ALGEBRAIC SIGNAL PROCESSING THEORY: COOLEY-TUKEY TYPE ALGORITHMS FOR POLYNOMIAL TRANSFORMS BASED ON INDUCTION*

ALIAKSEI SANDRYHAILA [†], JELENA KOVAČEVIĆ [‡], AND MARKUS PÜSCHEL [§]

Abstract. A *polynomial transform* is the multiplication of an input vector $x \in \mathbb{C}^n$ by a matrix $\mathcal{P}_{b,\alpha} \in \mathbb{C}^{n \times n}$, whose (k, ℓ)-th element is defined as $p_\ell(\alpha_k)$ for polynomials $p_\ell(x) \in \mathbb{C}[x]$ from a list $b = \{p_0(x), \dots, p_{n-1}(x)\}$ and sample points $\alpha_k \in \mathbb{C}$ from a list $\alpha = \{\alpha_0, \dots, \alpha_{n-1}\}$. Such transforms find applications in the areas of signal processing, data compression, and function interpolation. Important examples include the discrete Fourier and cosine transforms. In this paper we introduce a novel technique to derive fast algorithms for polynomial transforms. The technique uses the relationship between polynomial transforms and the representation theory of polynomial algebras. Specifically, we derive algorithms by decomposing the regular modules of these algebras as a stepwise induction. As an application, we derive novel $O(n \log n)$ general-radix algorithms for the discrete Fourier transform and the discrete cosine transform of type 4.

Key words. Polynomial transform, matrix factorization, algebra, module, fast algorithm, fast Fourier transform, discrete Fourier transform, discrete cosine transform, DFT, FFT, DCT, DST.

AMS subject classifications. Primary: 42C05, 42C10, 33C80, 33C90, 65T50, 65T99, 15B99. Secondary: 15A23, 13C05.

1. Introduction.

1.1. Polynomial transforms. Let $b = \{p_0(x), \dots, p_{n-1}(x)\} \subset \mathbb{C}[x]$ be a list[1] of complex polynomials that form a basis of the space of polynomials of degree less than n, and let $\alpha = \{\alpha_0, \dots, \alpha_{n-1}\} \subset \mathbb{C}$ be a list of distinct complex sample points. A *polynomial transform* is the matrix-vector product $\mathcal{P}_{b,\alpha} x$, where $x \in \mathbb{C}^n$ and $\mathcal{P}_{b,\alpha}$ is the $n \times n$ matrix whose (k, ℓ)-th element is defined as $p_\ell(\alpha_k)$, $0 \le k, \ell < n$:

$$\mathcal{P}_{b,\alpha} = \begin{pmatrix} p_0(\alpha_0) & p_1(\alpha_0) & \dots & p_{n-1}(\alpha_0) \\ p_0(\alpha_1) & p_1(\alpha_1) & \dots & p_{n-1}(\alpha_1) \\ \vdots & \vdots & & \vdots \\ p_0(\alpha_{n-1}) & p_1(\alpha_{n-1}) & \dots & p_{n-1}(\alpha_{n-1}) \end{pmatrix}. \tag{1.1}$$

By a slight abuse of notation, we also refer to $\mathcal{P}_{b,\alpha}$ as a polynomial transform.

Polynomial transforms are known in the literature under different names. For example, in [14] and [28], the authors refer to $\mathcal{P}_{b,\alpha}$ as a discrete polynomial transform. In [20], the authors call it a polynomial Vandermonde matrix. The most well-known example of a polynomial transform is the discrete Fourier transform (DFT).

Polynomial transforms have a number of important applications. For example, they are used for interpolation and approximation [17], solving differential equations [6], data compression and image processing [21–24], and the DFT specifically is widely used for spectral analysis and fast computation of correlation and convolution.

---

†Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA 15213 (asandryh@andrew.cmu.edu).

‡Departments of Biomedical Engineering and Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA 15213 (jelenak@cmu.edu).

§Department of Computer Science, ETH Zurich, Switzerland (pueschel@inf.ethz.ch).

[1]Hereafter, we view lists as ordered sets, i.e., without duplicate elements.

The origin and main motivation for our work lies in the *algebraic signal processing theory* [30, 32, 34]. This theory identifies polynomial transforms as equivalent to (generalized) Fourier transforms for shift-invariant 1-D signal models, and establishes a connection between these transforms and the representation theory of polynomial algebras. This connection has been used to algebraically derive many known and new fast algorithms for the DFT and discrete cosine and sine transforms (DCTs and DSTs) [32, 33] extending early ideas by Nussbaumer [27]. All these algorithms are derived and represented as factorizations of the transform matrix into a product of structured matrices with low computational costs.

In this paper, we develop a new algebraic method for a polynomial transform factorization. It is based on viewing the associated polynomial algebra as a regular module and decomposing it into an induction using a chosen subalgebra. This decomposition, performed in steps, yields a factorization of the polynomial transform. If all factors have sufficiently low computational costs, this factorization is a fast algorithm.

Our method extends the approach in [32, 33] to its most general form. As an application, we derive novel fast general-radix algorithms for the DFT and the DCT of type 4.

1.2. Related Work. Over the last decades, decompositions that lead to fast algorithms have been studied for certain polynomial transforms. Among them, the DFT is arguably the most famous and well-studied. The discovery of the Cooley-Tukey fast Fourier transform (FFT) algorithm [11], which reduced the computational cost of DFT_n to $O(n \log n)$ operations, led to decades of research and numerous FFTs (see [40, 41] and the references therein).

Most other polynomial transforms of interest form the class of trigonometric transforms, since their entries are cosine and sine expressions. This class includes the DFT, but also the DCTs and DSTs of various types, as well as the real DFT and the discrete Hartley transform. Fast algorithms with $O(n \log n)$ operations have been developed, for example in [3, 7, 15, 35, 37, 43].

A more general class of polynomial transforms that were studied are those based on orthogonal polynomials [14, 20, 28]. This class includes the DCTs and DSTs but also many other, non-trigonomatric transforms. For those, the best algorithms reported in the literature require $O(n \log^2 n)$ operation.

Among the hundreds of publications on this topic, most derived fast algorithms by clever, but often complicated manipulations of the matrix coefficients. This method provides little insight into the origin and the basic principles that account for the existence of these algorithms.

Another thread of research that we refer to as an algebraic theory of transform algorithms has uncovered these principles for a large class of algorithms for trigonometric transforms [31, 33, 42]. The theory exploits the connection between polynomial transforms and polynomial algebras and uses algebraic techniques to derive algorithms. Using these techniques, most existing algorithms were identified as special cases of two basic theorems, which greatly simplified the derivation and also yielded new algorithms.

The origin of the algebraic approach is in [1, 4, 26, 27], who recognized that the DFT_n can be interpreted as a decomposition matrix for the group algebra $\mathbb{C}[\mathbb{Z}_n]$, where $\mathbb{Z}_n$ is a cyclic group of order n [1, 4]. Since $\mathbb{C}[\mathbb{Z}_n]$ is identical to the polynomial algebra $\mathbb{C}[x]/(x^n - 1)$, this decomposition is

$$\mathbb{C}[\mathbb{Z}_n] \cong \mathbb{C}[x]/(x^n - 1) \to \mathbb{C}[x]/(x - \omega_n^0) \oplus \cdots \oplus \mathbb{C}[x]/(x - \omega_n^{n-1}). \qquad (1.2)$$

Algorithms are now derived by performing this decomposition in steps and reading off the respective matrices, which in turn factorize the DFT.

