# Interpolatory Tight Wavelet Frames with Prime Dilation

Youngmi Hur<sup>a,1</sup>, Zachary Lubberts<sup>b</sup>

<sup>a</sup>Department of Mathematics, Yonsei University, Seoul 03722, Korea. <sup>b</sup>Department of Applied Mathematics and Statistics, Johns Hopkins University, Baltimore, MD 21218, USA.

## Abstract

We introduce the prime coset sum method for constructing tight wavelet frames, which allows one to construct nonseparable multivariate tight wavelet frames with prime dilation, using a univariate lowpass mask with this same prime dilation as input. This method relies on the idea of finding a sum of hermitian squares representation for a nonnegative trigonometric polynomial related to the sub-QMF condition for the lowpass mask. We prove the existence of these representations under some conditions on the input lowpass mask, utilizing the special structure of the recently introduced prime coset sum method, which is used to generate the lowpass masks in our construction. We also prove guarantees on the vanishing moments of the wavelets arising from this method, some of which hold more generally.

*Keywords:* Prime coset sum method, wavelets, tight wavelet frames, sum of hermitian squares, interpolatory property 2000 MSC: 42C40, 42C15

## 1. Introduction

The construction of wavelets with special properties has been an active area of research for decades, with the more recent focus being on nonseparable multidimensional wavelets, i.e., those which are not the tensor product of univariate wavelets, and are therefore able to capture multidimensional structures more effectively. Unfortunately, the setting of orthonormal wavelet systems, while theoretically appealing, is quite restrictive, and forces the prospective wavelet filter bank designer in most cases to choose between a biorthogonal wavelet system, wherein the analysis and synthesis operators use different bases, and a tight wavelet frame, where the linear independence of the system is traded

*Email addresses:* yhur@yonsei.ac.kr (Youngmi Hur), zlubber1@jhu.edu (Zachary Lubberts)

 $<sup>^1{\</sup>rm This}$  research was supported in part by the National Research Foundation of Korea (NRF) [Grant Number 20151009350].

in favor of retaining the symmetry between analysis and synthesis. A particularly successful approach on this end is that of the Unitary Extension Principle (UEP) [5, 7, 12], which provides a set of conditions on a collection of trigonometric polynomials which ensure that the wavelet system generated from these is a tight frame for  $L^2(\mathbb{R}^n)$ . In what can perhaps be thought of as an analogous relaxation of the Quadrature Mirror Filter (QMF) condition, which is necessary for wavelets to form an orthonormal system, recent work [2, 3, 11] has shown that when a lowpass mask satisfies the sub-QMF condition, and the gap in the equality may be written as a sum of hermitian squares (sos) of trigonometric polynomials, then there is a related collection of highpass masks which satisfy the UEP conditions, and therefore form a tight wavelet frame for  $L^2(\mathbb{R}^n)$  with this same lowpass mask (see Section 2.3). We refer to this method as the Sum of Hermitian Squares Representation Method for Tight Wavelet Frames (SOSTF).

In [11], some discussion and work was done to address one undesirable aspect of the above construction, which often fails to have vanishing moments for all of the wavelet masks equal to the accuracy number of the lowpass mask, or in other words, fails to have maximum vanishing moments. In this paper, we show that additional study of SOSTF gives a nontrivial lower bound on the number of vanishing moments of the generated highpass masks, which is particularly strong in the case that the lowpass mask is interpolatory (see Section 2.4).

While the work in [2] extends SOSTF to the case of arbitrary dilation, the approach presented there requires finding sos representations for even more complicated trigonometric polynomials, and the approximation of the smoothness, vanishing moments, and other wavelet desiderata is similarly complicated. As such, it may be difficult to know where to begin if one wishes to construct a nonseparable multivariate tight wavelet frame with certain properties outside the setting of dyadic dilation. The Prime Coset Sum Method (PCS) allows one to construct a multidimensional lowpass mask from a one-dimensional lowpass mask with prime dilation, so that the resulting lowpass mask is nonseparable, and the output mask has the same prime dilation as the input [10]. Furthermore, a certain minimum accuracy number of the output mask is guaranteed by the method, with this bound related to similar properties of the input mask (namely the minimum of the flatness and accuracy numbers of the input). In this paper, we will prove some new results about the PCS lowpass masks (see Section 3.2). More precisely, we will improve the understanding of PCS by proving new bounds on the accuracy and flatness numbers of the output lowpass mask, which guarantee that under certain conditions, the accuracy number of the input lowpass mask is exactly the accuracy number of the output lowpass mask. We will also prove that when the input mask is interpolatory and satisfies the sub-QMF condition, the output also satisfies these properties, and the associated refinable function belongs to  $L^2(\mathbb{R}^n)$ , using a result from [7]. For more details about PCS, see [10], though some of the properties of this method are reviewed in Section 3.1.

We will use PCS to take a univariate lowpass mask R with odd prime dilation p, and from this construct an n-dimensional lowpass mask  $\tau$  with this same prime dilation<sup>2</sup>. Under certain conditions on R, we will find an sos representation for a trigonometric polynomial related to  $\tau$ , as required by the SOSTF method. We then use the generators of this sos representation to generate highpass masks satisfying the UEP conditions with  $\tau$  via the SOSTF method, which leads to a tight wavelet frame for  $L^2(\mathbb{R}^n)$ . We refer to this new method as the *Prime Coset Sum Method for Tight Wavelet Frames* (PCSTF), and use our results on the vanishing moments of the SOSTF highpass masks to prove that a lower bound for the number of vanishing moments of the generated frames is proportional to the accuracy number of the input lowpass mask. These results are informed by the new bounds on the accuracy and flatness numbers of lowpass masks arising from PCS.

In Section 2, we review some important ideas and results which will feature throughout, on the Unitary Extension Principle (UEP) and Sum of Hermitian Squares Representation Method for Tight Wavelet Frames (SOSTF). We then prove our results on the vanishing moments of SOSTF highpass masks. In Section 3, we review the Prime Coset Sum Method (PCS), and prove that it preserves the sub-QMF condition for interpolatory filters. We then prove new results on the flatness and accuracy numbers of lowpass masks generated from PCS. In Section 4, we recall the definition of a group action, and use this to define a particular orbit decomposition of the set of coset representatives input to PCS. We then use this orbit decomposition to prove that the desired sos representations for SOSTF exist for a certain class of input univariate lowpass masks (called *PCSTF-admissible*) to PCS, which gives us the Prime Coset Sum Method for Tight Wavelet Frames (PCSTF). We then apply our previous results on the vanishing moments of SOSTF highpass masks and the flatness and accuracy numbers of PCS lowpass masks to give bounds on the vanishing moments of PCSTF-generated tight wavelet frames. In Section 4.4, we give two examples of our full method, and concluding remarks are given in Section 5.

# 2. Review of SOSTF and New Properties of SOSTF Highpass Masks

In this section, we review some basic properties of filters and masks in the context of wavelets; wavelet frames and the unitary extension principle; and sums of squares and the SOSTF method. Then in Section 2.4, we prove new lower bounds on the number of vanishing moments of highpass masks arising from SOSTF.

# 2.1. Filters and Masks

Let p be an odd prime number. We call a trigonometric polynomial  $R(\omega) = p^{-1} \sum_{k \in \mathbb{Z}} r(k) \exp(-ik\omega)$ , where  $r : \mathbb{Z} \to \mathbb{C}$  is finitely supported, and  $\omega \in \mathbb{T} := [-\pi, \pi]$ , a lowpass or refinement mask when it satisfies R(0) = 1, and we call p

<sup>&</sup>lt;sup>2</sup>In this paper, we consider an odd prime dilation p only, since in the case p = 2, PCS reduces to the coset sum method of [9], and tight wavelet frames with lowpass masks arising from the coset sum method were constructed in [8].

the dilation factor of R. We call r the filter corresponding to the mask R.<sup>3</sup> If instead R(0) = 0, we call it a highpass or wavelet mask. We will assume that all lowpass masks have real filter coefficients, but will allow potentially complex coefficients for wavelet masks.

For a nonnegative integer m, we say that R has accuracy number m when the minimum order of zeroes of R at  $(2\pi/p)\{1, \ldots, p-1\}$  is m. The flatness number of a lowpass mask is the order of the zero of 1 - R at 0, and the corresponding quantity of interest for highpass masks is the order of the zero R has at 0, which is called the number of vanishing moments of R. A lowpass mask R is called interpolatory if

$$\sum_{\gamma \in (2\pi/p)\{0,\dots,p-1\}} R(\omega + \gamma) = 1, \quad \forall \omega \in \mathbb{T}.$$

These definitions may be extended to the multidimensional setting analogously, and we will use the notation  $\tau(\omega) = p^{-n} \sum_{k \in \mathbb{Z}^n} h(k) \exp(-ik \cdot \omega), \ \omega \in \mathbb{T}^n$  to denote an *n*-dimensional lowpass mask, so that we may clearly separate the input and output lowpass masks for the PCS method. Here and below,  $h : \mathbb{Z}^n \to \mathbb{R}$ is assumed to be finitely supported and  $k \cdot \omega$  denotes the inner product  $\omega^* k$  of k and  $\omega$  in  $\mathbb{R}^n$  or  $\mathbb{C}^n$ , where  $x^*$  denotes the conjugate transpose of the column vector x.

Given a set  $\Gamma$  of distinct coset representatives of  $\mathbb{Z}^n/p\mathbb{Z}^n$  containing 0, the polyphase component of  $\tau$  associated with the coset  $\nu \in \Gamma$  is defined as  $\tau_{\nu}(\omega) := p^{-n/2} \sum_{k \in \mathbb{Z}^n} h(pk - \nu) \exp(-ik \cdot \omega)$ , so that when  $\tau$  is a lowpass mask with positive accuracy number,  $\tau_{\nu}(0) = p^{-n/2}$  for all  $\nu \in \Gamma$ . An important identity relating the polyphase components to the original mask is

$$\tau(\omega) = p^{-n/2} \sum_{\nu \in \Gamma} \tau_{\nu}(p\omega) \exp(i\omega \cdot \nu), \quad \omega \in \mathbb{T}^n.$$
(1)

We will also use the dual identity

$$\tau_{\nu}(p\omega) = p^{-n/2} \sum_{\gamma \in \Omega} \tau(\omega + \gamma) \exp(-i(\omega + \gamma) \cdot \nu), \quad \omega \in \mathbb{T}^n,$$
(2)

where here and below,  $\Omega := (2\pi/p)\{0, \ldots, p-1\}^n$ .

