Some results on convolution idempotents

P Charantej Reddy
IIT Hyderabad
Email: ee18resch01010@iith.ac.in

Aditya Siripuram
IIT Hyderabad
Email: staditya@iith.ac.in

Brad Osgood
Stanford University
Email: osgood@stanford.edu

***Abstract*—We consider the problem of recovering N length vectors h that vanish on a given set of indices and satisfy $h{*}h = h$. We give some results on the structure of such h when N is a product of two primes, and investigate some bounds and their connections to certain graphs defined on $\mathbb{Z}_N$.**

***Index Terms*—Discrete Fourier transform, sampling, Ramanujan's sums, Fuglede's conjecture, convolution, idempotents**

I. Introduction

We say that an N length vector h is a convolution idempotent if $h{*}h = h$, where $*$ denotes discrete circular convolution. We consider the problem of recovering h when some of its entries are known to be zero. This problem has applications to sampling analog signals, and is possibly a useful connection to make progress on the Fuglede conjecture [1]. In this paper, we briefly review the motivations for considering such a problem. We then present some results when N is a product of two primes. This is a followup to our work in [2] where we characterized all possible idempotents with given zero sets, in the case when N is a prime power.

Some preliminary notations and observations before we proceed. We denote by $\mathbb{Z}_N$ the set of integers modulo N, and by $\mathcal{F}_N$ the $N \times N$ Discrete Fourier transform (DFT) matrix (we omit N if it is apparent from the context) [3], [4], so that for any $x \in \mathbb{C}^N$, we have

$$\mathcal{F}x(n) = \sum_{j \in \mathbb{Z}_N} x(j) e^{-2\pi i n j/N}, \text{ for } n \in \mathbb{Z}_N.$$

The discrete (circular) convolution of two signals $x, y \in \mathbb{C}^N$ is

$$(x * y)(n) = \sum_{j \in \mathbb{Z}_N} x(j) y(n-j), \text{ for } n \in \mathbb{Z}_N.$$

Recall that $\mathcal{F}(x * y) = (\mathcal{F}x)(\mathcal{F}y)$, so that for a convolution idempotent h we have $(\mathcal{F}h)^2 = \mathcal{F}h$. Thus the entries of $\mathcal{F}h$ are either 0 or 1, and an idempotent h is equivalently defined by the support of $\mathcal{F}h$. That is, for a (support) set $\mathcal{J} \subseteq \mathbb{Z}_N$, with $1_{\mathcal{J}} \in \mathbb{C}^N$ denoting the indicator of $\mathcal{J}$ the idempotent corresponding to $\mathcal{J}$ is $h_{\mathcal{J}} = \mathcal{F}^{-1} 1_{\mathcal{J}}$.

Just as an idempotent is characterized by its support $\mathcal{J} \subseteq \mathbb{Z}_N$, a foundational result is that the zero set of an idempotent is characterized by a subset of divisors of N (stated as Lemma 1, below). For this, we introduce the following notation: For a vector $h \in \mathbb{C}^N$, let $\mathcal{Z}(h) \subseteq \mathbb{Z}_N$ denote the indices where h vanishes. Let $\mathcal{D}_N$ be the set of all divisors of N in $\mathbb{Z}_N$ (so omitting N), let (i, N) denote the greatest common divisor (gcd) of i and N, and let

$$\mathscr{A}_N(k) = \{i \in \mathbb{Z}_N \colon (i, N) = k\}. \tag{1}$$

Lemma 1: The zero-set $\mathcal{Z}(h)$ is the disjoint union

$$\mathcal{Z}(h) = \{i \in \mathbb{Z}_N \colon (i, N) \in \mathcal{D}(h)\} = \bigcup_{k \in \mathcal{D}(h)} \mathscr{A}_N(k)$$

for some set of divisors $\mathcal{D}(h) \subseteq \mathcal{D}_N$.

We call $\mathcal{D}(h)$ the *zero-set divisors of* h. The lemma appears in many different forms and contexts, see [5], [6], [7] or [8, Theorem 2.1] for example: the key ingredient in the proof is the structure of cyclotomic polynomials.

For example if $N = 8$, $\mathcal{J} = \{0, 1, 4, 5\}$ then $\mathcal{Z}(h_{\mathcal{J}}) = \{1, 3, 4, 5, 7\} = \{1, 3, 5, 7\} \cup \{4\} = \mathscr{A}_8(1) \cup \mathscr{A}_8(4)$; here $\mathcal{D}(h_{\mathcal{J}})$ = {1,4}.

We can ask if a converse of Lemma 1 holds; i.e. given a set $\mathcal{Z}$ of the form in Lemma 1 (i.e. $\mathcal{Z}$ is a union of some $\mathscr{A}_N(k)$), is there an idempotent h whose zero set is Z? We formulate this as :

> *Problem* $\mathfrak{i}_N(\mathcal{D})$: Given a positive integer N and a set of divisors $\mathcal{D} \subseteq \mathcal{D}_N$ let
>
> $$\mathcal{Z} = \{i \in \mathbb{Z}_N \colon (i, N) \in \mathcal{D}\} \tag{2}$$
>
> Find all index sets $\mathcal{J}$ such that the idempotent $h_{\mathcal{J}} = \mathcal{F}^{-1} 1_{\mathcal{J}}$ vanishes on $\mathcal{Z}$.