The group point of view was then generalized to derive fast Fourier transforms for group algebras $\mathbb{C}[G]$ for noncyclic finite groups G [5, 9, 10, 13, 29, 36]. Some of them were based on the induction for group algebras, a construction that is algebraically analogous to the method used in this paper.

The polynomial algebra point of view was extended to derive and study larger classes of FFTs [2, 18, 19, 27, 44].

The extension to the algorithm derivation of the full class of trigonometric transforms and a large class of algorithms was then accomplished in [33, 42] based on early ideas from [38, 39]. Since all these algorithms are based on two theorems that generalize and account for the original Cooley-Tukey FFT, all the algorithms were called "Cooley-Tukey type." The close relation between transforms and algebra was fully developed and explained in the algebraic signal processing theory [32, 34].

In this paper we generalize the main theorem from [33] and hence the class of Cooley-Tukey type algorithms. Specifically, following the discussion in [33], we rigorously demonstrate in Chapter 5 that these algorithms can be viewed as based on a special case of algebraic induction. Then we generalize the construction method to its most general form and show that it produces novel algorithms. As examples, we derive new general-radix algorithms for the DFT and the DCT of type 4.

2. Polynomial algebras and transforms. In this section we discuss polynomial algebras and demonstrate that their decomposition matrices are exactly polynomial transforms. We assume that the reader is familiar with the basic theory of algebras, modules, and matrix representations, even though we strive for a self-contained presentation in this paper. A good introduction to these topics can be found in [12, 16, 17]. Below, we briefly review definitions and important properties.

A vector space that is also a ring is called an *algebra*. In this paper, we work with *polynomial algebras* of the form $\mathcal{A} = \mathbb{C}[x]/p(x)$. Elements of $\mathcal{A}$ are polynomials in x that are added and multiplied modulo $p(x)$. We assume $p(x) = \prod_{k=0}^{n-1}(x - \alpha_k) \in \mathbb{C}[x]$ is a polynomial of degree n and separable, i.e. $\alpha_k \neq \alpha_m$ for $k \neq m$. $\mathcal{A}$ is a commutative algebra of dimension n with a multiplicative identity.

A vector space $\mathcal{M}$ that permits a multiplication by elements of $\mathcal{A}$, such that

$$am \in \mathcal{M} \text{ for any } a \in \mathcal{A}, \ m \in \mathcal{M},$$

is called an $\mathcal{A}$-*module*. The special case $\mathcal{M} = \mathcal{A}$ is called a *regular* module. A subvector space $\mathcal{N} \leq \mathcal{M}$ that is also closed under the multiplication by elements of $\mathcal{A}$, is called an $\mathcal{A}$-*submodule* of $\mathcal{M}$. If $\mathcal{M}$ has only trivial submodules (i.e., $\{0\}$ and itself), it is called *irreducible*.

It follows from the Wedderburn theorem that a regular module $\mathcal{M} = \mathcal{A}$ can be decomposed into a direct sum of irreducible $\mathcal{A}$-modules [12, 16]. This decomposition is accomplished by the Chinese Remainder Theorem:

$$\begin{array}{rcl}
\Delta: & \mathcal{M} & \to & \bigoplus_{k=0}^{n-1} \mathbb{C}[x]/(x - \alpha_k), \\
& s(x) & \mapsto & \begin{pmatrix} s(\alpha_0) & s(\alpha_1) & \ldots & s(\alpha_{n-1}) \end{pmatrix}^T.
\end{array} \tag{2.1}$$

Suppose the basis of $\mathcal{M}$ is a list of polynomials $b = \{p_0(x), \ldots, p_{n-1}(x)\}$, and in each $\mathbb{C}[x]/(x - \alpha_k)$ we choose the basis consisting of 1. Then the matrix that describes the isomorphism (2.1) is precisely the polynomial transform shown in (1.1):

$$\mathcal{P}_{b,\alpha} = [p_\ell(\alpha_k)]_{0 \leq k, \ell < n}. \tag{2.2}$$

Kind	C	C_0, C_1	$C_n(\cos\theta)$	Symmetry	Zeros $(0 \le k < n)$
1st	T	$1, x$	$\cos(n\theta)$	$T_{-n} = T_n$	$\cos\frac{(2k+1)\pi}{2n}$
2nd	U	$1, 2x$	$\frac{\sin(n+1)\theta}{\sin\theta}$	$U_{-n} = -U_{n-2}$	$\cos\frac{(k+1)\pi}{n+1}$
3rd	V	$1, 2x-1$	$\frac{\cos(n+\frac{1}{2})\theta}{\cos\frac{\theta}{2}}$	$V_{-n} = V_{n-1}$	$\cos\frac{(2k+1)\pi}{2n+1}$
4th	W	$1, 2x+1$	$\frac{\sin(n+\frac{1}{2})\theta}{\sin\frac{\theta}{2}}$	$W_{-n} = -W_{n-1}$	$\cos\frac{(2k+2)\pi}{2n+1}$

TABLE 2.1
Chebyshev polynomials, their closed form $C_n(\cos\theta)$, symmetry, and zeros.

Namely, $s(x) = \sum_{\ell=0}^{n-1} s_\ell p_\ell(x) \in \mathcal{M}$ becomes, in coordinate form, the column vector

$$\widehat{s(x)} = \begin{pmatrix} s_0 & s_1 & \dots & s_{n-1} \end{pmatrix}^T,$$

and $\Delta(s(x))$ in (2.1) can be computed as the matrix-vector product

$$\Delta(s(x)) = \mathcal{P}_{b,\alpha} \cdot \widehat{s(x)}. \tag{2.3}$$

EXAMPLE 2.1. If $b = \{1, x, \dots, x^{n-1}\}$ is the standard basis, then the polynomial transform (2.2) is the Vandermonde matrix

$$\mathcal{P}_{b,\alpha} = \left[\alpha_k^\ell\right]_{0 \le k,\ell < n}. \tag{2.4}$$

If, in addition, $p(x) = x^n - 1$, then $\alpha_k = \omega_n^k$, where $\omega_n = e^{-i\frac{2\pi}{n}}$ with $i = \sqrt{-1}$, and the polynomial transform is precisely the discrete Fourier transform

$$\text{DFT}_n = \left[\omega_n^{k\ell}\right]_{0 \le k,\ell < n}. \tag{2.5}$$

EXAMPLE 2.2. If $b = \{T_0(x), \dots, T_{n-1}(x)\}$ is the basis consisting of the Chebyshev polynomials of the first kind[2], then the polynomial transform has the form

$$\mathcal{P}_{b,\alpha} = [T_\ell(\alpha_k)]_{0 \le k,\ell < n}. \tag{2.6}$$

If, in addition, $p(x) = T_n(x)$, then $\alpha_k = \cos\frac{(2k+1)\pi}{2n}$ (see Table 2.1), and the polynomial transform is the discrete cosine transform of type 3 [35]:

$$\text{DCT-3}_n = \left[\cos\frac{(2k+1)\ell\pi}{2n}\right]_{0 \le k,\ell < n}. \tag{2.7}$$

Scaled polynomial transforms. The notion of a polynomial transform can be generalized by allowing a different choice of a basis in the $\mathbb{C}[x]/(x - \alpha_k)$ in (2.1). Namely, if we choose the basis $\{1/c_k\}, c_k \in \mathbb{C} \setminus \{0\}$, in each $\mathbb{C}[x]/(x - \alpha_k)$, then (2.2) becomes the *scaled polynomial transform*

$$\mathcal{P}'_{b,\alpha} = \text{diag}\left(c_0, c_1, \dots, c_{n-1}\right) \cdot \mathcal{P}_{b,\alpha}, \tag{2.8}$$

---

[2]Chebyshev polynomials C_k are the polynomials that satisfy the three-term recurrence $C_{k+1} = 2xC_k - C_{k-1}$ [25]. Hence, the whole sequence of polynomials is determined by C_0 and C_1. By setting $x = \cos\theta$, Chebyshev polynomials can also be expressed in their trigonometric closed form as functions of θ. These and other properties are shown in Table 2.1.

