

Characterization of the Divisibility of DFT HTFs for \mathbb{C}^2

Justin Park*

Massachusetts Institute of Technology, Cambridge, MA 02139

Adviser: Dr. Kasso Okoudjou†

Department of Mathematics, University of Maryland, College Park, MD 20742

September 2019

Abstract

We expand on a prior result about the cardinalities of harmonic tight frames generated from the discrete Fourier transform. Harmonic finite unit-norm tight frames (FUNTFs) constructed from the first two rows of the $M \times M$ discrete Fourier transform have previously been described and characterized as prime or divisible, where $M \geq 2$ is an integer. We generalize the result to any choice of two rows b and c for which $c - b$ has up to two distinct prime factors. These new results allow for much more flexibility in constructing harmonic FUNTFs from M -th roots of unity.

1 Introduction

The discrete Fourier transform matrix (DFT) provides a simple construction for a class of frames known as harmonic finite unit-norm tight frames, or FUNTFs. In particular, by sampling and renormalizing any N rows of the $M \times M$ DFT matrix, a harmonic FUNTF for \mathbb{C}^N with M frame vectors is obtained. In this paper, we explore the concept of *divisibility* of such frames.

In [2], the concepts of *prime* and *divisible* tight frames are introduced. A tight frame for \mathbb{C}^N with M frame vectors is (M, n) -*divisible* if some subset with n frame vectors is a tight frame itself. If no such *divisor frame* exists, then the original frame is said to be prime. In addition to defining and characterizing prime tight frames, the authors analyze the divisibility of the harmonic tight frame (HTF) obtained by sampling the first N rows of the $M \times M$ DFT. Define:

$$\begin{aligned} D_{M,N} &= \{d \in \{N, \dots, M - N\} : d \text{ is a divisor of } M\} \\ P_{M,N} &= D_{M,N} \setminus \{d \in D_{M,N} : \exists c \in D_{M,N} \text{ such that } c \text{ is a proper divisor of } d\}, \text{ and} \\ S_{M,N} &= \left\{ s \in \{N, \dots, M - N\} : s = \sum_{k=1}^K a_k q_k \text{ and } M - s = \sum_{k=1}^K b_k q_k, \text{ where } a_k, b_k \in \mathbb{N}_0, q_k \in P_{M,N} \right\}. \end{aligned}$$

(Here, \mathbb{N}_0 refers to the set of non-negative integers. \mathbb{N} will be used to denote the set of positive integers.) It is shown in the same paper that $P_{M,N}$ is exactly the set of cardinalities of prime factors of the HTF, and $S_{M,N}$ is exactly the set of cardinalities of all divisors regardless of primality.

We wish to extend this result to the choice of any N rows, not just rows 0 through $N - 1$ (here, we will refer to the topmost row—the row of all ones—as row 0, and label the remaining rows sequentially up to $M - 1$). That is, consider a frame Φ obtained by sampling any N rows of the DFT. For this frame, which is itself a HTF, we seek to find an explicit construction of the set T_Φ of cardinalities of all its divisors. Note that $T_\Phi = S_{M,N}$ when Φ is sampled from the first N rows of the DFT.

Two distinct questions motivated this search:

*email: jpark00@mit.edu

†email: kasso@math.umd.edu

- For a given choice of Φ constructed from some N rows of the DFT, which elements of $S_{M,N}$ are in T_Φ ? It is simple to verify that, for example, not every T_Φ contains all elements of $S_{M,2}$.
- For a given M, N , does there exist some choice of Φ for which T_Φ contains elements not in $S_{M,N}$?

In the case where the first two rows are chosen, finding T_Φ is equivalent to finding vanishing sums of distinct M -th roots of unity, i.e. a set of distinct M -th root of unity that sums to 0. This problem has been solved in [3]. And if rows 0 and j are chosen, where j is relatively prime to M , the solution set T_Φ is exactly the same as for rows 0 and 1, since row j of the DFT is simply a permutation of row 1. However, if j is not relatively prime to M , the problem becomes significantly harder because row j is no longer a permutation of row 1 and contains repeated roots of unity.