Note that this is slightly different from a converse of Lemma 1: For $\mathcal{J}$ to be a solution to $\mathfrak{i}(\mathcal{D})$ we only ask if $h_{\mathcal{J}}$ vanishes on $\mathcal{Z}$. In particular, h may vanish outside $\mathcal{Z}$ (i.e. have a bigger zero set) as well.

In our previous work [6], we motivated the zero set problem $\mathfrak{i}(\mathcal{D})$ in the context of sampling. We revisit and summarize this in Section II. In [6], we also gave a complete characterization of all solutions to $\mathfrak{i}(\mathcal{D})$ when $N = p^M$ is a prime power, using base$-p$ expansions of elements of $\mathcal{J}$. In this work, we build a case for solving $\mathfrak{i}(\mathcal{D})$ when N has more than one prime factor, and generalize some of the results of [2]. The main contribution here is to characterize all solutions to $\mathfrak{i}(\mathcal{D})$ when $N = pq$ and $\mathcal{D} = \{1\}, \{p, q\}, \{1, p\}$ or $\{1, q\}$ (Theorem 1, Corollary 1, 2). Theorem 1 seems connected to results on vanishing sums of roots of unity [9], though the techniques we employ are different. The proof of Theorem 1 uses properties of Ramanujan sums [10], which were recently used for signal processing [11], [12]. In section IV we investigate some bounds on the *smallest* solution to $\mathfrak{i}(\mathcal{D})$, and relate it to the minrank [13] of certain graphs introduced in [6].

II. Motivation

A. Sampling

We describe a problem in the traditional multicoset sampling setting [14], [15] in which the zero set problem naturally arises. See [2] for details: here we will give a concise overview of the key ideas.

We are interested in sampling signals that have a *fragmented spectrum*: *i.e.* for any signal f in the space, the Fourier transform $\mathcal{F}f(s)$ is non zero only when the frequency s is in $\cup_{n\in\mathfrak{F}}[n, n+1]$. See Figure 1 for an example of a signal in such a space, with $\mathfrak{F} = \{0, 2\}$.

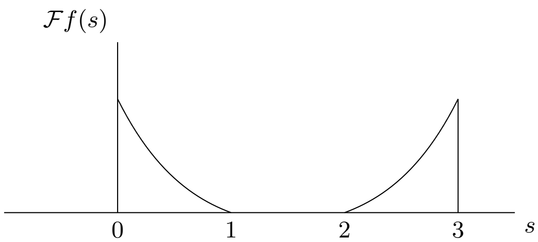

Fig. 1: Example signal with two fragments, for $\mathfrak{F} = \{0, 2\}$.

If we sample the signal from Fig 1 at the Nyquist rate, we need to take at least 3 samples per second. Instead, consider sampling the signal with the sampling pattern shown in Fig 2:

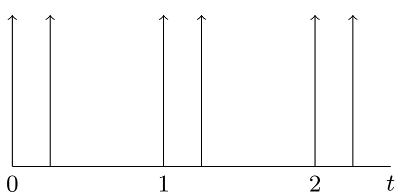

Fig. 2: Example sampling pattern in the case $\mathfrak{F} = \{0, 2\}$. Samples are taken at every second, and at a 0.25 second offset

Note that with the sampling pattern of Figure 2, we take on average 2 samples per second. With elementary Fourier analysis, one can show that the sampled signal has a spectrum shown in Fig 3 (see [2] for details, the main idea is from [14], [15]).

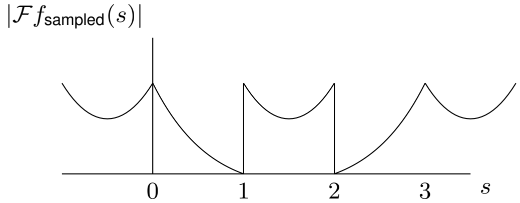

Fig. 3: Spectrum of signal in Fig 1 sampled with the spectrum from Fig 2.

The crucial observation from Fig 3 is that the original signal fragments are intact: aliasing primary occurs in the islands where the signal was non-existent anyway. This idea can be generalized to signal spaces with arbitrary locations of the fragments $\mathfrak{F}$, by picking a sampling pattern of the form

$$p_{\mathcal{J}}(t) = \sum_{m\in\mathcal{J}} \delta(t - m/N), \qquad (3)$$

where $\mathcal{J}$ and N are parameters that need to be picked. For example, for the sampling pattern in Fig 1, we have $N = 4, \mathcal{J} = \{0, 1\}$. Now we let $\mathcal{Z}$ be the difference set of $\mathfrak{F}$, and $\mathcal{D}$ the corresponding gcds, i.e.,

$$\mathcal{Z} = \{k_1 - k_2 : k_1, k_2 \in \mathfrak{F}\},$$
$$\mathcal{D} = \{d : (k, N) = d \text{ for some k} \in \mathfrak{F}.\}$$

We can show ([2, Proposition 2]) that any $\mathcal{J}$ providing a solution to the zero set problem $\mathfrak{i}(\mathcal{D})$ will ensure that the signal can be recovered from the samples taken according to (3). The average sampling rate would then be $|\mathcal{J}|$, which could potentially be much smaller than the Nyquist rate of $\max|\mathcal{Z}|$. Thus finding a feasible sampling pattern for multicoset sampling is closely connected to solving $\mathfrak{i}(\mathcal{D})$.