# 2.2. Wavelet Frames and the Unitary Extension Principle

We will use several results to justify our new PCSTF method. The first of these is the *unitary extension principle (UEP)*, which gives a set of conditions on a collection of trigonometric polynomials to guarantee that the wavelet system generated using these is actually a tight wavelet frame for  $L^2(\mathbb{R}^n)$ . Let us first define these terms. Given a lowpass mask  $\tau$  in n dimensions, we may define the

<sup>&</sup>lt;sup>3</sup>In some references, r is called the mask and R the symbol, but we use this terminology for consistency with [8, 10, 11].

corresponding refinable function  $\phi$  with dilation factor p by its Fourier transform, as  $\hat{\phi}(\omega) = \prod_{m=1}^{\infty} \tau(p^{-m}\omega), \, \omega \in \mathbb{R}^n$ . Given highpass masks  $q_j, \, 1 \leq j \leq J$ , we define the mother wavelets  $\psi^{(j)}$  by  $\widehat{\psi^{(j)}}(\omega) = q_j(p^{-1}\omega)\hat{\phi}(p^{-1}\omega), \, \omega \in \mathbb{R}^n$ . Then the wavelet system generated by  $\psi^{(j)}, \, 1 \leq j \leq J$ , is the collection

$$\Lambda := \Lambda(\{\psi^{(j)}\}) := \{\psi_{l,k}^{(j)} : 1 \le j \le J, l \in \mathbb{Z}, k \in \mathbb{Z}^n\},\tag{3}$$

where  $\psi_{l,k}^{(j)}(x) := p^{ln/2}\psi^{(j)}(p^l x - k), x \in \mathbb{R}^n$ . We say that  $\Lambda$  is a *(MRA-based)* tight wavelet frame when this set forms a tight frame for  $L^2(\mathbb{R}^n)$ . We now state the theorem of the UEP, the present version as given in [7], but specialized to our setting.

**Result 1** (UEP). Let  $\tau$  be a trigonometric polynomial with  $\tau(0) = 1$ , and let  $\phi$  be defined by  $\hat{\phi}(\omega) := \prod_{m=1}^{\infty} \tau(p^{-m}\omega)$  for  $\omega \in \mathbb{R}^n$ . If  $q_j, 1 \leq j \leq J$ , are trigonometric polynomials such that for all  $\omega \in \mathbb{T}^n$ :

$$\tau(\omega)\overline{\tau(\omega+\gamma)} + \sum_{j=1}^{J} q_j(\omega)\overline{q_j(\omega+\gamma)} = \begin{cases} 1, & \gamma = 0\\ 0, & \gamma \in \Omega \setminus \{0\} \end{cases}$$
(4)

where  $\Omega = (2\pi/p)\{0, \ldots, p-1\}^n$ , then  $\Lambda(\{\psi^{(j)}\})$  with  $\widehat{\psi^{(j)}} = q_j(p^{-1}\cdot)\widehat{\phi}(p^{-1}\cdot)$ ,  $1 \leq j \leq J$  is a tight wavelet frame for  $L^2(\mathbb{R}^n)$ .

When a set of masks  $\{\tau, q_j, 1 \leq j \leq J\}$  satisfy the UEP conditions as in (4), we will call the set a *tight wavelet filter bank*.

# 2.3. SOS Representation Method for Tight Wavelet Frames (SOSTF)

One way to find the trigonometric polynomials  $q_j$ ,  $1 \le j \le J$ , satisfying the UEP conditions with the lowpass mask  $\tau$ , is to find a sum of hermitian squares (sos) representation for the function

$$f(\tau;\omega) = 1 - \sum_{\gamma \in \Omega} |\tau(\omega/p + \gamma)|^2, \quad \omega \in \mathbb{T}^n.$$
(5)

It is easy to see that this is a trigonometric polynomial, and when it is nonnegative,  $\tau$  is said to satisfy the *sub-QMF* condition. We note that when  $\tau$ satisfies the sub-QMF condition,  $\tau$  must have positive accuracy, since for any  $\gamma' \in \Omega \setminus \{0\}, |\tau(\gamma')|^2 \leq \sum_{\gamma \in \Omega \setminus \{0\}} |\tau(\gamma)|^2 \leq 1 - |\tau(0)|^2 = 0.$ We may rewrite the function f above using the polyphase representation of

We may rewrite the function f above using the polyphase representation of the mask  $\tau$ , which gives

$$f(\tau;\omega) = 1 - \sum_{\nu \in \Gamma} |\tau_{\nu}(\omega)|^2, \quad \omega \in \mathbb{T}^n,$$
(6)

which is the form of f we will use more often. We now state an important result about lowpass filters satisfying the sub-QMF condition, which is from [7], but specialized to our setting here. **Result 2** (Sub-QMF lowpass masks yield  $L^2$  refinable functions). Suppose  $\tau$  is a lowpass mask that satisfies the sub-QMF condition. Then the refinable function  $\phi$  corresponding to  $\tau$  is a compactly supported function in  $L^2(\mathbb{R}^n)$ .

A sos representation of a trigonometric polynomial g is a collection of trigonometric polynomials  $g_j$ ,  $1 \leq j \leq N$ , such that  $g(\omega) = \sum_{j=1}^{N} |g_j(\omega)|^2$ ,  $\omega \in \mathbb{T}^n$ . The connection between sos representations for  $f(\tau; \cdot)$  and the UEP conditions is the content of the following theorem, which may be found in [2, 11], though we have specialized it to our setting. We will prove some lower bounds on the vanishing moments of the highpass masks coming from this method in Section 2.4.

**Result 3** (SOSTF). Suppose  $\tau$  is a lowpass mask that satisfies the sub-QMF condition, and let  $\Gamma$  be a set of distinct coset representatives of  $\mathbb{Z}^n/p\mathbb{Z}^n$  including 0. Suppose also that  $\sum_{\nu \in \Gamma} |\tau_{\nu}(\omega)|^2 + \sum_{j=1}^N |g_j(\omega)|^2 = 1$ , for all  $\omega \in \mathbb{T}^n$ . Then, with  $\tau$ , the  $p^n + N$  functions

$$q_{1,\nu}(\omega) = p^{-n/2} \exp(i\nu \cdot \omega) - \tau(\omega)\overline{\tau_{\nu}(p\omega)}, \quad \nu \in \Gamma,$$
$$q_{2,j}(\omega) = \tau(\omega)\overline{g_j(p\omega)}, \quad j = 1, \dots, N,$$

satisfy the UEP conditions, and thus form a tight wavelet filter bank.

We will also use two lemmas which guarantee the existence of sos representations under certain conditions. The first of these is the famous Fejér-Riesz Lemma, which says that a nonnegative univariate trigonometric polynomial has an sos representation with a single hermitian square. The statement and proof of this result may be found in [4]. The second comes from [13, Cor. 3.4] and the proof of [2, Th. 2.4], but we have adapted the notation to that of our paper.

**Result 4** (Sos Lemma). Suppose g is a nonnegative bivariate trigonometric polynomial. Then it has an sos representation.

## 2.4. New Properties of SOSTF Highpass Masks

We first prove a result about the vanishing moments of highpass masks constructed using the SOSTF method of Result 3. Here and below, we use standard multiindex notation as in [6].

**Proposition 1.** In Result 3, let  $\tau$  have accuracy number a > 0 and flatness number b. Then the highpass masks  $q_{1,\nu}, \nu \in \Gamma$  have at least min $\{a, b\}$  vanishing moments, and the highpass masks  $q_{2,j}, 1 \leq j \leq N$  have exactly as many vanishing moments as  $g_j, 1 \leq j \leq N$ .

*Proof.* We consider the  $q_{1,\nu}, \nu \in \Gamma$  first. Let  $m = \min\{a, b\}$ . The result is clear when m = 1, so let  $m \geq 2$ . If  $\beta$  is a multiindex with  $1 \leq |\beta| \leq m - 1$ , then by the assumptions on the accuracy and flatness numbers of  $\tau$ ,

$$D^{\beta}\tau(\gamma) = 0 \text{ for all } \gamma \in \Omega = (2\pi/p)\{0, \dots, p-1\}^n.$$
(7)

Now we compute  $D^{\alpha}q_{1,\nu}(\omega)$  for some  $\alpha$  with  $1 \leq |\alpha| \leq m-1$ . Recalling that we are assuming all lowpass filters have real coefficients, by Leibniz's formula, we obtain

$$\frac{i^{|\alpha|}\nu^{\alpha}}{p^{n/2}}\exp(i\nu\cdot\omega) - \sum_{\beta\leq\alpha} \binom{\alpha}{\beta} D^{\beta}\tau(\omega)\overline{D^{\alpha-\beta}[\tau_{\nu}(p\omega)]},$$

and at  $\omega = 0$ , this yields  $p^{-n/2}i^{|\alpha|}\nu^{\alpha} - \sum_{\beta \leq \alpha} {\alpha \choose \beta} D^{\beta}\tau(0) \overline{D^{\alpha-\beta}[\tau_{\nu}(p\omega)]_{\omega=0}}$ . By (7), only the term with  $\beta = 0$  remains in this sum. Since  $\tau(0) = 1$ , this yields

$$D^{\alpha}q_{1,\nu}(0) = p^{-n/2}i^{|\alpha|}\nu^{\alpha} - \overline{D^{\alpha}[\tau_{\nu}(p\omega)]_{\omega=0}}.$$
(8)

By (2), and using Leibniz's formula again, we see that  $D^{\alpha}[\tau_{\nu}(p\omega)]$  equals

$$p^{-n/2} \sum_{\gamma \in \Omega} \sum_{\beta \le \alpha} \binom{\alpha}{\beta} D^{\beta} \tau(\omega + \gamma) (-i)^{|\alpha - \beta|} \nu^{\alpha - \beta} \exp(-i\nu \cdot (\omega + \gamma)),$$

and at  $\omega = 0$ , by (7) and the positive accuracy of  $\tau$ , the only nonzero term in the sum is when  $\beta = 0$  and  $\gamma = 0$ , which yields  $D^{\alpha}[\tau_{\nu}(p\omega)]_{\omega=0} = p^{-n/2}(-i)^{|\alpha|}\nu^{\alpha}$ . From (8), we see that  $D^{\alpha}(q_{1,\nu})(0) = 0$  whenever  $|\alpha| \leq m-1$ , and thus  $q_{1,\nu}$  has at least m vanishing moments, as desired.