	$p(x)$			
C	$C_n(x)$	$C_n(x) - C_{n-2}(x)$	$C_n(x) - C_{n-1}(x)$	$C_n(x) + C_{n-1}(x)$
T	DCT-3, $\;1$	DCT-1, $\;1$	DCT-5, $\;1$	DCT-7, $\;1$
U	DST-1, $\;\sin\frac{(k+1)\pi}{n+1}$	DST-3, $\;\sin\frac{(2k+1)\pi}{2n}$	DST-7, $\;\sin\frac{(2k+1)\pi}{2n+1}$	DST-5, $\;\sin\frac{(2k+1)\pi}{2n+2}$
V	DCT-8, $\;\cos\frac{(2k+1)\pi}{4n+2}$	DCT-6, $\;\cos\frac{k\pi}{2n-1}$	DCT-2, $\;\cos\frac{k\pi}{2n}$	DCT-4, $\;\cos\frac{(2k+1)\pi}{4n}$
W	DST-6, $\;\sin\frac{(k+1)\pi}{2n+1}$	DST-8, $\;\sin\frac{(2k+1)\pi}{4n-2}$	DST-4, $\;\sin\frac{(2k+1)\pi}{4n}$	DST-2, $\;\sin\frac{(k+1)\pi}{2n}$

TABLE 2.2

16 types of discrete cosine and sine transforms as scaled polynomial transforms (2.8). Corresponding polynomial algebras are $\mathbb{C}[x]/p(x)$ with basis $b = \{C_0(x), \ldots, C_{n-1}(x)\}$, and $p(x) \in \{C_n(x), C_n(x) - C_{n-2}(x), C_n(x) - C_{n-1}(x), C_n(x) + C_{n-1}(x)\}$. The coefficients c_k are specified after the transform name.

with $\mathcal{P}_{b,\alpha}$ as defined in (2.2).

EXAMPLE 2.3. Let $p(x) = V_n(x) + V_{n-1}(x) = 2T_n(x)$, and choose the basis $b = \{V_0(x), \ldots, V_{n-1}(x)\}$ in $\mathcal{M}$, where $V_\ell(x)$ is the ℓ-th Chebyshev polynomial of the third kind. If we choose $c_k = \cos\frac{(k+1/2)\pi}{2n}$, then the associated scaled polynomial transform is the discrete cosine transform of type 4:

$$
\begin{aligned}
\mathcal{P}_{b,\alpha} &= \operatorname{diag}_{0 \le k < n}\left(\cos\frac{(k+1/2)\pi}{2n}\right) \cdot \left[\frac{\cos\frac{(k+1/2)(\ell+1/2)\pi}{n}}{\cos\frac{(k+1/2)\pi}{2n}}\right]_{0 \le k, \ell < n} \\
&= \left[\cos\frac{(k+1/2)(\ell+1/2)\pi}{n}\right]_{0 \le k, \ell < n} \\
&= \text{DCT-4}_n \, .
\end{aligned}
$$

Note that all 16 types of discrete sine and cosine transforms are scaled or unscaled polynomial transforms with bases consisting of Chebyshev polynomials [32]. They are summarized in Table 2.2.

3. Subalgebra and its structure. In this section we discuss the structure of subalgebras of $\mathcal{A} = \mathbb{C}[x]/p(x)$.

3.1. Definition. Choose a polynomial $r(x) \in \mathcal{A}$, and consider the space of polynomials in $r(x)$ with addition and multiplication modulo $p(x)$:

$$
\mathcal{B} = \left\{ \sum_{k \ge 0} c_k r^k(x) \mod p(x) \mid c_k \in \mathbb{C} \right\}, \tag{3.1}
$$

where all sums are finite. We call $\mathcal{B}$ the *subalgebra* of $\mathcal{A}$ *generated* by $r(x)$ and write $\mathcal{B} = \langle r(x) \rangle \le \mathcal{A}$.

3.2. Structure. Given $r(x) \in \mathcal{A}$, we first determine the dimension of $\mathcal{B} = \langle r(x) \rangle$. Then we identify $\mathcal{B}$ with a polynomial algebra of the form $\mathbb{C}[y]/q(y)$ with a suitably chosen polynomial $q(y)$.

Let $\alpha = \{\alpha_0, \ldots, \alpha_{n-1}\}$ be the list of roots of $p(x)$. The generator $r(x)$ maps α to the list $\beta = \{\beta_0, \ldots, \beta_{m-1}\}$, such that for each $\alpha_k \in \alpha$ there is a $\beta_j \in \beta$, for which $r(\alpha_k) = \beta_j$. Hence, $m \le n$, since for some k and ℓ we may have $r(\alpha_k) = r(\alpha_\ell)$.

THEOREM 3.1. *The dimension of $\mathcal{B} = \langle r(x) \rangle$ is $\dim \mathcal{B} = m = |\beta|$.*

Proof. Let $d = \dim \mathcal{B}$. Since $\mathcal{B} \leq \mathcal{A}$, $d \leq \dim \mathcal{A} = n$ and the polynomials $\{1, r(x), \ldots, r^{n-1}(x)\}$ span $\mathcal{B}$. From the isomorphism (2.1) we obtain

$$d = \operatorname{rank}\left(\Delta(1), \Delta(r(x)), \ldots, \Delta(r^{n-1}(x))\right)$$
$$= \operatorname{rank}\left[r^\ell(\alpha_k)\right]_{0 \leq k, \ell < n}.$$

Since $r(\alpha_k) \in \beta$ and $|\beta| = m$, the above matrix has only m different rows; hence, $d \leq m$. On the other hand, it contains the full-rank $m \times m$ Vandermonde matrix

$$\left[\beta_j^\ell\right]_{0 \leq j, \ell < m}$$

as a submatrix; hence, $d \geq m$. Thus, we conclude that $d = \dim \mathcal{B} = m$. □

Next, we identify $\mathcal{B}$ with a polynomial algebra.

THEOREM 3.2. *The subalgebra $\mathcal{B} = \langle r(x) \rangle$ can be identified with the polynomial algebra $\mathbb{C}[y]/q(y)$, where $q(y) = \prod_{j=0}^{m-1} (y - \beta_j)$, via the following canonical isomorphism of algebras:*

$$\kappa : \quad \begin{array}{ccc} \mathcal{B} & \to & \mathbb{C}[y]/q(y), \\ r(x) & \mapsto & y. \end{array} \tag{3.2}$$

We indicate this canonical isomorphism as $\mathcal{B} \cong \mathbb{C}[y]/q(y)$.