While the sampling pattern given in this section is motivated from [14] and [15], follow up works for e.g. in [16], [17] build on the techniques described here.

B. Fuglede conjecture

Another motivation is related to a conjecture of Fuglede [1]. We say that a set $\mathcal{J} \subseteq \mathbb{Z}_N$ tiles $\mathbb{Z}_N$ if $\mathcal{J}$ together with its translates forms a disjoint cover of $\mathbb{Z}_N$. More precisely, $\mathcal{J}$ tiles $\mathbb{Z}_N$ if there exists a set $\mathcal{K} \in \mathbb{Z}_N$ (representing the set of translates) such that $\mathcal{J} + \mathcal{K} = \{j + k : j \in \mathcal{J}, k \in \mathcal{K}\} = \mathbb{Z}_N$. We can write this as

$$1_{\mathcal{J}} * 1_{\mathcal{K}} = 1_{\mathbb{Z}_N}, \text{ or } h_{\mathcal{J}} h_{\mathcal{K}} = \delta_N, \qquad (4)$$

where δ_N is the canonical unit vector in $\mathbb{C}^N$ with a 1 in the leading position.

Next, $\mathcal{J} \subseteq \mathbb{Z}_N$ is called a *spectral set* if there exists a square unitary submatrix of $\mathcal{F}$ with columns indexed by $\mathcal{J}$ (when we say "unitary" we mean up to scaling).

A conjecture of Fuglede [1], for $\mathbb{Z}_N$, is:

Conjecture 1: (Spectral iff Tiling) A set $\mathcal{J} \subseteq \mathbb{Z}_N$ is spectral if and only if $\mathcal{J}$ tiles $\mathbb{Z}_N$.

See [6], [7], [18]–[22] for some discussion on this conjecture.

Let us do a straightforward analysis of Conjecture 1: starting with a spectral set $\mathcal{J}$, to prove that $\mathcal{J}$ is a tiling set we need to find the set of translates $\mathcal{K}$ such that (4) holds, thus $h_{\mathcal{K}}$ must vanish on $\mathbb{Z}_N \setminus \{0\}$ wherever $h_{\mathcal{J}}$ does not. In particular, finding a $\mathcal{K}$ is equivalent to solving the zero set problem; and finding such an idempotent – or the inability to find one – would hopefully give insights into the validity of Conjecture 1, at least in the direction spectral $\implies$ tiling.

C. A case for non prime powers

One particular solution of $\mathfrak{i}(\mathcal{D})$ for $N = p^M$ can readily be obtained with elementary means (proof is skipped for brevity). The complete solution space for the prime power case can also be characterized as in [2]. What is the situation when N has more than one prime factor?

In addition to natural interest, such a generalization is also pertinent if we consider the motivating problems introduced in Section II. Take the problem of sampling two- (or higher) dimensional signals with a fragmented spectrum, where each fragment occupies a single cell of an integer lattice. In the notation of Section II

$$\mathcal{F}f(s_1, s_2) = 0 \quad \text{when } (s_1, s_2) \notin \bigcup_{(m,n)\in\mathfrak{F}} [m, m+1] \times [n, n+1].$$

Here $\mathfrak{F} \subseteq \mathbb{Z}_N \times \mathbb{Z}_M$ indicates the locations of the spectral fragments (see Figure 4). An analysis similar to the prime power case leads to *two dimensional* idempotents $h \in \mathbb{C}^{N\times M}$. When N and M are coprime, the entries in h can be re-indexed to an $NM-$ length vector that is an idempotent in $\mathbb{C}^{NM}$. See the Prime Factor algorithm or Good's algorithm ([23], [24]) for details on using the Chinese remainder theorem for the re-indexing. For such scenarios, the idempotent to be reconstructed is associated with more than one prime factor.

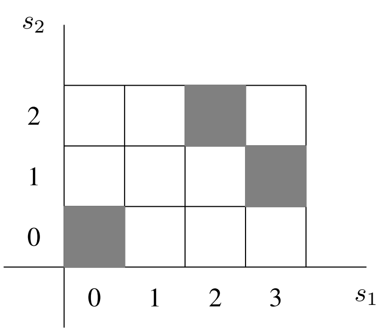

Fig. 4: Example fragmented spectrum of a 2-D signal. The Fourier transform $\mathcal{F}f(s_1, s_2)$ is non zero only in the shaded regions.

As for the sampling scenario, a solution of the zero set problem when N has more than one prime factor is relevant to Fuglede's conjecture as well. Fuglede's conjecture is known to be true when N is a prime power, [21], and the challenge is to make progress when N has more than a single prime factor. See [6], [7] for some attempts to generalize the conjecture for arbitrary N.