The analysis of the highpass masks  $q_{2,j}$  is simpler: since for  $\omega \approx 0, \tau(\omega) \approx 1$ , we see that  $g_j(\omega) = O(||\omega||^l)$  if and only if  $q_{2,j}(\omega) = O(||\omega||^l)$ .

We may obtain more detailed information about the vanishing moments of the sos generators  $g_j$  by taking a closer look at the relation  $f(\tau; \cdot) = \sum_{j=1}^{N} |g_j|^2$ . Notice from the definition of  $f(\tau; \cdot)$  in (5), we have  $f(\tau; 0) = 0$  for any lowpass mask  $\tau$  with positive accuracy, hence  $f(\tau; \cdot)$  can be considered as a highpass mask in such a case. In fact, we have the following result.

**Proposition 2.** Let  $\tau$  be a lowpass mask with accuracy number a > 0 and and flatness number b. Let c be the order of the zero of  $1 - |\tau|^2$  at 0. Then  $f(\tau; \cdot)$  has at least min $\{2a, c\} \ge \min\{2a, b\}$  vanishing moments.

*Proof.* By the assumptions on  $\tau$ , we see that for  $\omega \approx 0$ ,  $\tau(\omega) = 1 + O(||\omega||^b)$ , and for all  $\gamma \in \Omega \setminus \{0\}$ ,  $\tau(\omega + \gamma) = O(||\omega||^a)$ , hence expanding the square,  $|\tau(\omega)|^2 = 1 + O(||\omega||^b)$ , and  $|\tau(\omega + \gamma)|^2 = O(||\omega||^{2a})$ . This shows that  $c \geq b$ , and for  $\omega \approx 0$ ,

$$f(\tau; p\omega) = 1 - \sum_{\gamma \in \Omega} |\tau(\omega + \gamma)|^2 = O(||\omega||^c) + O(||\omega||^{2a}),$$

which completes the proof.

These results lead to the following theorem, which gives lower bounds on the vanishing moments of the highpass masks constructed from Result 3 in terms of the flatness and accuracy numbers of the lowpass mask  $\tau$ . Note that as a special case, when  $\tau$  is an interpolatory lowpass mask, the flatness number is always at least as large as the accuracy number. We construct highpass filters with exactly this many vanishing moments in Examples 2 and 3.

**Theorem 1** (VMs for SOSTF highpass masks). Let  $\tau$  be a lowpass mask with accuracy number a > 0 and flatness number b. Then if  $f(\tau; \cdot)$  has an sos representation with trigonometric polynomials  $g_j, 1 \leq j \leq N$ , then each  $g_j$  has at least min $\{a, \lceil b/2 \rceil\}$  vanishing moments. Therefore, for the highpass masks in Result 3,  $q_{1,\nu}, \nu \in \Gamma$  have at least min $\{a, b\}$  vanishing moments, and  $q_{2,j}, 1 \leq j \leq N$  have at least min $\{a, \lceil b/2 \rceil\}$  vanishing moments.

*Proof.* Let c be the order of the zero of  $1 - |\tau|^2$  at 0. Then, from the proof of Proposition 2,  $c \geq b$  and  $\sum_{j=1}^{N} |g_j(\omega)|^2 = f(\tau; \omega) = O(\|\omega\|^{\min\{2a,c\}})$  for  $\omega \approx 0$ . Thus all of the summands  $|g_j(\omega)|^2 = O(\|\omega\|^{\min\{2a,c\}})$  for  $\omega \approx 0$ , so  $g_j(\omega) = O(\|\omega\|^{\min\{a,c/2\}})$  for all  $1 \leq j \leq N$ , and these all have at least  $\min\{a, \lceil b/2 \rceil\}$  vanishing moments since  $c \geq b$ . The remaining statements follow from Proposition 1.

## 3. Review of PCS and New Properties of PCS Lowpass Masks

In this section, we review some basic properties of the prime coset sum method (PCS), before proving some new results which show that PCS preserves the sub-QMF property for interpolatory lowpass masks. We also find new bounds on the flatness number of  $\tau$  arising from PCS in terms of the flatness number of R, and use these bounds to get detailed information about the accuracy and flatness numbers of  $\tau$  in a special case.

We start by fixing some notation which will be used throughout the sequel. Let p be a fixed odd prime, and let I be a set of distinct coset representatives of  $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$  including 0. Let  $n \geq 2$  be the spatial dimension, and let  $\Gamma$  be a set of distinct coset representatives of  $\mathbb{Z}^n/p\mathbb{Z}^n$  including 0. We use the notation  $\Gamma', I'$  to denote the corresponding sets of nonzero cosets, and we denote by  $(a \pmod{p})$  the number  $b \in I$  such that  $a \equiv b \pmod{p}$ , for any integer a. In some cases, we will have multiple sets I under consideration, so we will use the notation  $(a \pmod{p})$  refers to the multiplicative inverse of a in  $\mathbb{Z}_p$ , when  $a \not\equiv 0 \pmod{p}$ , and we will adopt the convention that  $((a^{-1} \pmod{p})b \pmod{p})$  will be abbreviated as  $(a^{-1}b \pmod{p})$  throughout.

#### 3.1. Prime Coset Sum Method (PCS)

The prime coset sum method takes a univariate lowpass mask with prime dilation factor and outputs a nonseparable multidimensional lowpass mask with this same prime dilation factor.<sup>4</sup> For a specified dimension  $n \ge 2$ , given the input lowpass mask R and a set  $\Gamma$  of distinct coset representatives of  $\mathbb{Z}^n/p\mathbb{Z}^n$ 

 $<sup>^{4}</sup>$ In [10], this is extended to take univariate biorthogonal lowpass masks with prime dilation as input and generate a multidimensional biorthogonal wavelet system with the same prime dilation.

containing 0, the PCS lowpass mask is defined for all  $\omega \in \mathbb{T}^n$  as

$$\tau(\omega) := \frac{1}{(p-1)p^{n-1}} \left( 1 - p^{n-1} + \sum_{\nu \in \Gamma'} R(\omega \cdot \nu) \right).$$
(9)

A proof that  $\tau$  is well defined can be found in [10], as well as many important properties of this mask, some of which we collect below.

**Result 5** (Properties of PCS). Let R be a univariate lowpass mask with prime dilation p, and let  $\tau$  be the output of the PCS method as in (9). Then the following properties hold:

- (i) If R is interpolatory, then  $\tau$  is interpolatory.
- (ii) If R has accuracy number a and flatness number b, then  $\tau$  has accuracy number at least min $\{a, b\}$ .
- (iii) If  $R(\omega) = R(-\omega)$ , then  $\tau(\omega) = \tau(-\omega)$ .

We will prove additional properties of these lowpass masks in the current work.

# 3.2. New Properties of PCS Lowpass Masks

Let the prime number p and the set I be fixed as described above. Let R be a univariate lowpass mask with dilation p, and let  $\tau$  be the output of PCS with input R in n dimensions, and with a fixed set  $\Gamma$ . In presenting our results on PCS lowpass masks below and throughout the paper, we will use sets  $\mathcal{M}(\nu), \nu \in \Gamma'$  defined as

$$\mathcal{M}(\nu) = \{ (\nu', j) \in \Gamma' \times I' : j\nu' \equiv \nu \pmod{p\mathbb{Z}^n} \}.$$
<sup>(10)</sup>

We will say more about these sets after defining group actions in Section 4.1 (see Remark after Lemma 3), but for now the only property we require of them is that  $|\mathcal{M}(\nu)| = p - 1$ .

**Lemma 1** (Polyphase components of  $\tau$ ). The polyphase components of  $\tau$  are given as follows:

$$\tau_0(\omega) = \frac{p}{(p-1)p^{n/2}} \left( 1 - p^{n-1} + \frac{1}{\sqrt{p}} \sum_{\nu \in \Gamma'} R_0(\omega \cdot \nu) \right),$$
  
$$\tau_{\nu}(\omega) = \frac{\sqrt{p}}{(p-1)p^{n/2}} \sum_{(\nu',j) \in \mathcal{M}(\nu)} R_j(\omega \cdot \nu') \exp\left(i\omega \cdot \frac{j\nu' - \nu}{p}\right), \quad \nu \in \Gamma'.$$

*Proof.* We start by computing, to try to write  $\tau(\omega) = \sum_{\nu \in \Gamma} g_{\nu}(p\omega) \exp(i\omega \cdot \nu)$  as in (1), in which case the functions  $p^{n/2}g_{\nu}$  are the polyphase components. Starting from (9), and using (1) for R, where  $R_j, j \in I$  are its polyphase components, we see that

$$\tau(\omega) = \frac{1}{(p-1)p^{n-1}} \left( 1 - p^{n-1} + \frac{1}{\sqrt{p}} \sum_{\nu \in \Gamma'} \sum_{j \in I} R_j(p\omega \cdot \nu) \exp(ij\omega \cdot \nu) \right)$$
$$= \frac{1}{(p-1)p^{n-1}} \left( 1 - p^{n-1} + \frac{1}{\sqrt{p}} \sum_{\nu \in \Gamma'} R_0(p\omega \cdot \nu) \right)$$
$$+ \frac{\sqrt{p}}{(p-1)p^n} \sum_{\nu \in \Gamma'} \sum_{j \in I'} R_j(p\omega \cdot \nu) \exp(ij\omega \cdot \nu).$$

We observe that the first line of the last expression above gives us the desired formula for  $\tau_0$ . Since we are summing over  $\nu \in \Gamma'$  and  $j \in I'$  in the last line, and each coset in  $\Gamma'$  is congruent to  $j\nu \pmod{p\mathbb{Z}^n}$  for exactly p-1 pairs  $(\nu, j)$ , we repurpose  $\nu$  for this product and sum over the pairs  $(\nu', j) \in \Gamma' \times I'$  with  $j\nu' \equiv \nu$ , which leads to the following formula for  $\tau(\omega) - p^{-n/2}\tau_0(p\omega)$ :

$$\frac{\sqrt{p}}{(p-1)p^n} \sum_{\nu \in \Gamma'} \sum_{(\nu',j) \in \mathcal{M}(\nu)} R_j(p\omega \cdot \nu') \exp(i\omega \cdot j\nu')$$
$$= \frac{\sqrt{p}}{(p-1)p^n} \sum_{\nu \in \Gamma'} \left( \sum_{(\nu',j) \in \mathcal{M}(\nu)} R_j(p\omega \cdot \nu') \exp(i\omega \cdot (j\nu'-\nu)) \right) \exp(i\omega \cdot \nu).$$

The expression inside the large parentheses here is indeed a function of  $p\omega$ , so this completes the proof.