Proof. Observe that $\mathcal{B}$ and $\mathbb{C}[y]/q(y)$ have the same dimension m, and κ maps the generator $r(x)$ of $\mathcal{B}$ to the generator y of $\mathbb{C}[y]/q(y)$. Hence, it suffices to show that $q(r(x)) \equiv 0 \mod p(x)$ in $\mathcal{B}$. From (2.1) we obtain

$$\Delta(q(r(x))) = \left(q(r(\alpha_0)) \quad \ldots \quad q(r(\alpha_{n-1}))\right)^T$$
$$= \left(0 \quad \ldots \quad 0\right)^T,$$

which implies that $q(r(x)) \equiv 0 \mod p(x)$ in $\mathcal{A}$, and hence in $\mathcal{B}$. □

Let $c = \{q_0(y), \ldots, q_{m-1}(y)\}$ be a basis of $\mathbb{C}[y]/q(y)$. The polynomial transform (2.2) that decomposes the regular module $\mathbb{C}[y]/q(y)$ (and hence the regular $\mathcal{B}$-module $\mathcal{B}$) is given by (2.1) as

$$\mathcal{P}_{c,\beta} = [q_\ell(\beta_j)]_{0 \leq j, \ell < m}.$$

EXAMPLE 3.3.   Consider the polynomial algebra $\mathcal{A} = \mathbb{C}[x]/(x^4 - 1)$ with $\alpha = \{1, -i, -1, i\}$. The polynomial $r_1(x) = x^2$ generates the subalgebra $\mathcal{B}_1 = \langle r_1(x) \rangle \cong \mathbb{C}[y]/(y^2 - 1)$ of dimension 2, since $r_1(x)$ maps α to $\beta = \{1, -1\}$.

The polynomial $r_2(x) = (x + x^{-1})/2 = (x + x^3)/2$ generates the subalgebra $\mathcal{B}_2 = \langle r_2(x) \rangle \cong \mathbb{C}[y]/(y^3 - y)$ of dimension 3, since $r_2(x)$ maps α to $\beta = \{1, 0, -1\}$.

4. Module induction. In this section we introduce the concept of *module induction*, which constructs an $\mathcal{A}$-module $\mathcal{M}$ from a $\mathcal{B}$-module $\mathcal{N}$, where $\mathcal{B} \leq \mathcal{A}$ is a subalgebra. We show that every regular $\mathcal{A}$-module is an induction, which is the basis of our technique for polynomial transform decomposition.

4.1. Induction. Similar to the coset decomposition in group theory [12, 16], we can decompose a polynomial algebra $\mathcal{A} = \mathbb{C}[x]/p(x)$ using a subalgebra $\mathcal{B}$ and associated *transversal*:

DEFINITION 4.1 (Transversal). *Let $\mathcal{B} \le \mathcal{A}$ be a subalgebra of $\mathcal{A}$. A* transversal *of $\mathcal{B}$ in $\mathcal{A}$ is a list of polynomials $T = \{t_0(x), \ldots, t_{L-1}(x)\} \subset \mathcal{A}$, such that, as vector spaces,*

$$\mathcal{A} = \bigoplus_{\ell=0}^{L-1} t_\ell(x)\mathcal{B} = t_0(x)\mathcal{B} \oplus \cdots \oplus t_{L-1}(x)\mathcal{B}. \tag{4.1}$$

Later, in Theorem 4.6, we establish necessary and sufficient conditions for a list of polynomials to be a transversal of $\mathcal{B}$ in $\mathcal{A}$. In particular, for any $\mathcal{B} \le \mathcal{A}$ there always exists a transversal.

Given a transversal of $\mathcal{B}$ in $\mathcal{A}$, we define the module induction, which is analogous to the induction for group algebras [12].

DEFINITION 4.2 (Induction). *Let $\mathcal{B} \le \mathcal{A}$ be a subalgebra of $\mathcal{A}$ with a transversal T as in (4.1), and let $\mathcal{N}$ be a $\mathcal{B}$-module. Then the following construction is an $\mathcal{A}$-module:*

$$\mathcal{M} = \bigoplus_{\ell=0}^{L-1} t_\ell(x)\mathcal{N}, \tag{4.2}$$

where the direct sum is again of vector spaces. It is called the induction *of the $\mathcal{B}$-module $\mathcal{N}$ with the transversal T to an $\mathcal{A}$-module. We write this as $\mathcal{M} = \mathcal{N} \uparrow_T \mathcal{A}$.*

In this paper, we are primarily interested in regular modules. These are always inductions, as follows directly from (4.1) and (4.2):

LEMMA 4.3. *Let $\mathcal{B} \le \mathcal{A}$ with a transversal T. Then the regular module $\mathcal{A}$ is an induction of the regular module $\mathcal{B}$:*

$$\mathcal{A} = \mathcal{B} \uparrow_T \mathcal{A}. \tag{4.3}$$

4.2. Structure of cosets. We have established in (3.2) that the subalgebra $\mathcal{B} \le \mathcal{A}$, generated by $r(x) \in \mathcal{A}$, can be identified with a polynomial algebra $\mathbb{C}[y]/q(y)$. Next, we investigate the structure of each $\mathcal{B}$-module $t_\ell(x)\mathcal{B}$ in the induction (4.3).

Consider a polynomial $t(x) \in \mathcal{A}$. As in Theorem 3.2, let $r(x)$ map α to β, and let $q(y) = \prod_{j=0}^{m-1} (y - \beta_j)$. Further, let $\alpha' = \{\alpha_k \mid t(\alpha_k) \ne 0\} \subseteq \alpha$ be the sublist of α that consists of those α_k that are not roots of $t(x)$. Finally, let $r(x)$ map α' to $\beta' \subseteq \beta$, and denote $|\beta'| = m'$.

THEOREM 4.4. *The dimension of $t(x)\mathcal{B}$ is $\dim t(x)\mathcal{B} = |\beta'| = m'$.*

Proof. The proof is similar to that of Theorem 3.1. The list of polynomials $\{t(x), t(x)r(x), \ldots, t(x)r^{n-1}(x)\}$ generates $t(x)\mathcal{B}$ as a vector space. Using the isomorphism Δ in (2.1) we obtain

$$\begin{aligned}
\dim\big(t(x)\mathcal{B}\big) &= \operatorname{rank}\big(\Delta(t(x)), \Delta(t(x)r(x)), \ldots, \Delta(t(x)r^{n-1}(x))\big) \\
&= \operatorname{rank}\big[t(\alpha_k)r^\ell(\alpha_k)\big]_{0 \le k, \ell < n} \\
&= \operatorname{rank}\Big(\operatorname{diag}\big(t(\alpha_k)\big)_{0 \le k < n} \cdot \big[r^\ell(\alpha_k)\big]_{0 \le k, \ell < n}\Big).
\end{aligned} \tag{4.4}$$

Theorem 3.2 shows that $\big[r^\ell(\alpha_k)\big]_{0 \le k, \ell < n}$ has exactly $m = |\beta|$ linearly independent rows of the form

$$\begin{pmatrix} 1 & \beta_j & \beta_j^2 & \ldots & \beta_j^{n-1} \end{pmatrix}.$$

For each β_j, the above row contributes exactly 1 to the rank of the matrix (4.4) if and only if there exists α_k such that $t(\alpha_k) \neq 0$ and $r(\alpha_k) = \beta_j$. Since there are exactly $|\beta'| = m'$ such values of β_j, we conclude that $\dim\big(t(x)\mathcal{B}\big) = m'$. $\square$

Next, we identify the $\mathcal{B}$-module $t(x)\mathcal{B}$ with a $\mathbb{C}[y]/q(y)$-module.