However, unlike the prime power case, there may not be any nontrivial solution to $\mathfrak{i}_N(\mathcal{D})$ for an arbitrary N. For example, let $N = 6$ and $\mathcal{Z} = \{2, 3, 4\}$. An exhaustive search shows that there is no idempotent h on $\mathbb{Z}_6$ that vanishes only on $\mathcal{Z}$: in fact the only solution to $\mathfrak{i}(\mathcal{D})$ is $\mathbb{Z}_6$ (the corresponding idempotent is δ, which vanishes on all non zero indices). This can also be verified from Corollary 2.

III. Extension to non prime power case

We note some simple properties of solutions to $\mathfrak{i}(\mathcal{D})$ that we will use later in the proofs.

Lemma 2: With $\mathfrak{i}(\mathcal{D})$ as defined in the Introduction,

1) The set $\mathcal{J} = \mathbb{Z}_N$ is always a solution to $\mathfrak{i}(\mathcal{D})$, for any $\mathcal{D}$.
2) If $\mathcal{J}$ is a solution, so is any translate of $\mathcal{J}$, mod N.
3) If $\mathcal{J}_1$ and $\mathcal{J}_2$ are two disjoint solutions, so is $\mathcal{J}_1 \cup \mathcal{J}_2$.
4) Any solution to $\mathfrak{i}(\mathcal{D})$ is also a solution to $\mathfrak{i}(\mathcal{D}')$ for any $\mathcal{D}' \subseteq \mathcal{D}$.
5) If $\mathcal{J}$ and $\mathcal{J}'$ are solutions with $\mathcal{J}' \supseteq \mathcal{J}$, then $\mathcal{J}' \setminus \mathcal{J}$ is also a solution.

We omit the proof, which uses only the definition and basic properties of the Fourier transform.

Assume, for simplicity, that $N = pq$, so only the two prime factors p and q. Suppose that $1 \in \mathcal{D}$, first observe that any solution h to $\mathfrak{i}(\mathcal{D})$ satisfies

$$h \cdot 1_{\mathscr{A}_N(1)} = 0. \tag{5}$$

Recall that $\mathcal{F}h = 1_{\mathcal{J}}$, and set $c = \mathcal{F}^{-1}1_{\mathscr{A}_N(1)}$. Note that the entries in c are, by definition of the inverse Fourier transform,

$$c(k) = \frac{1}{N} \sum_{\substack{n\in\mathbb{Z}_q \\ (n,N)=1}} \exp(2\pi ink/q)$$

This is Ramanujan's sum; see his original paper [10], for example. As often presented, Ramanujan's sum is

$$\mathfrak{c}_N(k) = \sum_{\substack{n\in\mathbb{Z}_q \\ (n,N)=1}} \cos(2\pi nk/N) = \sum_{\substack{n\in\mathbb{Z}_q \\ (n,N)=1}} \exp(2\pi ink/N), \tag{6}$$

where N and k are positive integers. Ramanujan's sums have also recently been used for signal processing, see [11], [12]. For $k \in [0 : N-1]$, we can also interpret $\mathfrak{c}_N$ as the inverse Fourier transform of the N-length (scaled) indicator

$$\mathbf{1}_N(n) = \begin{cases} N, & \text{if } (n, N) = 1 \\ 0, & \text{otherwise.} \end{cases}$$

We shall need the following two properties:

(i) When $N = p^m$ is a prime power,

$$\mathfrak{c}_{p^m}(k) = \begin{cases} 0 & \text{if } p^{m-1} \nmid k, \\ -p^{m-1} & \text{if } p^{m-1} \mid k \text{ and } p^m \nmid k, \\ \phi(p^m) & \text{if } p^m \mid k, \end{cases} \tag{7}$$

where ϕ is the Euler totient function [25].

(ii) For any divisor d of N,

$$\sum_{\substack{n\in\mathbb{Z}_q \\ (n,N)=d}} \exp(2\pi ink/N) = \mathfrak{c}_{d'}(k).$$

where $d' = N/d$.

We also need the important multiplicative property:

$$\mathfrak{c}_{pq}(n) = \mathfrak{c}_p(n)\mathfrak{c}_q(n), \quad \text{if } p, q \text{ are co-prime.}$$

Then for $N = pq$ we have

$$\mathfrak{c}_N(j) = \mathfrak{c}_{pq}(j) = \begin{cases} -(p-1) \text{ if } j = p, 2p, \ldots, (q-1)p \\ -(q-1) \text{ if } j = q, 2q, \ldots, (p-1)q \\ (p-1)(q-1) \text{ if } j = 0 \\ 1 \text{ otherwise} \end{cases}, \tag{8}$$

for $0 \leq j \leq pq-1$.

Going back to (5) and taking Fourier transforms on both sides of $h \cdot 1_{\mathscr{A}_N(1)} = 0$, we get for any $n \in \mathbb{Z}_N$,

$$\sum_{j \in \mathcal{J}} c(n+j) = 0 \quad \text{or} \quad \sum_{j \in \mathcal{K}} c(j) = 0, \tag{9}$$

for any set $\mathcal{K}$ that is a translate of $\mathcal{J}$.