We next find an upper bound for  $|\tau_{\nu}(\omega)|^2$  when  $\nu \in \Gamma'$ .

**Lemma 2** (Squared polyphase components of  $\tau$ ). For  $\nu \in \Gamma'$ , the polyphase components of  $\tau$  satisfy

$$|\tau_{\nu}(\omega)|^{2} \leq \frac{p}{(p-1)p^{n}} \sum_{(\nu',j)\in\mathcal{M}(\nu)} |R_{j}(\omega\cdot\nu')|^{2}.$$

*Proof.* By viewing the formula for  $\tau_{\nu}(\omega)$  given in Lemma 1 as, up to a multiplicative constant, the inner product of the vectors  $[R_j(\omega \cdot \nu')]_{(\nu',j)\in\mathcal{M}(\nu)}$  and  $[\exp(i\omega \cdot (\nu - j\nu')/p)]_{(\nu',j)\in\mathcal{M}(\nu)}$  for some ordering of the set  $\mathcal{M}(\nu)$ , we may apply the Cauchy-Schwarz Inequality to conclude that

$$|\tau_{\nu}(\omega)|^{2} \leq \frac{p}{(p-1)^{2}p^{n}} \left[ (p-1) \sum_{(\nu',j) \in \mathcal{M}(\nu)} |R_{j}(\omega \cdot \nu')|^{2} \right].$$

**Definition 1.** We say that a univariate lowpass mask R satisfying the interpolatory and sub-QMF conditions is PCSTF-admissible.

Note that every PCSTF-admissible mask R has positive accuracy as R is necessarily lowpass and satisfies the sub-QMF condition (c.f. Section 2.3).

**Theorem 2** (PCS preserves the sub-QMF condition for interpolatory masks). Let R be PCSTF-admissible. Then  $\tau$  satisfies the multivariate sub-QMF condition.

*Proof.* Using the fact that the PCS method preserves the interpolatory and positive accuracy properties (c.f. Result 5(i-ii)),  $\tau_0(\omega) = p^{-n/2}$ , so from (6) and the preceding lemma, we have that

m

$$f(\tau;\omega) = \frac{p^n - 1}{p^n} - \sum_{\nu \in \Gamma'} |\tau_{\nu}(\omega)|^2$$

$$\geq \frac{p^n - 1}{p^n} - \frac{p}{(p-1)p^n} \sum_{\nu \in \Gamma'} \sum_{(\nu',j) \in \mathcal{M}(\nu)} |R_j(\omega \cdot \nu')|^2$$

$$= \frac{p^n - 1}{p^n} - \frac{p}{(p-1)p^n} \sum_{\nu \in \Gamma'} \sum_{j \in I'} |R_j(\omega \cdot \nu)|^2$$

$$= \frac{p}{(p-1)p^n} \sum_{\nu \in \Gamma'} \left( \frac{p-1}{p} - \sum_{j \in I'} |R_j(\omega \cdot \nu)|^2 \right)$$

$$= \frac{p}{(p-1)p^n} \sum_{\nu \in \Gamma'} f(R; \omega \cdot \nu) \geq 0.$$
(11)

This completes the proof.

Applying Result 2, we immediately obtain the following corollary:

**Corollary 1.** Let R be PCSTF-admissible. Then the refinable function associated with  $\tau$  is a compactly supported  $L^2(\mathbb{R}^n)$  function.

When  $\tau$  is the output of PCS with input R, Result 5(ii) tells us that its accuracy number is at least the minimum of the flatness and accuracy numbers of R. In light of Theorem 1, we see the importance of the flatness and accuracy numbers of  $\tau$  for the vanishing moments of highpass masks constructed from SOSTF when the lowpass mask arises from PCS, which is the approach we take in the PCSTF method, detailed in Section 4. To this end we have the following result which shows the relationship between the flatness numbers of  $\tau$  and R.

**Proposition 3** (Flatness number of  $\tau$ ). Let R have flatness number s, and let t be the smallest even integer such that  $D^t(1-R)(0) \neq 0$ . Then  $1 \leq s \leq t$  and the flatness number of  $\tau$  lies between s and t (inclusive of s, t). Furthermore,

- (i) If  $R(\omega) = R(-\omega), \omega \in \mathbb{T}$ , then the flatness number of  $\tau$  is s = t.
- (ii) If  $\Gamma = -\Gamma$ , then the flatness number of  $\tau$  is t.

*Proof.* Let  $\alpha$  be a multiindex with  $|\alpha| > 0$ . Then from (9):

$$D^{\alpha}\tau(\omega) = \frac{1}{(p-1)p^{n-1}} \sum_{\nu \in \Gamma'} \nu^{\alpha} D^{|\alpha|} R(\omega \cdot \nu),$$

$$D^{\alpha}\tau(0) = \frac{D^{|\alpha|}R(0)}{(p-1)p^{n-1}} \sum_{\nu \in \Gamma'} \nu^{\alpha}.$$

This proves the lower bound immediately. If we consider  $\alpha = [t, 0, \dots, 0]^T$ ,  $\sum_{\nu \in \Gamma'} \nu^{\alpha} > 0$ , so we see that  $D^{\alpha} \tau(0) \neq 0$ . Furthermore,

(i) If  $R(\omega) = R(-\omega)$ , then  $R(\omega) = c_0 + \sum_{k=1}^d c_k \cos(k\omega)$ , for some  $c_k$  and d, so for any integer  $j \ge 0$ ,  $D^{2j+1}R(\omega) = (-1)^{j+1} \sum_{k=1}^d c_k k^{2j+1} \sin(k\omega)$ , which is 0 at  $\omega = 0$ . Then in this case, s = t.

(ii) If  $\Gamma = -\Gamma$ , then  $\sum_{\nu \in \Gamma'} \nu^{\alpha} = \sum_{\nu \in \Gamma'} (-\nu)^{\alpha} = -\sum_{\nu \in \Gamma'} \nu^{\alpha}$  for any multiindex  $\alpha$  with odd  $|\alpha|$ , which means this sum is 0. Then  $D^{\alpha}\tau(0) = 0$  for all  $\alpha$  with odd  $|\alpha|$ , which completes the proof.

Note that it is possible to have s < t in this proposition. For example,  $R(\omega) = \frac{1}{3}(1 + \exp(i\omega) + \exp(2i\omega))$  is PCSTF-admissible with accuracy and flatness numbers equal to 1 (hence s = 1), but t = 2.

The following corollary illustrates a simple but illuminating use of this proposition.

**Corollary 2** (Accuracy and flatness numbers equal and even). Let R be interpolatory, and have accuracy and flatness numbers both equal to an even integer m > 0. Then  $\tau$  has accuracy and flatness numbers both equal to m.

*Proof.* By Result 5(i-ii),  $\tau$  is interpolatory, and its accuracy number is at least m. By the interpolatory property, the flatness number of  $\tau$  is at least its accuracy number, but the proposition above tells us this flatness number is m (= s = t, in the notation of the proposition). Thus both numbers are equal to m.

Since a PCSTF-admissible mask is interpolatory, Corollary 2 says that in particular  $\tau$  has accuracy and flatness numbers both equal to an even positive m whenever the univariate mask R is PCSTF-admissible with the same property.

# 4. Prime Coset Sum Tight Wavelet Frames

We would like more detailed information about the function  $f(\tau; \cdot)$  (c.f. (5)) when  $\tau$  is the output of PCS with PCSTF-admissible input R in n dimensions, and with a fixed set  $\Gamma$ . In particular, we would like to know whether  $f(\tau; \cdot)$ has an sos representation in this setting, and as it happens, this is guaranteed to exist for any p and n, and any set  $\Gamma$ . This fact clearly relies heavily on the structure of PCS, since in [2, Th. 2.5], it is shown that there exist lowpass masks in 3 dimensions for which  $f(\tau; \cdot)$  has no sos representation. We begin by recalling the definition of a group action, which we will use to define the orbit decomposition of the set  $\Gamma$ , and will be useful for finding sos representations for  $f(\tau; \cdot)$ . After this, we prove a useful lemma from lattice theory which is used to ensure that variables with certain properties exist.

 $\mathbf{SO}$ 

# 4.1. Group Actions

We recall that a finite group G is said to *act on a set* X when there is an associated permutation of X for each element of G, such that the identity element of G acts as the identity permutation, and  $\langle g_1, \langle g_2, x \rangle \rangle = \langle g_1g_2, x \rangle$  for all  $g_1, g_2 \in G$  and  $x \in X$ , where we denote the permutation of X associated with  $g \in G$  by  $\langle g, x \rangle$  for all  $x \in X$ , and we denote the group multiplication by juxtaposition. Then the *orbit* of  $x \in X$  is the set  $\langle G, x \rangle := \{y \in X : y = \langle g, x \rangle$  for some  $g \in G \}$ .