A naïve approach to this more general problem would be to use [1, Theorem 5.2], which gives all possible n for which n M -th roots of unity can sum to 0, allowing for repetition. However, in the case of finding T_Φ , there is a hard restriction on the number of times a root can be repeated. As an example, consider $M = 6$ and $j = 2$. The j -th row of the $M \times M$ DFT has all of the cube roots of unity, repeated twice.

A second approach would be to split any vanishing sum of roots of unity, possibly including repetition, into one or more vanishing sums without repetition. Thus, it would be helpful if any *minimal* vanishing sum—that is, one which cannot be split into two or more vanishing sums—contains no repetitions. However, this turns out to not be true in general, as shown by [4, Theorem 1.1].

The result in [1] mentioned above provides a necessary but insufficient condition for an element to be in T_Φ . For the cases where $m = \frac{M}{j}$ has one or two distinct prime factors, we establish a necessary and sufficient condition in order to fully characterize T_Φ .

2 Main Results

For the purposes of our analysis, let $M \geq 2$ be an integer and let $m \neq 1$ be a divisor of M . Clearly, the values of $(m, \frac{M}{m})$ take on every pair of divisors of M other than $(1, M)$.

One way to determine if a frame for \mathbb{C}^2 is a tight frame is to take the inner product between its two rows when written as a matrix. Specifically, if we have a frame

$$\left\{ \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}, \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}, \dots, \begin{bmatrix} x_k \\ y_k \end{bmatrix} \right\},$$

then the frame is tight exactly when $\langle (x_1, x_2, \dots, x_k), (y_1, y_2, \dots, y_k) \rangle = 0$. This is what we mean by taking the inner product between the rows of a frame. It follows that when sampling from the $M \times M$ DFT matrix, we only have to consider the HTFs obtained by sampling rows 0 and a since, for our purposes, this is equivalent to sampling rows b and $a + b$.

Note that row $\frac{M}{m}$ is of the form $[1, \omega^{M/m}, \omega^{2M/m}, \dots, \omega^{(M-1)M/m}]$, where $\omega = e^{2\pi i/M}$. The order of $\omega^{M/m}$ in the multiplicative group of M -th roots of unity is m . This also means that $\omega^{M/m}$ is a primitive m -th root of unity. So, row $\frac{M}{m}$ contains all of the m -th roots of unity, each repeated exactly $\frac{M}{m}$ times.

Denote by Φ_j the HTF obtained by sampling rows 0 and j from the DFT matrix. Let q be any positive integer relatively prime to m such that $q < m$. Over all possible m and q , the value of $\frac{qM}{m}$ takes on every positive integer less than M , so every possible HTF for \mathbb{C}^2 sampled from the DFT is accounted for by $\Phi_{qM/m}$. Since q is relatively prime to m , $\omega^{qM/m}$ is also a primitive m -th root of unity, from which it follows that row $\frac{qM}{m}$ of the DFT is simply a permutation of row $\frac{M}{m}$. Thus, we only need to look at the HTFs $\Phi_{M/m}$, where m is a divisor of M other than 1.

Let $\tilde{\Phi}_{M/m}$ be a subset of $\Phi_{M/m}$ with n vectors, $1 \leq n < M$. Then T_Φ is the set of all n for which some $\tilde{\Phi}_{M/m}$ is a tight frame. In order for $\tilde{\Phi}_{M/m}$ to be a tight frame, the inner product between the rows of this frame when written as a matrix must be 0. Since the first row of $\tilde{\Phi}_{M/m}$ is all ones, this condition for T_Φ reduces to finding all n for which there exists a vanishing sum of n m -th roots of unity, given the condition that no term may be repeated more than $\frac{M}{m}$ times.

However, we can also impose a second condition. Because the m -th roots of unity sum to 0, there exists a vanishing sum of n m -th roots of unity with multiplicity no greater than $\frac{M}{m}$ if and only if there exists such a sum with $M - n$ roots. Stated in terms of the HTF, $\Phi_{M/m}$ is (M, n) -divisible if and only if it is $(M, M - n)$ -divisible. With the observation that $P_{M,2}$ is the set of prime factors of M , [1, Theorem 5.2] allows us to conclude that $T_{\Phi_{M/m}} \subseteq S_{M,2}$ for any choice of m .