We can now move to the main result of this section, characterizing the solutions to $\mathfrak{i}_{pq}(\{1\})$:

Theorem 1: Suppose p and q are distinct primes, and let $A_p = \{0, p, 2p, \ldots, (q-1)p\}$ and $A_q = \{0, q, 2q, \ldots, (p-1)q\}$ be subsets of $\mathbb{Z}_{pq}$ containing multiples of p and multiples of q, respectively. Then any solution to $\mathfrak{i}_{pq}(\{1\})$ is either a (disjoint) union of translates of A_p or a (disjoint) union of translates of A_q.

Proof: First, we note that both A_p and A_q are solutions to $\mathfrak{i}(\{1\})$: we can easily verify from the definition of the discrete Fourier transform

$$h_{A_p} = \mathcal{F}^{-1}\underline{1}_{A_p} = \frac{1}{p}\underline{1}_{A_q}, \quad \text{and } h_{A_q} = \mathcal{F}^{-1}\underline{1}_{A_q} = \frac{1}{q}\underline{1}_{A_p},$$

and so both h_{A_p} and h_{A_q} vanish on indices coprime to pq.

Now we prove that any solution to $\mathfrak{i}(\{1\})$ is a disjoint union of translates of either A_p or A_q. Consider any solution $\mathcal{J}$ to $\mathfrak{i}(\{1\})$ in $\mathbb{Z}_{pq}$, and assume, by a suitable translation, that $0 \in \mathcal{J}$. The other elements of $\mathcal{J}$ are either multiples of p, multiples of q, or coprime to pq. Let

$$\alpha = |\mathcal{J} \cap A_p \setminus \{0\}|, \quad \beta = |\mathcal{J} \cap A_q \setminus \{0\}|, \quad \gamma = |\mathcal{J}| - \alpha - \beta - 1.$$

Here α, β are the number of nonzero elements of $\mathcal{J}$ that are multiples of p and q, respectively, and γ is is the number of elements of $\mathcal{J}$ coprime to pq. Then we must have, by (8) and (9) (with $n = 0$)

$$(p-1)(q-1) - \alpha(p-1) - \beta(q-1) + \gamma = 0. \tag{10}$$

Note that $\alpha \leq |A_p \setminus \{0\}| = q-1$, $\beta \leq |A_q \setminus \{0\}| = p-1$, and $\gamma \leq \phi(pq) = (p-1)(q-1)$. We will next argue that either $\alpha = q-1$ or $\beta = p-1$ (i.e. either α or β take their largest possible values); thus establishing that $\mathcal{J}$ contains either A_p or A_q.

If $\alpha = q-1$, then $A_p \subseteq \mathcal{J}$ and we are done. So suppose that $\alpha < q-1$. Then there exists a non zero multiple of p, say ap, such that $ap \notin \mathcal{J}$. Now consider the set $\mathcal{J}' = \tau^{ap}\mathcal{J}$ obtained by translating $\mathcal{J}$ by ap. We first make these simple observations:

1) By construction, $0 \notin \mathcal{J}'$. The element $0 \in \mathcal{J}$ translated by ap results in a non zero multiple of p.
2) Translating non zero multiples of p in $\mathcal{J}$ by ap results in indices that are non zero multiples of p.
3) Translating non zero multiples of q in $\mathcal{J}$ by ap results in indices that are co-prime to pq.
4) Translating indices in $\mathcal{J}$ that are co-prime to pq by ap could potentially result in indices that are multiples of q. Let $\gamma_1 \leq \gamma$ be the number of such indices.

Applying (9) with $n = -ap$, and using (8) results in

$$-(\alpha+1)(p-1) - \gamma_1(q-1) + \beta + (\gamma - \gamma_1) = 0. \tag{11}$$

Subtracting (11) from (10) results in

$$(p-1-\beta+\gamma_1)q = 0 \quad \text{or } p-1+\gamma_1 = \beta.$$

Since $\beta \leq p-1$, the above equality only possible when $\beta = p-1$ and $\gamma_1 = 0$. In particular $\beta = p-1$ implies that $A_q \subseteq \mathcal{J}$. Thus either $A_p \subseteq \mathcal{J}$ or $A_q \subseteq \mathcal{J}$.

Now we argue as follows: isolate either A_p or A_q from $\mathcal{J}$, as in

$$\mathcal{J}_1 = \begin{cases} A_p \text{ if } A_p \subseteq \mathcal{J} \\ A_q \text{ otherwise} \end{cases}$$

We note, as before, that $\mathcal{J} \setminus \mathcal{J}_1$ is a solution to $\mathfrak{i}(\{1\})$. Applying the argument repeatedly, we can write

$$\mathcal{J} = \mathcal{J}_1 \cup \mathcal{J}_2 \cup \mathcal{J}_3 \ldots$$

where each $\mathcal{J}_i$ is a translate of A_p or A_q, and all the $\mathcal{J}_i$ are disjoint. We will argue next that all of the $\mathcal{J}_i$ are translates of *the same set:* either A_p or A_q. Suppose that $\mathcal{J}_1 = \{0, p, 2p, \ldots, (q-1)p\}$ and $\mathcal{J}_k = \{l, l+q, l+2q, \ldots, l+(p-1)q\}$ is a translate of A_q. Then there exists an element of $\mathcal{J}_k$ that is a multiple of p: this is obtained by solving the congruence

$$l + xq \equiv 0 \mod p$$

in x. Thus $\mathcal{J}_1$ and $\mathcal{J}_k$ have a common element, contradicting their disjointedness.