THEOREM 4.5. *The $\mathcal{B}$-module $t(x)\mathcal{B}$ can be identified with the $\mathbb{C}[y]/q(y)$-module* $\mathbb{C}[y]/q'(y)$, *where* $q'(y) = \prod_{\beta_j \in \beta'}(y - \beta_j)$, *via the module isomorphism*

$$\eta: \quad \begin{aligned} t(x)\mathcal{B} &\rightarrow \mathbb{C}[y]/q'(y), \\ t(x)r^k(x) &\mapsto y^k. \end{aligned} \tag{4.5}$$

By a slight abuse of notation, we write $t(x)\mathcal{B} \cong \mathbb{C}[y]/q'(y)$. *This is an isomorphism of modules and should not be confused with the isomorphism of algebras in Theorem 3.2.*

Proof. It follows from Theorem 4.4 that $\big\{t(x), t(x)r(x), \ldots, t(x)r^{m'-1}(x)\big\}$ is a basis of $t(x)\mathcal{B}$. On the other hand, $\big\{1, y, \ldots, y^{m'-1}\big\}$ is obviously a basis of $\mathbb{C}[y]/q'(y)$. Hence, η in (4.5) is a bijective linear mapping between $t(x)\mathcal{B}$ and $\mathbb{C}[y]/q'(y)$.

For η to be an isomorphism of modules, it must also be a module homomorphism, i.e., it must preserve the addition and multiplication in $t(x)\mathcal{B}$ and $\mathbb{C}[y]/q'(y)$. Namely, for $h(x) \in \mathcal{B}$ and $u(x), v(x) \in t(x)\mathcal{B}$, the following conditions must hold:

$$\eta\big(u(x) + v(x)\big) = \eta(u(x)) + \eta(v(x)),$$
$$\eta\big(h(x)v(x)\big) = \kappa(h(x)) \cdot \eta(v(x)).$$

The first condition is trivial. To show that the second condition holds, let $h(x) = \sum_{k=0}^{m-1} h_k r^k(x) \in \mathcal{B}$ and $v(x) = \sum_{j=0}^{m'-1} v_j t(x) r^j(x) \in t(x)\mathcal{B}$. Then

$$\eta\big(h(x)v(x)\big) = \eta\left(\sum_{j=0}^{m+m'-2}\sum_{k=0}^{j} h_k v_{j-k} t(x) r^j(x)\right) = \sum_{j=0}^{m+m'-2}\sum_{k=0}^{j} h_k v_{j-k} y^j$$

$$= \sum_{k=0}^{m-1} h_k y^k \cdot \sum_{j=0}^{m'-1} v_j y^j = \kappa(h(x)) \cdot \eta(v(x)).$$

Hence, η is a module isomorphism. $\square$

Note that, depending on $t(x)$, the dimension of $t(x)\mathcal{B}$ may be smaller than the dimension of $\mathcal{B}$: $m' \leq m$. This effect is called *annihilation*.

Also, the definition of η in (4.5) assumes the standard basis $\big\{1, y, \ldots, y^{m'-1}\big\}$ in $\mathbb{C}[y]/q'(y)$. If another basis $\big\{b_0(y), \ldots, b_{m'-1}(y)\big\}$ were desired, the corresponding basis in $t(x)\mathcal{B}$ would be $\big\{t(x)b_0(r(x)), \ldots, t(x)b_{m'-1}(r(x))\big\}$.

As a consequence of Theorem 4.5 and the above discussion, decomposing the $\mathcal{B}$-module $t(x)\mathcal{B}$ with basis $\big\{t(x)q_0(r(x)), \ldots, t(x)q_{m'-1}(r(x))\big\}$ is the same as decomposing the $\mathbb{C}[y]/q(y)$-module $\mathbb{C}[y]/q'(y)$ with basis $c = \big\{q_0(y), \ldots, q_{m'-1}(y)\big\}$. The decomposition matrix is the same as for the regular module $\mathbb{C}[y]/q'(y)$ with the same basis, namely

$$\mathcal{P}_{c,\beta'} = [q_\ell(\beta_j)]_{0 \leq j, \ell < m'}. \tag{4.6}$$

4.3. Existence of a transversal. Consider $T = \big\{t_0(x), \ldots, t_{L-1}(x)\big\} \subset \mathcal{A}$, and let $\dim\big(t_\ell(x)\mathcal{B}\big) = m_\ell$ for $0 \leq \ell < L$. Then $\big\{t_\ell(x), t_\ell(x)r(x), \ldots, t_\ell(x)r^{m_\ell-1}(x)\big\}$ is a basis of $t_\ell(x)\mathcal{B}$, as follows from Theorem 4.4. Hence, T satisfies (4.1) if and only if $m_0 + \cdots + m_{L-1} = n$ and the concatenation of bases

$$b' = \bigcup_{\ell=0}^{L-1} \left\{ t_\ell(x), \ldots, t_\ell(x) r^{m_\ell-1}(x) \right\} \tag{4.7}$$

is a basis in $\mathcal{A}$. The following theorem states this condition in a matrix form.

THEOREM 4.6. *Using previous notation, T is a transversal if and only if the following is a full-rank $n \times n$ matrix:*

$$M' = \begin{pmatrix} D_0 B_0 & | & D_1 B_1 & | & \ldots & | & D_{L-1} B_{L-1} \end{pmatrix}, \tag{4.8}$$

where $D_\ell = \mathrm{diag} \left(t_\ell(\alpha_k) \right)_{0 \le k < n}$, and $B_\ell = \left[r^j(\alpha_k) \right]_{0 \le k < n, 0 \le j < m_\ell}$.

Proof. The proof is similar to the proofs of Theorems 3.1 and 4.4. Observe that the k-th element of b' in (4.7) is mapped to the k-th column of M' in (4.8) by the isomorphism Δ in (2.1). Hence, b' is a basis in $\mathcal{A}$ if and only if M' has exactly n columns and rank $M' = n$. $\square$

It follows from Theorem 4.6 that for any algebra $\mathcal{A}$ and its subalgebra $\mathcal{B}$ there always exists a transversal. For example, we can choose $T = \{ t_0(x), \ldots, t_{n-1}(x) \}$, where $t_\ell(\alpha_k) = 0$ for $\ell \ne k$ and $t_\ell(\alpha_\ell) \ne 0$. In this case $M' = \mathrm{diag} \left(t_\ell(\alpha_\ell) \right)_{0 \le \ell < n}$ in (4.8) is a full-rank diagonal matrix.

EXAMPLE 4.7. Consider the subalgebras constructed in Example 3.3.