We will approach the problem of finding T_Φ based on the number of distinct prime factors of m . This is tied closely to the prime factors of M , since a prime p divides m only if it divides M as well. We analyze the cases where m has one or two distinct prime factors.

2.1 One prime factor

Assume m has exactly one distinct prime factor p . Then $m = p^\alpha$ for some $\alpha \geq 1$. From [1, Theorem 3.3], the only possible minimal vanishing sum of m -th roots of unity (up to rotation) is the sum of all p -th roots of unity. Therefore, any vanishing sum of m -th roots of unity must contain cp roots of unity for some $c \in \mathbb{N}$.

Is this condition sufficient for our problem? That is, can a divisor frame $\tilde{\Phi}_{M/m}$ with $n = cp$ vectors be found for any choice of c ? The answer is yes, as long as $n < M$.

Theorem 1. *Let m and M be positive integers for which $m \mid M$. If m has exactly one distinct prime factor p , and Φ is the HTF obtained by sampling rows 0 and $\frac{M}{m}$ from the $M \times M$ DFT matrix, then*

$$T_\Phi = \{n = cp : c \in \mathbb{N}, n < M\}. \quad (1)$$

Proof. Consider the structure of row $\frac{M}{m}$ of the DFT. It contains $\frac{M}{m}$ cycles of the m -th roots of unity. It is possible to fit anywhere from 0 to $r = \frac{m}{p}$ minimal vanishing sums in each cycle, simply by rotation. This result follows from [3, Theorem 2], but here we present a more specific proof that illuminates the structure of the vanishing sum and thus of the divisor frame.

Let $\zeta = e^{2\pi i/m}$. Then one cycle in row $\frac{M}{m}$ contains the elements $\{1, \zeta, \zeta^2, \dots, \zeta^{m-1}\}$, which can be decomposed into the disjoint subsets

$$\bigcup_{k=0}^{r-1} \left\{ \zeta^k, \zeta^{k+r}, \zeta^{k+2r}, \dots, \zeta^{k+(p-1)r} \right\}.$$

Each of these subsets is a minimal vanishing sum of m -th roots of unity, so each cycle contains $r = \frac{m}{p}$ disjoint vanishing sums. It follows that, for any positive multiple of p less than or equal to M , there exists a subset of row $\frac{M}{m}$ with that many elements that forms a vanishing sum. Then a divisor frame with n vectors can be found if n is a multiple of p less than M .

Therefore,

$$T_\Phi = \{n = cp : c \in \mathbb{N}, n < M\}.$$

□

From this, we immediately have the following result as well.

Corollary. *If M has exactly one distinct prime factor p and Φ is the HTF obtained by sampling any two rows of the $M \times M$ DFT matrix, then*

$$T_\Phi = \{n = cp : c \in \mathbb{N}, n < M\}. \quad (2)$$

Proof. As noted earlier, we reduced this problem to only searching $\Phi_{M/m}$ where m is a divisor of M other than 1. Since M has only one distinct prime factor p , we see that m only has p as a prime factor as well. Then we may apply the previous theorem. □

2.2 Two prime factors

Assume m has exactly two distinct prime factors p_1 and p_2 . Then $m = p_1^{\alpha_1} p_2^{\alpha_2}$ for some $\alpha_1, \alpha_2 \geq 1$. From [1, Theorem 3.3], the only possible minimal vanishing sums of m -th roots of unity (up to rotation) are the sum of all p_1 -th roots of unity and the sum of all p_2 -th roots of unity. Therefore, any vanishing sum of m -th roots of unity must contain $c_1 p_1 + c_2 p_2$ roots of unity for some $c_1, c_2 \in \mathbb{N}_0$.

As in the case of one prime factor, we ask: is this condition sufficient? That is, can a divisor frame $\tilde{\Phi}_{M/m}$ with $n = c_1 p_1 + c_2 p_2$ vectors be found for any choice of c_1 and c_2 ? In general, the answer is no. However, we will now identify a more specific criterion that tells us for exactly which values of n a divisor frame exists.