In our setting, there is a natural action of the multiplicative group  $(\mathbb{Z}_p)^{\times}$ on the set  $\Gamma'$ . Let I be a set of distinct coset representatives of  $\mathbb{Z}_p$  containing 0, and let I' be the corresponding set of nonzero cosets. Then we may define  $\langle k, \nu \rangle$  as the element  $\nu' \in \Gamma'$  such that  $k\nu \equiv \nu' \pmod{p\mathbb{Z}^n}$ , which is well-defined because  $\Gamma$  contains distinct coset representatives. This is also independent of the choice of I, since if  $k \equiv j \pmod{p}$ , then  $k\nu \equiv j\nu \pmod{p\mathbb{Z}^n}$ , which are then both congruent to the same element  $\nu' \in \Gamma'$ . We will refer to this as the group action of  $(\mathbb{Z}_p)^{\times}$  on  $\Gamma'$ . In particular, given  $\Gamma$ , we can always find a set  $M \subset \Gamma'$ of distinct orbit representatives for this action, so that  $\Gamma' = \bigcup_{\mu \in M} \mathcal{O}_{\mu}$ , where  $\mathcal{O}_{\mu} = \langle (\mathbb{Z}_p)^{\times}, \mu \rangle$  is the notation we will use below for the orbit of  $\mu$  in this group action, where  $\mu \in \Gamma'$ .

We will use the following fact about the group action just described at several points in what follows.

**Lemma 3** (All orbits have size p-1). In the group action of  $(\mathbb{Z}_p)^{\times}$  on  $\Gamma'$ , each orbit has p-1 elements.

*Proof.* Let *I* be a set of distinct coset representatives of  $\mathbb{Z}_p$  including 0. Given  $\nu \in \Gamma'$ , the map  $\langle \cdot, \nu \rangle : I' \to \Gamma'$  is injective, since for  $\nu \in \Gamma'$ , there is some  $1 \leq i \leq n$  such that  $\nu(i) \not\equiv 0 \pmod{p}$ , and if  $k\nu \equiv j\nu \pmod{p}$ , then  $k\nu(i) \equiv j\nu(i) \pmod{p}$ , so  $k \equiv j \pmod{p}$ , which means that k = j, since *I* contains distinct coset representatives. By definition, the orbit  $\mathcal{O}_{\nu}$  is the image of this map, so  $|\mathcal{O}_{\nu}| = |I'| = p - 1$ .

**Remark:** For the set  $\mathcal{M}(\nu)$  in (10), we observe that we could index  $\mathcal{M}(\nu)$  by its first component, which just covers the elements of  $\mathcal{O}_{\nu}$ . Indeed, when  $j\nu' \equiv$  $\nu \pmod{p\mathbb{Z}^n}$ ,  $\nu' \equiv (j^{-1} \pmod{p})\nu \pmod{p\mathbb{Z}^n}$ , which shows that  $\nu' \in \mathcal{O}_{\nu}$ . Then  $\mathcal{M}(\nu)$  could equivalently be written  $\{(\nu', j) \in \mathcal{O}_{\nu} \times I' : j\nu' \equiv \nu \pmod{p\mathbb{Z}^n}\}$ , and this further shows that  $|\mathcal{M}(\nu)| = p - 1$  for all  $\nu \in \Gamma'$ , which is used in proving Lemmas 1 and 2. We may also index  $\mathcal{M}(\nu)$  by  $j \in I'$ , in which case  $\mathcal{M}(\nu) = \{(\langle (j^{-1} \pmod{p}), \nu \rangle, j) : j \in I'\}$ .

Note that since  $|\Gamma'| = p^n - 1$ , and the size of each orbit in the group action of  $(\mathbb{Z}_p)^{\times}$  on  $\Gamma'$  is p - 1, M must have  $(p^n - 1)/(p - 1) = \sum_{k=0}^{n-1} p^k$  elements.

In the following example, as throughout the paper, we use the notation  $e_i$  to denote the *i*th standard unit vector of the appropriate size.

**Example 1.** For p = 3, n = 2, let  $\Gamma_1 = \{-1, 0, 1\}^2$  and  $I = \{-1, 0, 1\}$ . We see that one choice of M is given by  $\{(1, -1), (1, 0), (1, 1), (0, 1)\}$ , and for each  $\mu \in M, \mathcal{O}_{\mu} = \{\mu, -\mu\}$ .

For the same p, n and I, if we let  $\Gamma_2 = (\{-1, 0, 1\}^2 \setminus \{-e_1\}) \cup \{2e_1\}$ , the same M again gives a set of distinct orbit representatives in the group action of  $(\mathbb{Z}_3)^{\times}$  on  $\Gamma'$ . When  $\mu \in M \setminus \{e_1\}$ ,  $\mathcal{O}_{\mu} = \{\mu, -\mu\}$ , and when  $\mu = e_1$ ,  $\mathcal{O}_{\mu} = \{\mu, 2\mu\}$ , so  $\langle -1, e_1 \rangle = 2e_1$ .

A diagram of these sets for  $\Gamma := \Gamma_1$  or  $\Gamma_2$  is depicted in Figure 1, where the  $\cdot$  indicate elements of  $\mathbb{Z}^2$  that do not belong to  $\Gamma$ ,  $\times$  indicates the origin,  $\bigstar$  indicate members of  $M \subset \Gamma$ , and  $\bullet$  indicate members of  $\Gamma \setminus (\{0\} \cup M)$ .



Figure 1: Examples of  $\Gamma$  for p = 3, n = 2 from Example 1

#### 4.2. A Lemma from Lattice Theory

In the following lemma, we show that a nonnegative trigonometric polynomial with nonzero coefficients only on a dimension-m subspace may be written coherently as a trigonometric polynomial in m variables  $\omega \cdot \zeta_i$  for some  $\zeta_i \in \mathbb{Z}^n$ ,  $1 \leq i \leq m$ . Our interest will be in the special cases of this lemma for m = 1 or 2, but we give the more general statement.

**Lemma 4.** Let  $\{x_1, \ldots, x_m\} \subset \mathbb{Z}^n$  be a linearly independent set. Then there are vectors  $\zeta_i \in \mathbb{Z}^n, 1 \leq i \leq m$ , such that if  $Z = [\zeta_1 | \zeta_2 | \cdots | \zeta_m]$ , then

- 1.  $\{x_1,\ldots,x_m\} \subset \mathbb{Z}\mathbb{Z}^m$ , and
- 2.  $Z: \mathbb{Z}^m \to \mathbb{Z}^n$  is injective mod p, i.e., for  $a \in \mathbb{Z}^m$ ,

if  $Za \equiv 0 \pmod{p\mathbb{Z}^n}$ , then  $a \equiv 0 \pmod{p\mathbb{Z}^m}$ .

*Proof.* Let  $\mathcal{L} = \text{span}(\{x_1, \ldots, x_m\}) \cap \mathbb{Z}^n$ , which is an *m*-dimensional lattice. Then by [1, Th. 10.4], there are vectors  $\zeta_i \in \mathbb{Z}^n, 1 \leq i \leq m$  such that each element of  $\mathcal{L}$  may be represented uniquely as Za for some  $a \in \mathbb{Z}^m$ , where Z is the matrix with columns  $\zeta_i, 1 \leq i \leq m$ . This shows the first point immediately.

For the second statement, if we let  $u \in p\mathcal{L} = \operatorname{span}(\{x_1, \ldots, x_m\}) \cap (p\mathbb{Z}^n)$ , then  $u/p \in \mathcal{L}$ , so u/p = Za, or u = Z(pa). Then since  $u \in \mathcal{L}$ , a' = pa is the unique integer vector such that u = Za'. This proves that if  $Za \equiv 0 \pmod{p\mathbb{Z}^n}$ , then  $a \equiv 0 \pmod{p\mathbb{Z}^m}$ .

## 4.3. Prime Coset Sum Method for Tight Wavelet Frames (PCSTF)

We are now ready to present our main result, a new method for constructing interpolatory tight wavelet frames with prime dilation for  $L^2(\mathbb{R}^n)$  based on the two known methods, PCS and SOSTF.

We start by showing that an sos representation for  $f(\tau; \cdot)$  (c.f. (5)) exists, provided that  $\tau$  is generated by PCS from a PCSTF-admissible univariate mask R, and then investigate the vanishing moments of the highpass filters arising from SOSTF using this  $\tau$  and sos representation.

**Theorem 3.** Let R be PCSTF-admissible, and let  $\tau$  be the output of PCS with input R in n dimensions. Then  $f(\tau; \cdot)$  has an sos representation.

The idea of the proof is as follows: We know that if  $G(\omega), \omega \in \mathbb{R}^n$  is a nonnegative trigonometric polynomial in one or two variables  $\omega \cdot \zeta$  or  $\omega \cdot \zeta_i$ , i = 1, 2, where  $\zeta, \zeta_1, \zeta_2 \in \mathbb{Z}^n$ , then  $G(\omega) = |g(\omega \cdot \zeta)|^2$  in the first case, by the Fejér-Riesz Lemma, or else is a sum of finitely many squares  $|g_j(\omega \cdot \zeta_1, \omega \cdot \zeta_2)|^2$ , by Result 4. The goal is then to decompose  $f(\tau; \cdot)$  into a sum of finitely many nonnegative trigonometric polynomials  $G_{\mu}$ , such that for each  $G_{\mu}$  we may find appropriate  $\zeta$ , or  $\zeta_i, i = 1, 2$ , with the property that  $G_{\mu}$  is a trigonometric polynomial in  $\omega \cdot \zeta$  or  $\omega \cdot \zeta_i, i = 1, 2$ . Combining this with the aforementioned results will then guarantee the existence of an sos representation for  $f(\tau; \cdot)$ . Our main assumption is that R satisfies the sub-QMF condition, and this will serve as a guide in the proof, since we will try to decompose  $f(\tau; \cdot)$  into  $G_{\mu}$ which are lower bounded by  $f(R; \omega \cdot \zeta)$  or some suitable combination of two  $f(R; \omega \cdot \zeta_i), i = 1, 2$ .