So $\mathcal{J}$ is a disjoint union of translates of A_p, or a disjoint union of translates of A_q, proving the theorem. ∎

Corollary 1: If p and q are distinct primes, any solution to $\mathfrak{i}_{pq}(\{1\})$ is a solution to either $\mathfrak{i}_{pq}(\{1,p\})$ or $\mathfrak{i}_{pq}(\{1,q\})$. In particular, there is no idempotent that vanishes only on $\mathscr{A}_{pq}(1)$.

Proof: Recall that

$$h_{A_p} = \mathcal{F}^{-1}\underline{1}_{A_p} = \frac{1}{p}\underline{1}_{A_q}, \quad \text{and } h_{A_q} = \mathcal{F}^{-1}\underline{1}_{A_q} = \frac{1}{q}\underline{1}_{A_p}.$$

Thus h_{A_p} is nonzero only on multiples of q, i.e. it vanishes on $\mathscr{A}(1) \cup \mathscr{A}(p)$, and so A_p is a solution to $\mathfrak{i}(\{1,p\})$ and (similarly) A_q is a solution to $\mathfrak{i}(\{1,q\})$. From Theorem 1, any solution to $\mathfrak{i}(\{1\})$ is a disjoint union of translates of A_p or A_q. From this and Lemma 2 properties 2) and 3), it follows that any solution to $\mathfrak{i}(\{1\})$ is a solution to either $\mathfrak{i}(\{1,p\})$ or $\mathfrak{i}(\{1,q\})$. ∎

Corollary 2: If p and q are distinct primes, then the only solution to $\mathfrak{i}_{pq}(\{p,q\})$ is $\mathbb{Z}_N$.

Proof: Let $\mathcal{J}$ be a solution to $\mathfrak{i}_{pq}(\{p,q\})$, and $\mathcal{K}$ any solution to $\mathfrak{i}_{pq}(\{1\})$. Then $h_{\mathcal{J}} \cdot h_{\mathcal{K}}$ must vanish at all indices in $\mathbb{Z} \setminus \{0\}$. Note that $h_{\mathcal{J}}(0) = |\mathcal{J}|/N$ and $h_{\mathcal{K}}(0) = |\mathcal{K}|/N$ (here $N = pq$). Then we must have $h_{\mathcal{J}} \cdot h_{\mathcal{K}} = |\mathcal{J}||\mathcal{K}|\delta_{pq}/N^2$. Using that $\mathcal{F}h_{\mathcal{J}} = 1_{\mathcal{J}}$ and $\mathcal{F}h_{\mathcal{K}} = 1_{\mathcal{K}}$, we obtain

$$1_{\mathcal{J}} * 1_{\mathcal{K}} = N\mathcal{F}(h_{\mathcal{J}} \cdot h_{\mathcal{K}}) = \frac{|\mathcal{J}||\mathcal{K}|}{N} 1_{\mathbb{Z}_N}.$$

In particular, since $1_{\mathcal{J}}, 1_{\mathcal{K}}$ are indicators, the convolution $1_{\mathcal{J}} * 1_{\mathcal{K}}$ can only have integer entries; and so we must have that $N = pq$ divides $|\mathcal{J}||\mathcal{K}|$. This must be true for any $\mathcal{K}$ that is solution to $\mathfrak{i}_{pq}(\{1\})$. In particular, we can use $\mathcal{K} = A_p$ or $\mathcal{K} = A_q$ to conclude that $|\mathcal{J}| = pq$, or in other words $\mathcal{J} = \mathbb{Z}_N$. ■

IV. A bound on the smallest solution to $\mathfrak{i}(\mathcal{D})$

Recall from our sampling based motivation for the zero set problem in Section II that the average sampling rate of the multi-coset scheme discussed is $|\mathcal{J}|$, which we would like to keep as small as possible. Naturally, instead of asking for *all* possible idempotents with a given zero set (as in $\mathfrak{i}(\mathcal{D})$) we can ask for the smallest solution to $\mathfrak{i}(\mathcal{D})$. This leads to the definition

$$\Xi(\mathcal{D}) = \arg\min\{|\mathcal{J}| : \mathcal{J} \text{ solves } \mathfrak{i}(\mathcal{D})\}.$$

This quantity, in some sense, characterizes the smallest possible sampling rate achievable by the multicoset scheme.

In this section, we derive some simple bounds on $\Xi(\mathcal{D})$, and look at some connections to difference graphs defined in an earlier work [6]. To define the bound, given a set of divisors $\mathcal{D}$, recall that the corresponding zero set $\mathcal{Z}$ is defined as in (2) by including all indices whose gcd with N is in $\mathcal{D}$. In the (inverse) DFT matrix, suppose we remove all rows except those with indices in $\mathcal{Z} \cup \{0\}$, to obtain the matrix $\mathcal{F}^{-1}_{\mathcal{Z}\cup\{0\}}$.