For $\mathcal{B}_1 = \left\langle x^2 \right\rangle$ of dimension 2, we can choose the transversal $T = \{1, x\}$, since $\{1, x^2\} \cup \{x, x^3\}$ is a basis for $\mathcal{A}$. Since x maps α to $\{1, -i, -1, i\}$, we have $\alpha' = \{1, -i, -1, i\}$ and $\beta' = \{1, -1\}$. Hence, $q'(y) = (y-1)(y+1)$ and $x\mathcal{B}_1 \cong \mathbb{C}[y]/(y^2-1)$ is of dimension 2.

For $\mathcal{B}_2 = \left\langle (x + x^{-1})/2 \right\rangle$ of dimension 3, we can choose the transversal $T = \{1, (x - x^{-1})/2\}$, since the corresponding matrix

$$M' = \begin{pmatrix} 1 & & 1 & 1 & \\ 1 & & & & -i \\ 1 & & -1 & 1 & \\ 1 & & & & i \end{pmatrix}$$

from (4.8) has full rank. Since $(x - x^{-1})/2$ maps α to $\{0, -i, 0, i\}$, we obtain $\alpha' = \{-i, i\}$, $\beta' = \{0\}$, and thus $q'(y) = y$. Hence, $(x - x^{-1})/2 \cdot \mathcal{B}_2 \cong \mathbb{C}[y]/y$ is of dimension 1.

5. Decomposition of polynomial transforms using induction. In this section we use the induction (4.3) to express the polynomial transform of $\mathcal{A}$ via the polynomial transforms of each $t_\ell(x)\mathcal{B} \cong \mathbb{C}[y]/q'_\ell(y)$ in (4.1). As before, we consider $\mathcal{A} = \mathbb{C}[x]/p(x)$, where $p(x) = \prod_{k=0}^{n-1}(x - \alpha_k)$. We view it as a regular $\mathcal{A}$-module with the chosen basis $b = \{ p_0(x), \ldots, p_{n-1}(x) \}$.

Let $\mathcal{B} = \left\langle r(x) \right\rangle \le \mathcal{A}$ be the subalgebra generated by $r(x) \in \mathcal{A}$, and $\mathcal{B} \cong \mathbb{C}[y]/q(y)$ using Theorem 3.2, where $q(y) = \prod_{j=0}^{m-1}(y - \beta_j)$ and $\beta = \{ \beta_0, \ldots, \beta_{m-1} \}$.

Suppose $T = \{ t_0(x), \ldots, t_{L-1}(x) \}$ is a transversal of $\mathcal{B}$ in $\mathcal{A}$. Let each $t_\ell(x)\mathcal{B}$ in (4.1) be identified with a $\mathbb{C}[y]/q(y)$-module $\mathbb{C}[y]/q^{(\ell)}(y)$ using Theorem 4.5, where $q^{(\ell)}(y) = \prod_{\beta_j \in \beta^{(\ell)}}(y - \beta_j)$ and $m_\ell = |\beta^{(\ell)}|$. The basis $b^{(\ell)} = \{ b_0^{(\ell)}(y), \ldots, b_{m_\ell-1}^{(\ell)}(y) \}$ of $\mathbb{C}[y]/q^{(\ell)}(y)$ corresponds to the basis $\{ t_\ell(x)b_0^{(\ell)}(r(x)), \ldots, t_\ell(x)b_{m_\ell-1}^{(\ell)}(r(x)) \}$ of $t_\ell(x)\mathcal{B}$. Hence, the corresponding polynomial transform (4.6) is $\mathcal{P}_{b^{(\ell)}, \beta^{(\ell)}}$.

THEOREM 5.1. *Given the induction (4.3), the polynomial transform $\mathcal{P}_{b,\alpha}$ can be decomposed as*

$$\mathcal{P}_{b,\alpha} = \left(D_0 M_0 \quad | \quad D_1 M_1 \quad | \quad ... \quad | \quad D_{L-1} M_{L-1}\right) \left(\bigoplus_{\ell=0}^{L-1} \mathcal{P}_{b^{(\ell)},\beta^{(\ell)}}\right) B. \qquad (5.1)$$

Here, B is the base change matrix from the basis b to the concatenation of bases

$$\bigcup_{\ell=0}^{L-1} \{t_\ell(x) b_0^{(\ell)}(r(x)), \dots, t_\ell(x) b_{m_\ell-1}^{(\ell)}(r(x))\}.$$

Each $D_\ell = \mathrm{diag}\left(t_\ell(\alpha_k)\right)_{0 \le k < n}$ is a diagonal matrix. Each M_ℓ is an $n \times m_\ell$ matrix whose (k,j)-th element is 1 if $r(\alpha_k)$ is equal to the j-th element of $\beta^{(\ell)}$, and 0 otherwise. $\oplus$ denotes the direct sum of matrices:

$$\bigoplus_{\ell=0}^{L-1} \mathcal{P}_{b^{(\ell)},\beta^{(\ell)}} = \begin{pmatrix} \mathcal{P}_{b^{(0)},\beta^{(0)}} & & & \\ & \mathcal{P}_{b^{(1)},\beta^{(1)}} & & \\ & & \ddots & \\ & & & \mathcal{P}_{b^{(L-1)},\beta^{(L-1)}} \end{pmatrix}.$$

Proof. We prove the theorem for $L = 2$; that is, for $\mathcal{A} = t_0(x)\mathcal{B} \oplus t_1(x)\mathcal{B}$. The proof for arbitrary L is analogous.

Let $\mathcal{B} \cong \mathbb{C}[y]/q(y)$ according to Theorem 3.2, where $q(y) = \prod_{j=0}^{m-1}(y - \beta_j)$ and $\beta = \{\beta_0, \dots, \beta_{m-1}\}$. For $\ell \in \{0,1\}$, let $t_\ell(x)\mathcal{B} \cong \mathbb{C}[y]/q^{(\ell)}(y)$ according to Theorem 4.5, where $q^{(\ell)}(y) = \prod_{\beta_j \in \beta^{(\ell)}}(y - \beta_j)$ and $m_\ell = |\beta^{(\ell)}|$. Let $b^{(\ell)} = \{b_0^{(\ell)}(y), \dots, b_{m_0-1}^{(\ell)}(y)\}$ be a basis of $\mathbb{C}[y]/q^{(\ell)}(y)$.

Let $t_\ell(x)b^{(\ell)}(r(x)) = \{t_\ell(x)b_0^{(\ell)}(r(x)), \dots, t_\ell(x)b_{m_0-1}^{(\ell)}(r(x))\}$. As we established in Theorem 4.6, $b' = t_0(x)b^{(0)}(r(x)) \bigcup t_1(x)b^{(1)}(r(x))$ is a basis of $\mathcal{A}$. The original basis b can be expressed in the new basis b' as $p_k(x) = \sum_{\ell=0}^{m_0-1} B_{k,\ell} t_0(x) b_\ell^{(0)}(r(x)) + \sum_{\ell=0}^{m_1-1} C_{k,\ell} t_1(x) b_\ell^{(1)}(r(x))$. Hence, if B is the base change matrix from b to b', then

$$\mathcal{P}_{b,\alpha} = \mathcal{P}_{b',\alpha} \cdot B. \qquad (5.2)$$

The ℓ-th column of B is $(B_{0,\ell}, \dots, B_{m_0-1,\ell}, C_{0,\ell}, \dots, C_{m_1-1,\ell})^T$.