*Proof.* Let I be a set of distinct coset representatives of  $\mathbb{Z}_p$  containing 0, and let I' be the corresponding set of nonzero cosets. Let  $\Gamma$  be the set of distinct cosets of  $\mathbb{Z}^n/p\mathbb{Z}^n$  containing 0 used in the PCS method for constructing  $\tau$ , and let  $\Gamma'$  be the set of nonzero cosets. In the group action of  $(\mathbb{Z}_p)^{\times}$  on  $\Gamma'$ , which we recall is denoted  $\langle k, \nu \rangle$  for  $k \in I'$  and  $\nu \in \Gamma'$ , let M be a set of distinct orbit representatives. We define the following vector, which will significantly simplify our calculations, where  $k \in I'$ ,  $\mu \in M$  and  $\omega \in \mathbb{T}^n$ :

$$\mathcal{R}_{k,\mu}(\omega) = \left[ R_{(k^{-1}j \pmod{p})}(\omega \cdot \langle k, \mu \rangle) \exp\left(i\omega \cdot \frac{(k^{-1}j \pmod{p})\langle k, \mu \rangle}{p}\right) \right]_{j \in I'}.$$

Observe that

$$\frac{p-1}{p} - \|\mathcal{R}_{k,\mu}(\omega)\|^2 = \frac{p-1}{p} - \sum_{j \in I'} |R_{(k^{-1}j \pmod{p})}(\omega \cdot \langle k, \mu \rangle)|^2$$
$$= \frac{p-1}{p} - \sum_{j \in I'} |R_j(\omega \cdot \langle k, \mu \rangle)|^2$$
$$= f(R; \omega \cdot \langle k, \mu \rangle).$$

In particular, this shows that  $\|\mathcal{R}_{k,\mu}(\omega)\|^2 \leq \frac{p-1}{p}, \forall \omega \in \mathbb{T}^n$ .

Now we compute

$$f(\tau;\omega) = \frac{p^n - 1}{p^n} - \sum_{\nu \in \Gamma'} |\tau_{\nu}(\omega)|^2$$
  
=  $\frac{1}{p^n} \sum_{\mu \in M} \left[ p - 1 - p^n \sum_{j \in I'} |\tau_{\langle j, \mu \rangle}(\omega)|^2 \right] =: \frac{1}{p^n} \sum_{\mu \in M} G_{\mu}(\omega).$ 

Now using our computation of  $\tau_{\nu}, \nu \in \Gamma'$  from Lemma 1 and the remark after Lemma 3 on the set  $\mathcal{M}(\nu)$ , we see that  $G_{\mu}(\omega)$  equals

$$\begin{split} p-1 &- \frac{p}{(p-1)^2} \sum_{j \in I'} \sum_{k,\ell \in I'} R_{(k^{-1}j \pmod{p})} (\omega \cdot \langle k, \mu \rangle) \overline{R_{(\ell^{-1}j \pmod{p})} (\omega \cdot \langle \ell, \mu \rangle)} \\ &\quad \times \exp\left(i\omega \cdot \frac{(k^{-1}j \pmod{p}) \langle k, \mu \rangle - (\ell^{-1}j \pmod{p}) \langle \ell, \mu \rangle}{p}\right) \\ &= p-1 - \frac{p}{(p-1)^2} \sum_{k,\ell \in I'} (\mathcal{R}_{k,\mu}(\omega) \cdot \mathcal{R}_{\ell,\mu}(\omega)) \\ &= p-1 - \frac{p}{(p-1)^2} \sum_{k \in I'} (\|\mathcal{R}_{k,\mu}(\omega)\|^2) \\ &\quad - \frac{2p}{(p-1)^2} \sum_{\substack{k,\ell \in I' \\ k > \ell}} (\operatorname{Re}(\mathcal{R}_{k,\mu}(\omega) \cdot \mathcal{R}_{\ell,\mu}(\omega))) \\ &= \frac{p}{(p-1)^2} \sum_{\substack{k,\ell \in I' \\ k > \ell}} \left( \frac{p-1}{p} - \|\mathcal{R}_{k,\mu}(\omega) \cdot \mathcal{R}_{\ell,\mu}(\omega)) \right), \end{split}$$

where the identities  $\frac{p}{(p-1)^2}(p-1)\left(\frac{p-1}{p}\right) = 1$  and  $\frac{2p}{(p-1)^2}\left(\frac{(p-1)(p-2)}{2}\right)\left(\frac{p-1}{p}\right) = p-2$  along with  $|I'| = p-1, |\{k, \ell \in I' : k > \ell\}| = (p-1)(p-2)/2$  are used in the last line. Then defining  $G_{k,\ell,\mu}(\omega) = \frac{p-1}{p} - \operatorname{Re}(\mathcal{R}_{k,\mu}(\omega) \cdot \mathcal{R}_{\ell,\mu}(\omega))$ , we have

$$G_{\mu}(\omega) = \frac{p}{(p-1)^2} \sum_{k \in I'} (f(R; \omega \cdot \langle k, \mu \rangle)) + \frac{2p}{(p-1)^2} \sum_{\substack{k, \ell \in I' \\ k > \ell}} (G_{k,\ell,\mu}(\omega)).$$

Since  $f(R; \cdot)$  is a nonnegative univariate polynomial, which has an sos representation by the Fejér-Riesz Lemma, the proof is complete if we are able to show that  $G_{k,\ell,\mu}$  is a nonnegative bivariate trigonometric polynomial for every  $k, \ell, \mu$ , by Result 4. The nonnegativity is straightforward, since

$$\frac{p-1}{p} - \operatorname{Re}(\mathcal{R}_{k,\mu}(\omega) \cdot \mathcal{R}_{\ell,\mu}(\omega)) \ge \frac{p-1}{p} - \|\mathcal{R}_{k,\mu}(\omega)\| \|\mathcal{R}_{\ell,\mu}(\omega)\| \ge 0.$$

We see that

$$\mathcal{R}_{k,\mu}(\omega) \cdot \mathcal{R}_{\ell,\mu}(\omega) = \sum_{j \in I'} R_{(k^{-1}j \pmod{p})}(\omega \cdot \langle k, \mu \rangle) \overline{R_{(\ell^{-1}j \pmod{p})}(\omega \cdot \langle \ell, \mu \rangle)} \\ \times \exp\left(i\omega \cdot \frac{(k^{-1}j \pmod{p})\langle k, \mu \rangle - (\ell^{-1}j \pmod{p})\langle \ell, \mu \rangle}{p}\right)$$

Now take  $x = \langle k, \mu \rangle$  and  $y = \langle \ell, \mu \rangle$ . If x and y are linearly dependent, then use Lemma 4 with m = 1 to find  $\zeta$  using x as input. Then  $x = a\zeta$ ,  $y = b\zeta$ , for some  $a, b \in \mathbb{Z}$ , and  $G_{k,\ell,\mu}$  is a trigonometric polynomial in  $\omega \cdot \zeta$ , since

$$(k^{-1}j \pmod{p})(a\zeta) - (\ell^{-1}j \pmod{p})(b\zeta) \equiv 0 \pmod{p\mathbb{Z}^n} \Longrightarrow \frac{((k^{-1}j \pmod{p})a - (\ell^{-1}j \pmod{p})b}{p} \in \mathbb{Z},$$

using property 2 of Lemma 4. That is:

$$\mathcal{R}_{k,\mu}(\omega) \cdot \mathcal{R}_{\ell,\mu}(\omega) = \sum_{j \in I'} R_{(k^{-1}j \pmod{p})}(a(\omega \cdot \zeta)) \overline{R_{(\ell^{-1}j \pmod{p})}(b(\omega \cdot \zeta))} \\ \times \exp\left(i(\omega \cdot \zeta) \frac{(k^{-1}j \pmod{p})a - (\ell^{-1}j \pmod{p})b}{p}\right)$$

is a trigonometric polynomial in  $\omega \cdot \zeta$ .

Otherwise, x and y are linearly independent, and we may use Lemma 4 with m = 2 to find  $\zeta_1, \zeta_2$ . Then if  $x = a\zeta_1 + b\zeta_2$ ,  $y = c\zeta_1 + d\zeta_2$ ,

$$(k^{-1}j \pmod{p})x - (\ell^{-1}j \pmod{p})y = [\zeta_1|\zeta_2] \begin{bmatrix} (k^{-1}j \pmod{p})a - (\ell^{-1}j \pmod{p})c \\ (k^{-1}j \pmod{p})b - (\ell^{-1}j \pmod{p})d \end{bmatrix}$$

which is  $\equiv 0 \pmod{p\mathbb{Z}^n}$ , so the latter vector is in  $p\mathbb{Z}^2$ , by property 2 of Lemma 4. This means that the coefficients of  $\omega \cdot \zeta_1$  and  $\omega \cdot \zeta_2$  in the exponential are integers. That is,  $\mathcal{R}_{k,\mu}(\omega) \cdot \mathcal{R}_{\ell,\mu}(\omega)$ , which equals

$$\sum_{j \in I'} R_{(k^{-1}j \pmod{p})}(a(\omega \cdot \zeta_1) + b(\omega \cdot \zeta_2)) \overline{R_{(\ell^{-1}j \pmod{p})}(c(\omega \cdot \zeta_1) + d(\omega \cdot \zeta_2))} \times \exp\left(i[\omega \cdot \zeta_1|\omega \cdot \zeta_2] \left[\frac{(k^{-1}j \pmod{p})a - (\ell^{-1}j \pmod{p})c}{(k^{-1}j \pmod{p})b - (\ell^{-1}j \pmod{p})d}\right]\right)$$

is a bivariate trigonometric polynomial in  $\omega \cdot \zeta_1$ ,  $\omega \cdot \zeta_2$ . This completes the proof.

Combining Theorem 3 with Results 1 and 3, we obtain the prime coset sum method for constructing tight wavelet frames (PCSTF).

**Theorem 4** (PCSTF). Let R be PCSTF-admissible, and let  $\tau$  be the output of PCS with input R in n dimensions. Let  $g_j, 1 \leq j \leq N$  be the sos generators for  $f(\tau; \cdot)$  as guaranteed by Theorem 3. Then, along with  $\tau$ , the following highpass masks form a tight wavelet filter bank:

$$q_{1,\nu}(\omega) := p^{-n/2} \exp(i\nu \cdot \omega) - \tau(\omega) \overline{\tau_{\nu}(p\omega)}, \quad \nu \in \Gamma,$$

$$q_{2,j}(\omega) := \tau(\omega)g_j(p\omega), \quad 1 \le j \le N.$$

Therefore the wavelet system  $\Lambda(\{\psi^{(i)}\})$  (c.f. (3)) is a tight frame for  $L^2(\mathbb{R}^n)$ .