Note that if $\mathcal{J}$ is a solution to $\mathfrak{i}(\mathcal{D})$, then $\mathcal{F}^{-1}1_{\mathcal{J}}$ vanishes on $\mathcal{Z}$ by definition. In addition, we also have $\mathcal{F}^{-1}1_{\mathcal{J}}(0) = |\mathcal{J}|/N \neq 0$, so that we may say

$$\mathcal{F}^{-1}_{\mathcal{Z}\cup\{0\}}\left(1_{\mathcal{J}}N/|\mathcal{J}|\right) = \delta,$$

where, as usual, δ is standard unit vector with 1 in the topmost position. Now we construct a lower-bound to $\Xi(\mathcal{D})$ by replacing $1_{\mathcal{J}}N/|\mathcal{J}|$ with x in the above equation:

$$\xi(\mathcal{D}) = \min_{x\in\mathbb{C}^N}\{\|x\|_0 : \mathcal{F}^{-1}_{\mathcal{Z}\cup\{0\}}x = \delta\},$$

where $\|x\|_0$ is the number of non zero entries in x. The above formulation asks us to find the sparsest solution to a system of linear equations, for which we can potentially apply standard algorithms like Orthogonal Matching Pursuit or Basis Pursuit [26]–[28]. By construction, we have

$$\xi(\mathcal{D}) \leq \Xi(\mathcal{D}). \tag{12}$$

A. Difference graphs

Given a divisor set $\mathcal{D}$ and the corresponding zero set $\mathcal{Z}$ we can define a graph $\mathscr{G}(\mathcal{D})$ with vertex set $\mathbb{Z}_N$ and edge between i, j if $(i-j, N) \in \mathcal{Z}$. Such graphs were investigated in our prior work [6], in the context of sampling discrete signals. We explore some connections of the bound $\xi(\mathcal{D})$ to certain graph invariants.

We say that a matrix M fits a graph G if the diagonal entries of M are 1, and ij entry M_{ij} is zero if i, j are not adjacent in G. Recall that the minrank of a graph (over $\mathbb{C}$)) is the smallest possible rank among all complex matrices that fit G [13], [29], [30].

Start with a divisor set $\mathcal{D}$ and the corresponding zero set $\mathcal{Z}$. Let $x \in \mathbb{C}^N$ satisfy $\mathcal{F}^{-1}_{\mathcal{Z}\cup\{0\}}x = \delta$. Construct an $N \times N$ circulant matrix [31] M with first column $\mathcal{F}^{-1}x$. Note that the eigen values of M are the entries of x, and consequently the rank of M is $\|x\|_0$. Also note that the diagonal entries of M are 1, and the ij entry is zero if $i - j \in \mathcal{Z}$. Thus M fits $\mathscr{G}^c(\mathcal{D})$, and so

$$\text{minrank}(\mathscr{G}^c(\mathcal{D})) \leq \xi(\mathcal{D}).$$

The bound $\xi(\mathcal{D})$ is similar to minimum circulant rank defined in [32]. We can infact prove that the bound in (12) is tight, suprisingly in the case when $\mathcal{J}$ is spectral.

Lemma 3: Suppose $\mathcal{J}$ is spectral, and $h = \mathcal{F}^{-1}1_{\mathcal{J}}$, as before. Then the bound in (12) is tight, i.e. $\xi(\mathcal{D}(h)) = \Xi(\mathcal{D}(h))$.

Proof: From [6, Lemma 3], if $\mathcal{J}$ is spectral then there exists an independent set in $\mathscr{G}^c(\mathcal{D})$ of size $|\mathcal{J}|$. Since minrank is an upper bound on the independence number [13], it follows that $|\mathcal{J}| \leq \text{minrank}(\mathscr{G}^c(\mathcal{D}))$. Combining with (12) we have that

$$|\mathcal{J}| \leq \text{minrank}(\mathscr{G}^c(\mathcal{D})) \leq \xi(\mathcal{D}) \leq \Xi(\mathcal{D}) \leq |\mathcal{J}|,$$

and so all the inequalities involved are tight. ■

Another lower bound can be defined using Linear programs [7, Section IV.B]. Note that this bound is non integral, unlike the bound ξ given in this section.

V. Conclusion

We introduced the zero set problem for convolution idempotents, briefly reviewed the motivations, and presented some results when the ambient dimension is a product of two primes. The connection to results on vanishing sums of roots of unity [9] and tiling [21] need to be explored further. We also gave some bounds on the smallest solution to the zero set problem and explored its connection to minrank of certain graphs defined on $\mathbb{Z}_N$. Of interest is to investigate generalizations to arbitrary N. Of particular interest is to understand the solution space of $\mathfrak{i}(\mathcal{D})$ when $\mathcal{D}$ corresponds to spectral or tiling sets [21], the conditions under which the bound $\Xi(\mathcal{D})$ can be efficiently computed, and provable algorithms to solve (or approximate) the solutions to $\mathfrak{i}(\mathcal{D})$.

References

[1] B. Fuglede, "Commuting self-adjoint partial differential operators and a group theoretic problem," *Journal of Functional Analysis*, vol. 16, no. 1, pp. 101–121, 1974.

[2] A. Siripuram and B. Osgood, "Convolution idempotents with a given zero-set," 2020.

[3] A. V. Oppenheim, *Discrete-time signal processing*. Pearson Education India, 1999.

[4] B. Osgood, *Lectures on the Fourier Transform and Its Applications*. American Mathematical Society, 2018.