Next, observe that

$$\mathcal{P}_{b',\alpha} = \left(\mathcal{P}_{t_0(x)b^{(0)}(r(x)),\alpha} \mid \mathcal{P}_{t_1(x)b^{(1)}(r(x)),\alpha}\right). \qquad (5.3)$$

For each ℓ, the (k,j)-th element of $\mathcal{P}_{t_\ell(x)b^{(\ell)}(r(x)),\alpha}$ is $t_\ell(\alpha_k)b_j^{(\ell)}(r(\alpha_k))$. Hence,

$$\mathcal{P}_{t_\ell(x)b^{(\ell)}(r(x)),\alpha} = D_\ell \cdot M_\ell \cdot \mathcal{P}_{b^{(\ell)},\beta^{(\ell)}}, \qquad (5.4)$$

where M_ℓ is an $n \times m_\ell$ matrix whose (k,j)-th element is 1 if $r(\alpha_k)$ equals to the j-th element of $\beta^{(\ell)}$, and 0 otherwise; and $D_\ell = \mathrm{diag}\left(t_\ell(\alpha_k)\right)_{0 \le k \le n-1}$.

Hence, from (5.2-5.4) we obtain the desired decomposition:

$$\mathcal{P}_{b,\alpha} = \left(D_0 M_0 \mid D_1 M_1\right) \cdot \left(\mathcal{P}_{b^{(0)},\beta^{(0)}} \oplus \mathcal{P}_{b^{(1)},\beta^{(1)}}\right) \cdot B. \qquad (5.5)$$

□

COROLLARY 5.2. *Consider the $n \times m$ matrix M whose (k,j)-th element is 1 if $r(\alpha_k) = \beta_j$ and 0 otherwise. Then*

1. M contains exactly n 1s and $n(m-1)$ 0s .
2. Each matrix M_ℓ in Theorem 5.1 is a submatrix of M. It contains the j-th column of M if and only if $\beta_j \in \beta^{(\ell)}$.
3. If the number of non-zero elements in the j-th column of M is c_j, then there are precisely c_j matrices among $M_0, \ldots, M_{L-1}$ that contain this column.

Discussion. The three factors in (5.1) correspond to the decomposition (2.1) of the regular module $\mathcal{A} = \mathcal{M} = \mathbb{C}[x]/p(x)$ in three steps:

Step 1. $\mathcal{A}$ is represented as an induction (4.3) by changing the basis in $\mathcal{A}$ to the concatenation of bases $b^{(\ell)}$ of $t_\ell(x)\mathcal{B}$, using the base change matrix B.

Step 2. Each $t_\ell(x)\mathcal{B}$ is decomposed into a direct sum of irreducible $\mathcal{B}$-submodules, using the corresponding polynomial transform $\mathcal{P}_{b^{(\ell)},\beta^{(\ell)}}$.

Step 3. The resulting direct sum of irreducible $\mathcal{B}$-modules is decomposed into a direct sum of irreducible $\mathcal{A}$-modules, using the matrix M.

The factorization (5.1) is a fast algorithm for $\mathcal{P}_{b,\alpha}$ if the matrices B and M have sufficiently low costs, since the recursive nature of the second step allows for repeated application of Theorem 5.1. We illustrate this with two examples of novel algorithms derived using this theorem in Section 6.

Special case: decomposition of $p(x)$. A special case of Theorem 5.1 has been derived in [31,33]. Namely, assume that $\mathcal{A} = \mathbb{C}[x]/p(x)$, and we can decompose $p(x) = q(r(x))$. Then $\mathcal{B} = \langle r(x) \rangle \cong \mathbb{C}[y]/q(y)$, and any basis $t = \{1, t_1(x), \ldots, t_{k-1}(x)\}$ of $\mathbb{C}[x]/r(x)$ is a transversal of $\mathcal{B}$ in $\mathcal{A}$. This leads to the following result.

COROLLARY 5.3. *Choose* $c = \{c_0(y), \ldots, c_{m-1}(y)\}$ *as the basis of* $\mathbb{C}[y]/q(y)$. *Denote the roots of* $r(x) - \beta_j$ *as* $\gamma^{(j)} = \{\gamma_0^{(j)}, \ldots, \gamma_{k-1}^{(j)}\}$. *Notice that* $\bigcup_{j=0}^{m-1} \{\gamma_0^{(j)}, \ldots, \gamma_{k-1}^{(j)}\}$ *is simply a permutation of* $\{\alpha_0, \ldots, \alpha_{n-1}\}$, *and denote the corresponding permutation matrix as* P. *Then, the polynomial transform decomposition* (5.1) *has the form*

$$\mathcal{P}_{b,\alpha} = P^{-1} \Big(\bigoplus_{j=0}^{m-1} \mathcal{P}_{t,\gamma^{(j)}} \Big) L_m^n \Big(I_k \otimes \mathcal{P}_{c,\beta} \Big) B. \qquad (5.6)$$

Here, $\otimes$ *denotes the tensor product of matrices.*

Corollary 5.3 has been used to derive a large class of fast algorithms for real and complex DFTs, and DCTs and DSTs [31,33,42]. Theorem 5.1 further generalizes this approach, and, as we show in the following example and in Section 6, also yields fast algorithms not based on Corollary 5.3.

EXAMPLE 5.4. Consider the polynomial algebra $\mathcal{A} = \mathbb{C}[x]/(x^4 - 1)$ with basis $b = \{1, x, x^2, x^3\}$. As we showed in Example 2.1, the corresponding polynomial transform is $\mathcal{P}_{b,\alpha} = \mathrm{DFT}_4$.

We continue from Example 4.7. First, consider $\mathcal{B}_1 = \langle x^2 \rangle$ and the induction $\mathcal{A} = \mathcal{B}_1 \oplus x\mathcal{B}_1$. Let us choose $b^{(0)} = \{1, y\}$ as the basis of $\mathbb{C}[y]/(y^2 - 1) \cong \mathcal{B}_1$; it corresponds to the basis $\{1, x^2\}$ of $\mathcal{B}_1$. We then choose $b^{(1)} = \{1, y\}$ as the basis of $\mathbb{C}[y]/(y^2 - 1) \cong x\mathcal{B}_1$; it corresponds to the basis $\{x, x^3\}$ of $x\mathcal{B}_1$. According to Theorem 5.1, $D_0 = \mathrm{diag}\,(1, 1, 1, 1)$, $D_1 = \mathrm{diag}\,(1, -i, -1, i)$,

$$M_0 = M_1 = \begin{pmatrix} 1 & & \\ & & 1 \\ 1 & & \\ & & & 1 \end{pmatrix}, \quad \mathcal{P}_{b^{(0)},\beta^{(0)}} = \mathcal{P}_{b^{(1)},\beta^{(1)}} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \mathrm{DFT}_2,$$

and B is the base change matrix from $\{1, x, x^2, x^3\}$ to $\{1, x^2\} \cup \{x, x^3\}$. Hence,

$$\text{DFT}_4 = \begin{pmatrix} 1 & & 1 & \\ & 1 & & -i \\ 1 & & -1 & \\ & 1 & & i \end{pmatrix} \begin{pmatrix} \text{DFT}_2 & \\ & \text{DFT}_2 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & & 1 & \\ & 1 & & \\ & & & 1 \end{pmatrix}. \qquad (5.7)$$

This is exactly the Cooley-Tukey FFT for DFT_4 [11].