Theorem 2. *Let m and M be positive integers for which $m \mid M$. If m has exactly two distinct prime factors p_1 and p_2 , and Φ is the HTF obtained by sampling rows 0 and $\frac{M}{m}$ from the $M \times M$ DFT matrix, then*

$$T_\Phi = \{n : 0 < n < M \text{ and } n, M - n \in \mathbb{N}_0 p_1 + \mathbb{N}_0 p_2\}. \quad (3)$$

Proof. Let $\zeta = e^{2\pi i/m}$ and $r = \frac{m}{p_1 p_2}$. As in the case of one prime factor, one cycle in row $\frac{M}{m}$ contains the elements $\{1, \zeta, \zeta^2, \dots, \zeta^{m-1}\}$, which can be decomposed into the disjoint subsets

$$\bigcup_{k=0}^{r-1} \left\{ \zeta^k, \zeta^{k+r}, \zeta^{k+2r}, \dots, \zeta^{k+(p_1 p_2 - 1)r} \right\}.$$

Each of these subsets is a vanishing sum of m -th roots of unity, so each cycle contains $r = \frac{m}{p_1 p_2}$ disjoint vanishing sums. Therefore, the entirety of row $\frac{M}{m}$ can be split into $rM/m = \frac{M}{p_1 p_2}$ disjoint subsets, each of which is equivalent to $\left\{1, \zeta^r, \zeta^{2r}, \dots, \zeta^{(p_1 p_2 - 1)r}\right\}$ up to rotation. We observe that each of these subsets are the $p_1 p_2$ -th roots of unity (up to rotation), and we refer to these subsets as the *minimal subsets* of row $\frac{M}{m}$.

Additionally, note that each minimal subset also contains minimal vanishing sums with p_1 terms and p_2 terms. In fact, following a similar procedure as in Section 2.1, we can show that each minimal subset contains p_2 minimal vanishing sums with p_1 terms and p_1 minimal vanishing sums with p_2 terms.

Starting with $n = c_1 p_1 + c_2 p_2$ (which must be true in order for a divisor frame to exist), Euclidean division performed twice allows us to write n as $a_1 p_1 + a_2 p_2 + a_3 p_1 p_2$ for non-negative integers a_1, a_2, a_3 with $a_1 < p_2$ and $a_2 < p_1$. Let $b = a_1 p_1 + a_2 p_2$. We claim that there exists a subset of row $\frac{M}{m}$ with n elements that forms a vanishing sum if and only if at least one of the following conditions is true:

- $a_3 < \frac{M}{p_1 p_2} - 1$
- $p_1 p_2 - b \in \mathbb{N}_0 p_1 + \mathbb{N}_0 p_2$.

First, we show that if $a_3 < \frac{M}{p_1 p_2} - 1$ or $p_1 p_2 - b \in \mathbb{N}_0 p_1 + \mathbb{N}_0 p_2$, then there exists a subset of row $\frac{M}{m}$ with n elements that forms a vanishing sum. If $a_3 < \frac{M}{p_1 p_2} - 1$, we can construct a subset as follows. Combine all of the elements from any a_3 of the minimal subsets, which leaves at least two remaining minimal subsets. Add to this set the elements from a_1 of the minimal sums with p_1 terms in one of the remaining minimal subsets, as well as the elements from a_2 of the minimal sums with p_2 terms in one of the other remaining minimal subsets. This combined set is a subset of row $\frac{M}{m}$ and has n elements that sum to 0, as desired.

Now, assume $a_3 = \frac{M}{p_1 p_2} - 1$ and $p_1 p_2 - b \in \mathbb{N}_0 p_1 + \mathbb{N}_0 p_2$ (note that a_3 cannot be any greater, or else n would be at least as large as M). We begin the construction as in the previous case, combining all of the elements from a_3 of the minimal subsets, which leaves one remaining minimal subset. By definition, $b \in \mathbb{N}_0 p_1 + \mathbb{N}_0 p_2$, and we assumed that $p_1 p_2 - b \in \mathbb{N}_0 p_1 + \mathbb{N}_0 p_2$. So by [3, Theorem 2], a vanishing sum with b distinct $p_1 p_2$ -th roots of unity exists. These roots (or some rotation) must be contained in the remaining minimal subset because, as observed earlier, each minimal subset comprises the $p_1 p_2$ -th roots of unity up to rotation. Thus, we may add these elements to our set and end up with a subset of row $\frac{M}{m}$ with n elements that sum to 0, as desired.