We now specialize Theorem 1 to the tight wavelet frames constructed in Theorem 4.

**Theorem 5** (VMs for PCSTF highpass masks). Let R be PCSTF-admissible, and let  $\tau$  be the output of PCS with input R in n dimensions. Let  $\tau$  have accuracy number a and flatness number b. Then for the highpass masks of Theorem 4,  $q_{1,\nu}, \nu \in \Gamma$  have at least a vanishing moments, and  $q_{2,j}, 1 \leq j \leq N$  have at least min $\{a, \lceil b/2 \rceil\}$  vanishing moments.

In particular, if R has accuracy number m, then the masks  $q_{1,\nu}, \nu \in \Gamma$  have at least m vanishing moments, and  $q_{2,j}, 1 \leq j \leq N$  have at least  $\lceil m/2 \rceil$  vanishing moments.

*Proof.* Since  $\tau$  is interpolatory,  $b \ge a$ . Theorem 3 guarantees the existence of an sos representation for  $f(\tau; \cdot)$ , so we obtain the relations between the vanishing moments of the highpass masks of Theorem 4,  $\{q_{1,\nu} : \nu \in \Gamma\}$ ,  $\{q_{2,j} : 1 \le j \le N\}$ , and a, b immediately from Theorem 1. By Result 5(ii),  $b \ge a \ge m$  (since R is interpolatory), so we obtain the relations between the vanishing moments of these masks and m.

## 4.4. Examples

In this section, we give two examples in the case n = 2, p = 3, demonstrating our method and computing the vanishing moments of the constructed highpass masks. In both cases, the input lowpass mask has flatness and accuracy numbers equal to some positive, even integer, so the lowpass masks constructed from PCS are guaranteed to have the same flatness and accuracy numbers as the input by Corollary 2. We will see that the lower bounds proved in Theorems 1 and 5 are achieved in these examples.

**Example 2.** Let p = 3, and

$$R(\omega) = \frac{1}{9}(3 + 4\cos(\omega) + 2\cos(2\omega)).$$

Then R is PCSTF-admissible. Moreover, it's easy to see that this has accuracy and flatness numbers equal to 2, since  $D^1R(\omega) = -\frac{1}{9}(4\sin(\omega)+4\sin(2\omega))$ , which is equal to 0 at  $\omega \in \{0, \frac{2\pi}{3}, \frac{4\pi}{3}\}$ , and  $D^2R(\omega) = -\frac{1}{9}(4\cos(\omega)+8\cos(2\omega))$ , which equals -4/3 at 0, and equals 2/3 at  $\omega \in \{\frac{2\pi}{3}, \frac{4\pi}{3}\}$ .

Let  $\Gamma = \{-1, 0, 1\}^2$ . Then

$$\tau(\omega) = \frac{1}{9} + \frac{4}{27}(\cos(\omega_1) + \cos(\omega_2) + \cos(\omega_1 + \omega_2) + \cos(\omega_1 - \omega_2)) + \frac{2}{27}(\cos(2\omega_1) + \cos(2\omega_2) + \cos(2(\omega_1 + \omega_2)) + \cos(2(\omega_1 - \omega_2))))$$

Since  $\tau_{-\nu}(\omega) = \overline{\tau_{\nu}(\omega)}$  for  $\nu \in \Gamma'$ , by Lemma 1 and Equation (11), we obtain

$$f(\tau;\omega) = \frac{8}{9} - \frac{1}{6} \sum_{\substack{\nu \in \Gamma' \\ \nu > lex^0}} \left| \sum_{\substack{(\nu',j) \in \mathcal{M}(\nu) \\ \nu' > lex^0}} R_j(\omega \cdot \nu') \exp\left(i\omega \cdot \frac{j\nu' - \nu}{3}\right) \right|^2$$
$$= \frac{8}{9} - \frac{1}{6} \sum_{\substack{\nu \in \Gamma' \\ \nu > lex^0}} |R_1(\omega \cdot \nu) + R_{-1}(\omega \cdot (-\nu))|^2,$$

where we have taken  $I = \{-1, 0, 1\}$ , and we use the Remark after Lemma 3 on the set  $\mathcal{M}(\nu)$  in the last line. Since  $R_1(\omega) = \frac{\sqrt{3}}{9}(2 + \exp(-i\omega))$ , and  $R_{-1}(\omega) = \overline{R_1(\omega)}$ , we have

$$f(\tau;\omega) = \frac{8}{9} - \frac{2}{81} \sum_{\substack{\nu \in \Gamma' \\ \nu >_{\text{lex}} 0}} |2 + \exp(-i\omega \cdot \nu)|^2 = \frac{8}{81} \sum_{\substack{\nu \in \Gamma' \\ \nu >_{\text{lex}} 0}} (1 - \cos(\omega \cdot \nu)),$$

and this yields

$$f(\tau;\omega) = \sum_{\substack{\nu \in \Gamma'\\\nu >_{lex}0}} \left| \frac{2}{9} (1 - \exp(-i\omega \cdot \nu)) \right|^2.$$

Since  $\tau_{\nu}(\omega) = \frac{1}{9}(2 + \exp(-i\omega \cdot \nu))$ , we obtain the highpass filters

$$\begin{aligned} q_{1,0}(\omega) &= \frac{1}{3}(1 - \tau(\omega)), \\ q_{1,\nu}(\omega) &= \frac{1}{3}\exp(i\omega \cdot \nu) - \frac{1}{9}\tau(\omega)(2 + \exp(3i\omega \cdot \nu)) & \nu \in \Gamma', \\ q_{2,\mu}(\omega) &= \frac{2}{9}\tau(\omega)(1 - \exp(3i\omega \cdot \mu)), & \mu \in M, \end{aligned}$$

where  $M = \{e_1, e_2, e_1 + e_2, e_1 - e_2\} = \Gamma' \cap \{k \in \mathbb{Z}^2 : k >_{\text{lex}} 0\}.$ 

One can easily see that the  $q_{2,\mu}$  have exactly 1 vanishing moment. Clearly,  $q_{1,0}$  has 2 vanishing moments (this is just the flatness number for  $\tau$ ). For  $\nu \in \Gamma'$ , we can see that  $q_{1,\nu}(0) = 0$ , and  $D^{\alpha}q_{1,\nu}(0)$ ,  $|\alpha| = 1$  is equal to  $\frac{i\nu^{\alpha}}{3} - \frac{3i\nu^{\alpha}}{9} = 0$ , since  $\tau(0) = 1$ ,  $D^{\alpha}\tau(0) = 0$ . Thus the  $q_{1,\nu}, \nu \in \Gamma'$ , have at least two vanishing moments, and since  $D^{(2,0)}q_{1,\nu}(0) = 2$  for  $\nu \in \{e_1, e_1 + e_2, e_1 - e_2\}$ , and  $D^{(0,2)}q_{1,e_2}(0) = 2$ , we see that these all have exactly two vanishing moments (using  $D^{(2,0)}\tau(0) = D^{(0,2)}\tau(0) = -4/3$ ,  $D^{(1,1)}\tau(0) = 0$ ). Both of these numbers match the lower bound given by Theorem 5. The filter coefficient diagrams for these masks are given in Figures 2 and 3, where the boldface number indicates the origin, and the grid of numbers show the filter coefficients for the corresponding mask in the plane.

Note that the filters for  $q_{1,\nu}, \nu \in \{-e_1, e_2, -e_2\}$  are just the corresponding rotation of  $q_{1,e_1}$  shown in Figure 2c, and the filters for  $q_{1,\nu}, \nu \in \{-(e_1+e_2), e_1-e_2, -(e_1-e_2)\}$  are just the corresponding rotation of  $q_{1,e_1+e_2}$  shown in Figure 2d, so we do not show these additional filters. The same reasoning is used for Figure 3 as well.

1/3	0	1/3	0	1/3	-1/9	0	-1/9	0	-1/9
0	2/3	3 2/3	2/3	0	0	-2/9	-2/9	-2/9	0
1/3	2/3	<b>3</b> 1	2/3	1/3	-1/9	-2/9	8/3	-2/9	-1/9
0	2/3	3 2/3	2/3	0	Ó	-2/9	-2/9	-2/9	Ó
1/3	0	1/3	0	1/3	-1/9	Ó	-1/9	Ó	-1/9
(a) $\tau(\omega)$				(b) $q_{1,(0,0)}(\omega)$					
-1/2	27	0	-1/27	-2/27	-1/27	-2/27	0	-2/	27
0		-2/27	-2/27	-2/27	-4/27	-4/27	-4/27	0	)
-1/2	27	-2/27	-1/9	-4/27	76/27	-2/9	-4/27	-2/	27
0		-2/27	-2/27	-2/27	-4/27	-4/27	-4/27	, O	)
-1/2	27	0	-1/27	-2/27	-1/27	-2/27	0	-2/	27
(c) $q_{1,(1,0)}(\omega)$									
				-2/27	0	-2/27	0	-2/	/27
				0	-4/27	-4/27	-4/27	7 (	)
				-2/27	-4/27	-2/9	-4/27	7 -2/	/27
-1/	27	0	-1/27	0	76/27	-4/27	-4/27	7 (	)
0	)	-2/27	-2/27	-4/27	0	-2/27	0	-2/	/27
-1/	27	-2/27	-1/9	-2/27	-1/27				
0	)	-2/27	-2/27	-2/27	0				
-1/	27	0	-1/27	0	-1/27				
(d) $q_{1,(1,1)}(\omega)$									

Figure 2: Wavelet and lowpass filters from Example 2

Example 3. Let

$$R(\omega) = \frac{1}{243}(81 + 120\cos(\omega) + 60\cos(2\omega) - 10\cos(4\omega) - 8\cos(5\omega)),$$

which is a lowpass mask with prime dilation 3. A calculation reveals that R has accuracy and flatness numbers both equal to 4, and R is clearly interpolatory and PCSTF-admissible. Then letting  $\tau$  be the output of PCS with input R for any choice of n and  $\Gamma$ , Corollary 2 tells us that the accuracy and flatness numbers of  $\tau$  are also both equal to 4.

