, pp. 2275–2284, 2009.

[4] G. E. Pfander, H. Rauhut, and J. Tanner, "Identification of matrices having a sparse representation," *IEEE Trans. Signal Process.*, vol. 56, no. 11, pp. 5376–5388, 2008.

[5] M. Lustig, D. Donoho, and J. M. Pauly, "Sparse MRI: The application of compressed sensing for rapid MR imaging," *Magnetic Resonance in Medicine: An Official Journal of the International Society for Magnetic Resonance in Medicine*, vol. 58, no. 6, pp. 1182–1195, 2007.

[6] Z. Han, H. Li, and W. Yin, *Compressive Sensing for Wireless Networks*. Cambridge University Press, 2013.

[7] E. J. Candes and T. Tao, "Near-optimal signal recovery from random projections: Universal encoding strategies?" *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5406–5425, 2006.

[8] R. Baraniuk, M. Davenport, R. DeVore, and M. Wakin, "A simple proof of the restricted isometry property for random matrices," *Constr. Approx.*, vol. 28, no. 3, pp. 253–263, 2008.

[9] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, D. Kutzarova *et al.*, "Explicit constructions of RIP matrices and related problems," *Duke Math. J.*, vol. 159, no. 1, pp. 145–185, 2011.

[10] D. G. Mixon, "Explicit matrices with the restricted isometry property: Breaking the square-root bottleneck," in *Compressed Sensing and its Applications*. Springer, 2015, pp. 389–417.

[11] A. S. Bandeira, M. Fickus, D. G. Mixon, and P. Wong, "The road to deterministic matrices with the restricted isometry property," *J. Fourier Anal. Appl.*, vol. 19, no. 6, pp. 1123–1149, 2013.

[12] A. S. Bandeira, D. G. Mixon, and J. Moreira, "A conditional construction of restricted isometries," *International Mathematics Research Notices*, vol. 2017, no. 2, pp. 372–381, 2017.

[13] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge University Press, 1997, vol. 20.

[14] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge University Press, 1990.

[15] M.-C. Chang, "Character sums in finite fields," in *Proceedings 9th Intern. Conf. on Finite Fields and Applications*, AMS, Dublin, 2009.

[16] A. A. Karatsuba, "Arithmetic problems in the theory of Dirichlet characters," *Russian Math. Surveys*, vol. 63, no. 4, pp. 641–690, 2008.

[17] A. Karatsuba, "The distribution of values of Dirichlet characters on additive sequences," in *Doklady Acad. Sci. USSR*, vol. 319, 1991, pp. 543–545.

[18] D. D. Falconer, F. Adachi and B. Gudmundson, "Time division multiple access methods for wireless personal communications," *IEEE Communications Magazine*, vol. 33, no. 1, pp. 50–57, 1995.

[19] W. Zimmermann and R. Schmidgall, *Bussysteme in der Fahrzeugtechnik*. Springer, 2006.

[20] F. R. Chung, "Several generalizations of Weil sums," *J. Number Theory*, vol. 49, no. 1, pp. 95–106, 1994.