Next, we prove the inverse statement, namely that if $a_3 = \frac{M}{p_1 p_2} - 1$ and $p_1 p_2 - b \notin \mathbb{N}_0 p_1 + \mathbb{N}_0 p_2$ then there does not exist a subset of row $\frac{M}{m}$ with n elements that forms a vanishing sum. We have that $M - n = M - b - a_3 p_1 p_2 = p_1 p_2 - b$, but since this is not in $\mathbb{N}_0 p_1 + \mathbb{N}_0 p_2$, [1, Theorem 5.2] tells us that no vanishing sum of $M - n$ roots of unity exists. Therefore, no subset of row $\frac{M}{m}$ with $M - n$ elements can form a vanishing sum, so no subset of row $\frac{M}{m}$ with n elements forms a vanishing sum.

Having checked both directions of the bi-conditional, we have proven the claim. However, it is actually possible to combine the two conditions into one. Note that if $a_3 < \frac{M}{p_1 p_2} - 1$, then $M - n = M - a_1 p_1 - a_2 p_2 - a_3 p_1 p_2 = M - (p_2 - a_1) p_1 - (p_1 - a_2) p_2 - (a_3 + 2) p_1 p_2$, so $M - n \in \mathbb{N}_0 p_1 + \mathbb{N}_0 p_2$. But if $a_3 = \frac{M}{p_1 p_2} - 1$, then $M - n = M - b - a_3 p_1 p_2 = p_1 p_2 - b$, so $M - n \in \mathbb{N}_0 p_1 + \mathbb{N}_0 p_2$ if and only if $p_1 p_2 - b \in \mathbb{N}_0 p_1 + \mathbb{N}_0 p_2$. Therefore, $M - n \in \mathbb{N}_0 p_1 + \mathbb{N}_0 p_2$ if and only if at least one of the conditions is true, so

$$T_\Phi = \{n : 0 < n < M \text{ and } n, M - n \in \mathbb{N}_0 p_1 + \mathbb{N}_0 p_2\}.$$

□

3 Conclusions and Future Research

For the HTF Φ sampled from rows 0 and $\frac{M}{m}$ of the $M \times M$ DFT matrix, we have established the following results through our two main theorems. In the case where m has only one distinct prime factor p , we prove in Section 2.1 that

$$T_\Phi = \{n = cp : c \in \mathbb{N}, n < M\}.$$

Similarly, when m has only two distinct prime factors p_1 and p_2 , we prove in Section 2.2 that

$$T_\Phi = \{n : 0 < n < M \text{ and } n, M - n \in \mathbb{N}_0 p_1 + \mathbb{N}_0 p_2\}.$$

The immediate next question is how to generalize these results to any number of distinct prime factors of m . It is worth noting that, in both the one prime and two prime cases, the set T_Φ is exactly the same as the set of positive integers n for which there exists a vanishing sum of n distinct m -th roots of unity,

which is given in [3]. One may conjecture that this will be the case regardless of the number of prime factors of m , although this seems unlikely in light of the asymmetrical minimal vanishing sums that arise with three or more distinct prime factors (see [1, Section 6]). The ultimate goal would be to characterize the set T_{Φ} for all M and choice of N rows.

References

- [1] T. Y. Lam and K. H. Leung. “On vanishing sums of roots of unity”. In: *Journal of Algebra* 224 (1 Feb. 2000), pp. 91–109. DOI: <https://doi.org/10.1006/jabr.1999.8089>.
- [2] J. Lemvig, C. Miller, and K. Okoudjou. “Prime tight frames”. In: *Advances in Computational Mathematics* 40 (2 Apr. 2014), pp. 315–334. DOI: <https://doi.org/10.1007/s10444-013-9309-0>.
- [3] G. Sivek. “On vanishing sums of distinct roots of unity”. In: *Integers* 10 (3 July 2010), pp. 365–368. DOI: <https://doi.org/10.1515/integ.2010.031>.
- [4] J. P. Steinberger. “Minimal vanishing sums of roots of unity with large coefficients”. In: *Proceedings of the London Mathematical Society* 97 (3 Nov. 2008), pp. 689–717. DOI: <https://doi.org/10.1112/plms/pdn006>.