-2/27	0	-2/27	2/27	-2/27	2/27	0	2/27
0	-4/27	-4/27	-4/27	4/27	4/27	4/27	0
-2/27	-4/27	-2/9	-2/27	2/27	2/9	4/27	2/27
0	-4/27	-4/27	-4/27	4/27	4/27	4/27	0
-2/27	0	-2/27	2/27	-2/27	2/27	0	2/27

(a)  $q_{2,(1,0)}(\omega)$ 

			2/27	0	2/27	0	2/27	
			0	4/27	4/27	4/27	0	
			2/27	4/27	2/9	4/27	2/27	
-2/27	0	-2/27	0	2/27	4/27	4/27	0	
0	-4/27	-4/27	-2/27	0	2/27	0	2/27	
-2/27	-4/27	-2/9	-4/27	-2/27				
0	-4/27	-4/27	-4/27	0				
-2/27	0	-2/27	0	-2/27				
(b) $q_{2,(1,1)}(\omega)$								

Figure 3: Wavelet filters from Example 2

Choosing n = 2 and  $\Gamma = \{-1, 0, 1\}^2$ , we see that

$$\tau(\omega) = \frac{1}{9} + \frac{1}{729} \sum_{\substack{\nu \in \Gamma' \\ \nu >_{\mathrm{lex}} 0}} (120\cos(\omega \cdot \nu) + 60\cos(2\omega \cdot \nu) - 10\cos(4\omega \cdot \nu) - 8\cos(5\omega \cdot \nu)).$$

This gives  $\tau_{\nu}(\omega) = \frac{1}{243}(-5\exp(i\omega\cdot\nu) + 60 + 30\exp(-i\omega\cdot\nu) - 4\exp(-2i\omega\cdot\nu))$  for all  $\nu \in \Gamma'$ , and

$$\begin{split} f(\tau;\omega) &= \frac{40}{3^{10}} \sum_{\substack{\nu \in \Gamma' \\ \nu >_{\text{lex}} 0}} (101 - 138 \cos(\omega \cdot \nu) + 39 \cos(2\omega \cdot \nu) - 2 \cos(3\omega \cdot \nu)) \\ &=: \frac{1}{9} \sum_{\nu \in M} G_{\nu}(\omega), \end{split}$$

where  $M = \{e_1, e_2, e_1 + e_2, e_1 - e_2\}$ . Letting  $\tilde{G}$  be the univariate polynomial such that  $G_{\nu}(\omega) = \tilde{G}(\omega \cdot \nu)$ , we see that  $\tilde{G}(\omega) = \frac{20}{38}(2(1 - \cos(\omega)))^2(31 - 4\cos(\omega))$ , for  $\omega \in \mathbb{T}$ . Moreover, searching for  $\alpha, \beta \in \mathbb{C}$  such that  $|\alpha + \beta \exp(i\omega)|^2 = 31 - 4\cos(\omega)$  yields  $\alpha = (\sqrt{27} + \sqrt{35})/2$  and  $\beta = (\sqrt{27} - \sqrt{35})/2$ . Then, since  $2(1 - \cos(\omega)) = |1 - \exp(i\omega)|^2$ , with  $a = 5\sqrt{7}, b = \sqrt{15}, \tilde{G}(\omega)$  equals

$$\frac{5}{3^8} \left| |1 - \exp(i\omega)|^2 (\sqrt{35} + \sqrt{27} - (\sqrt{35} - \sqrt{27}) \exp(i\omega)) \right|^2$$
$$= \left| \frac{1}{81} \left( (a+3b) \exp(-i\omega) - 3(a+b) + 3(a-b) \exp(i\omega) - (a-3b) \exp(2i\omega) \right) \right|^2.$$

Then the highpass masks satisfying the UEP conditions with  $\tau$  are given by

$$\begin{split} q_{1,\nu}(\omega) &= \frac{1}{3} \exp(i\omega \cdot \nu) - \tau(\omega) \overline{\tau_{\nu}(3\omega)}, \quad \nu \in \Gamma, \\ q_{2,\mu}(\omega) &= \frac{\tau(\omega)}{243} ((a+3b) \exp(3i\omega \cdot \mu) - 3(a+b) + 3(a-b) \exp(-3i\omega \cdot \mu)) \\ &\quad - \frac{\tau(\omega)}{243} (a-3b) \exp(-6i\omega \cdot \mu), \quad \mu \in \{e_1, e_2, e_1 + e_2, e_1 - e_2\} = M. \end{split}$$

We can clearly see that all of the  $q_{2,\mu}$  have exactly 2 vanishing moments by our computation above. The  $q_{1,\nu}$  all have at least 4 vanishing moments, and  $q_{1,0}$  has exactly 4 because this is just the flatness number of  $\tau$ . For  $\nu \in \Gamma'$ , using the calculation in the proof of Proposition 1, when  $|\alpha| = 4$ ,

$$D^{\alpha}q_{1,\nu}(0) = \frac{\nu^{\alpha}}{3} - \overline{D^{\alpha}[\tau_{\nu}(3\omega)]_{\omega=0}} - \frac{1}{3}D^{\alpha}\tau(0),$$

using  $D^{\beta}\tau(0) = \delta(\beta)$  for  $|\beta| \leq 3$ . Since

$$D^{\alpha}\tau_{\nu}(3\omega)|_{\omega=0} = \frac{(3i)^{|\alpha|}\nu^{\alpha}}{243}(-5+30(-1)^{|\alpha|}-4(-2)^{|\alpha|}),$$

which equals  $\nu^{\alpha}(-13)$ , and  $D^{(4,0)}\tau(0) = D^{(0,4)}\tau(0) = -80/3$ , we see that for  $\alpha \in \{(4,0), (0,4)\}, D^{\alpha}q_{1,\nu}(0) = \nu^{\alpha}(40/3) + 80/9$ , which can be made nonzero for some choice of  $\alpha$  in this set for each  $\nu \in \Gamma'$ . Thus the  $q_{1,\nu}$  have exactly 4 vanishing moments for  $\nu \in \Gamma$ .

## 5. Conclusions

In this paper, we developed the prime coset sum method for constructing tight wavelet frames, a novel method for generating nonseparable tight wavelet frames with prime dilation, using the theory of sos representations for nonnegative trigonometric polynomials. We studied the vanishing moments of the wavelets resulting from our method and those of the more general SOSTF of [2], and we proved new results about the accuracy and flatness numbers of lowpass masks arising from the prime coset sum method.

The idea of orbit decompositions and the lemma from lattice theory were used in our setting to decompose  $f(\tau; \cdot)$  into components that could be written as a univariate or bivariate trigonometric polynomial in some appropriate variable or variables. These ideas can be extended to more general dilation matrices than those considered here, and this may be a fruitful approach for finding sos representations in those cases. This is most likely to be successful in cases where there is some symmetry to exploit related to this structure, as there is in the case of PCS-generated lowpass masks. As a simple example, since  $\Gamma$  acts on itself through addition mod  $A\mathbb{Z}^n$ , where A is an integer dilation matrix, taking some additive subgroup  $\langle \mu \rangle$  of  $\Gamma$  generated by a single element  $\mu$ , we obtain a group action of  $\langle \mu \rangle$  on  $\Gamma$ . If the polyphase components of  $\tau$  depend only on a few parameters for the  $\nu$  in a certain orbit, then it may be worthwhile to group the polyphase components in this orbit together when looking for an sos representation of  $f(\tau; \cdot)$ .

There are myriad possibilities for related future work, but some of particular interest to the authors are bounds on the number of sos generators for  $f(\tau; \omega)$  with fixed n and length of support for R, determining conditions for which there are sos representations with real coefficients, and extending the current work to more general dilation matrices. As indicated in the previous paragraph, the last of these investigations is likely to require more detailed study of the lattice  $\mathbb{Z}^n/A\mathbb{Z}^n$ , where A is an integer dilation matrix.

- A. Barvinok. Integer Points in Polyhedra. European Mathematical Society, Zurich, 2008.
- [2] M. Charina, M. Putinar, C. Scheiderer, and J. Stöckler. An algebraic perspective on multivariate tight wavelet frames. *Constructive Approximation*, 38(2):253–276, 2013.
- [3] M. Charina, M. Putinar, C. Scheiderer, and J. Stöckler. An algebraic perspective on multivariate tight wavelet frames. II. Applied and Computational Harmonic Analysis, 39(2):185–213, 2015.
- [4] I. Daubechies. *Ten Lectures on Wavelets*. Society for Industrial and Applied Mathematics, Philadelphia, PA, 1992.
- [5] I. Daubechies, B. Han, A. Ron, and Z. Shen. Framelets: MRA-based constructions of wavelet frames. *Applied and Computational Harmonic Analysis*, 14(1):1–46, 2003.
- [6] L. Evans. *Partial Differential Equations*. American Mathematical Society, Providence, RI, second edition, 2010.
- [7] B. Han. Compactly supported tight wavelet frames and orthonormal wavelets of exponential decay with a general dilation matrix. *Journal of Computational and Applied Mathematics*, 155(1):43–67, 2003.
- [8] Y. Hur and Z. Lubberts. New constructions of nonseparable tight wavelet frames. *Linear Algebra and its Applications*, 534:13–35, 2017.
- [9] Y. Hur and F. Zheng. Coset Sum: An alternative to the tensor product in wavelet construction. *IEEE Transactions on Information Theory*, 59(6):3554–3571, 2013.
- [10] Y. Hur and F. Zheng. Prime coset sum: A systematic method for designing multi-D wavelet filter banks with fast algorithms. *IEEE Transactions on Information Theory*, 62(11):6580–6593, 2016.
- [11] M.-J. Lai and J. Stöckler. Construction of multivariate compactly supported tight wavelet frames. Applied and Computational Harmonic Analysis, 21(3):324–348, 2006.

- [12] A. Ron and Z. Shen. Affine systems in  $L_2(\mathbb{R}^d)$ : The analysis of the analysis operator. Journal of Functional Analysis, 148(2):408–447, 1997.
- [13] C. Scheiderer. Sums of squares on real algebraic surfaces. Manuscripta Mathematica, 119(4):395–410, 2006.