[5] W. Wu, "Discrete sampling: Generalizations of the Nyquist-Shannon sampling theorem," Ph.D. dissertation, Stanford University, 2010.

[6] A. Siripuram, W. Wu, and B. Osgood, "Discrete sampling: A graph theoretic approach to orthogonal interpolation," *IEEE Transactions on Information Theory*, 2019.

[7] A. Siripuram and B. Osgood, "Lp relaxations and fuglede's conjecture," in *2018 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2018, pp. 2525–2529.

[8] R.-D. Malikiosis and M. N. Kolountzakis, "Fuglede's conjecture on cyclic groups of order $p^n q$," *arXiv preprint arXiv:1612.01328*, 2016.

[9] T. Lam and K. Leung, "On vanishing sums of roots of unity," *Journal of algebra*, vol. 224, no. 1, pp. 91–109, 2000.

[10] S. Ramanujan, “On certain trigonometrical sums and their applications in the theory of numbers,” *Trans. Cambridge Philos. Soc*, vol. 22, no. 13, pp. 259–276, 1918.

[11] P. Vaidyanathan, “Ramanujan sums in the context of signal processing—part i: Fundamentals,” *IEEE transactions on signal processing*, vol. 62, no. 16, pp. 4145–4157, 2014.

[12] ——, “Ramanujan sums in the context of signal processing—part ii: FIR representations and applications,” *IEEE Transactions on Signal Processing*, vol. 62, no. 16, pp. 4158–4172, 2014.

[13] W. Haemers *et al.*, “An upper bound for the shannon capacity of a graph,” in *Colloq. Math. Soc. János Bolyai*, vol. 25, 1978, pp. 267–272.

[14] A. Kohlenberg, “Exact interpolation of band-limited functions,” *Journal of Applied Physics*, vol. 24, no. 12, pp. 1432–1436, 1953.

[15] Y.-P. Lin and P. Vaidyanathan, “Periodically nonuniform sampling of bandpass signals,” *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 45, no. 3, pp. 340–351, 1998.

[16] C. Herley and P. W. Wong, “Minimum rate sampling and reconstruction of signals with arbitrary frequency support,” *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1555–1564, 1999.

[17] R. Venkataramani and Y. Bresler, “Perfect reconstruction formulas and bounds on aliasing error in sub-nyquist nonuniform sampling of multiband signals,” *IEEE Transactions on Information Theory*, vol. 46, no. 6, pp. 2173–2183, 2000.

[18] A. Iosevich, N. Katz, and T. Tao, “The Fuglede spectral conjecture holds for convex planar domains,” *Mathematical Research Letters*, vol. 10, no. 5, pp. 559–569, 2003.

[19] I. Laba, “The spectral set conjecture and multiplicative properties of roots of polynomials,” *Journal of the London Mathematical Society*, vol. 65, no. 03, pp. 661–671, 2002.

[20] T. Tao, “Fuglede’s conjecture is false in 5 and higher dimensions,” *arXiv preprint math/0306134*, 2003.

[21] E. M. Coven and A. Meyerowitz, “Tiling the integers with translates of one finite set,” *Journal of Algebra*, vol. 212, no. 1, pp. 161–174, 1999.

[22] D. E. Dutkay and C.-K. LAI, “Some reductions of the spectral set conjecture to integers,” in *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 156, no. 01. Cambridge Univ Press, 2014, pp. 123–135.

[23] I. J. Good, “The interaction algorithm and practical fourier analysis,” *Journal of the Royal Statistical Society. Series B (Methodological)*, pp. 361–372, 1958.

[24] P. Duhamel and M. Vetterli, “Fast fourier transforms: a tutorial review and a state of the art,” *Signal processing*, vol. 19, no. 4, pp. 259–299, 1990.

[25] R. L. Graham, D. E. Knuth, O. Patashnik, and S. Liu, “Concrete mathematics: a foundation for computer science,” *Computers in Physics*, vol. 3, no. 5, pp. 106–107, 1989.

[26] T. T. Cai and L. Wang, “Orthogonal matching pursuit for sparse signal recovery with noise.” Institute of Electrical and Electronics Engineers, 2011.

[27] M. Elad, *Sparse and redundant representations: from theory to applications in signal and image processing*. Springer Science & Business Media, 2010.

[28] E. J. Candès and M. B. Wakin, “An introduction to compressive sampling [a sensing/sampling paradigm that goes against the common knowledge in data acquisition],” *IEEE signal processing magazine*, vol. 25, no. 2, pp. 21–30, 2008.

[29] A. Blasiak, R. Kleinberg, and E. Lubetzky, “Broadcasting with side information: Bounding and approximating the broadcast rate,” *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 5811–5823, 2013.

[30] B. Bukh and C. Cox, “On a fractional version of haemers’ bound,” *IEEE Transactions on Information Theory*, vol. 65, no. 6, pp. 3340–3348, 2018.

[31] P. J. Davis, *Circulant matrices*. American Mathematical Soc., 2013.

[32] L. Deaett and S. A. Meyer, “The minimum rank problem for circulants,” *Linear Algebra and its Applications*, vol. 491, pp. 386–418, 2016.