Next, consider $\mathcal{B}_2 = \langle (x + x^{-1})/2 \rangle$ and the induction $\mathcal{A} = \mathcal{B}_2 \oplus (x - x^{-1})/2 \cdot \mathcal{B}_2$. We choose $b^{(0)} = \{T_0(y), T_1(y), T_2(y)\} = \{1, y, 2y^2 - 1\}$ as the basis of $\mathbb{C}[y]/(y^3 - y) \cong \mathcal{B}_2$; it corresponds to the basis $\{1, (x + x^{-1})/2, (x^2 + x^{-2})/2\}$ of $\mathcal{B}_2$. We then choose $b^{(1)} = \{1\}$ as the basis of $\mathbb{C}[y]/y \cong (x - x^{-1})/2 \cdot \mathcal{B}_2$; it corresponds to the basis $\{(x - x^{-1})/2\}$ of $(x - x^{-1})/2 \cdot \mathcal{B}_2$. Using Theorem 5.1, $D_0 = \text{diag}\,(1, 1, 1, 1)$, $D_1 = \text{diag}\,(0, -i, 0, i)$, $\mathcal{P}_{b^{(1)}, \beta^{(1)}} = (1) = \text{DST-1}_1$,

$$M_0 = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \\ 1 & & \end{pmatrix}, M_1 = \begin{pmatrix} 1 & \\ & \\ & 1 \end{pmatrix}, \mathcal{P}_{b^{(0)}, \beta^{(0)}} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & & -1 \\ 1 & -1 & 1 \end{pmatrix} = \text{DCT-1}_3,$$

and B is the base change matrix from $\{1, x, x^2, x^3\}$ to $\{1, (x + x^{-1})/2, (x^2 + x^{-2})/2\} \cup \{(x - x^{-1})/2\}$. Hence,

$$\text{DFT}_4 = \begin{pmatrix} 1 & & & \\ & 1 & & -i \\ & & 1 & \\ & 1 & & i \end{pmatrix} \begin{pmatrix} \text{DCT-1}_3 & \\ & \text{DST-1}_1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1 & & 1 \\ & & 1 & \\ & 1 & & -1 \end{pmatrix}. \qquad (5.8)$$

This is the Britanak-Rao algorithm for DFT_4 [8].

6. Fast Signal Transforms. In this section use Theorem 5.1 to construct novel fast algorithms for the DFT and for the DCT, type 4. These algorithms cannot be obtained with the special case Corollary 5.3 which as used in [31, 33, 42].

We will first briefly touch on the algebraic signal processing theory to explain why these transforms are associated with polynomial algebras. Then we derive the Cooley-Tukey FFT as special case of Theorem 5.1, which motivates why we call all such algorithms "Cooley-Tukey type." Then we derive the novel algorithms, both of which generalize existing algorithms that had no satisfying algebraic explanation before.

6.1. Algebraic Signal Processing. In [31–34], the authors introduced an axiomatic approach to the signal processing called the *algebraic signal processing theory*. They observed that the basic assumptions used in signal processing are equivalent to viewing *filters* as elements of an algebra $\mathcal{A}$, and *signals* as elements of an associated $\mathcal{A}$- module $\mathcal{M}$. In particular, in the shift-invariant signal processing of finite discrete one-dimensional filters and signals $\mathcal{A} = \mathcal{M} = \mathbb{C}[x]/p(x)$ is necessarily a polynomial algebra. The choice of $\mathcal{A} = \mathcal{M}$, together with a bijective mapping Φ that maps samples from $\mathbb{C}^n$ to signals in $\mathcal{M}$, defines a *signal model* $(\mathcal{A}, \mathcal{M}, \Phi)$.

The fundamental tool in signal processing is the *Fourier transform*, which computes the frequency content of a signal. From the algebraic point of view, the Fourier transform for a signal model $(\mathcal{A}, \mathcal{M}, \Phi)$ is precisely the decomposition (2.1). It can be computed as a matrix-vector product (2.3) with the appropriate polynomial transform (2.2).

6.2. Notation. We define and use the following special matrices:

I_n is the identity matrix of size n.

J_n is the flipped identity matrix of size n: its $(k, n-1-k)$-th element is 1 for $0 \le k < n$, and 0 otherwise.

$1_n = \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix}^T$ is a column vector of n ones.

Z_n is the $n \times n$ circular shift matrix:

$$Z_n = \begin{pmatrix} & 1 \\ I_{n-1} & \end{pmatrix}.$$

L_k^n, where k divides n, is an $n \times n$ permutation matrix that selects elements of $0, 1, \dots, n-1$ at the stride k; the corresponding permutation is $ik+j \mapsto jm+i$, where $0 \le i < m$ and $0 \le j < k$. The (i, j)-th element of L_k^n is 1 if $j = \lfloor \frac{ik(n+1)}{n} \rfloor \mod n$, and 0 otherwise.

$K_k^n = (I_m \oplus J_m \oplus I_m \oplus \dots)L_k^n$, where k divides n, is another permutation matrix.

$T_k^n = \mathrm{diag}\left(w_n^{ij} \mid 0 \le i < k, 0 \le j < m \right)$, where the index i runs faster, and $n = km$, is the twiddle factor matrix used in the Cooley-Tukey FFT.

We define the complimentary direct sum of matrices as

$$\oslash_{j=0}^{m-1} A_j = \begin{pmatrix} & & A_0 \\ & \cdot^{\cdot^{\cdot}} & \\ A_{m-1} & & \end{pmatrix}.$$

6.3. Cooley-Tukey FFT. We derive the general-radix Cooley-Tukey FFT using Theorem 5.1. As was shown in [31], Corollary 5.3 is sufficient in this case.

Consider $\mathcal{A} = \mathcal{M} = \mathbb{C}[x]/(x^n - 1)$. Let $b = \{1, x, \dots, x^{n-1}\}$ be the basis of $\mathcal{M}$. As we showed in Example 2.1, the corresponding polynomial transform is DFT_n. Assume $n = km$. Let $r(x) = x^k$, and $\mathcal{B} = \langle r(x) \rangle$. Then $x^\ell \mathcal{B} \cong \mathbb{C}[y]/(y^m - 1)$, for $\ell = 0 \dots k-1$, and $\mathcal{A} = \oplus_{\ell=0}^{k-1} x^\ell \mathcal{B}$. Choosing the same basis $b^{(\ell)} = \{1, y, \dots, y^{m-1}\}$ in each $\mathbb{C}[y]/(y^m - 1) \cong x^\ell \mathcal{B}$ yields $\mathcal{P}_{b^{(\ell)}, \beta^{(\ell)}} = \mathrm{DFT}_m$. By Theorem 5.1, we obtain

$$\mathrm{DFT}_{km} = M \cdot (I_k \otimes \mathrm{DFT}_m) \cdot B.$$

Here, $B = L_k^{km}$ and $M = (D_0 M_0 | \dots | D_{k-1} M_0)$, where $M_0 = 1_k \otimes I_m$, and $D_\ell = \mathrm{diag}\left(\omega_{km}^{\ell j} \right)_{0 \le j < km}$ for $0 \le \ell < k$. Hence, we can rewrite

$$M = L_k^{km} (I_m \otimes \mathrm{DFT}_k) T_k^{km} L_m^{km}.$$

to obtain the well-known general-radix Cooley-Tukey FFT algorithm [40, 41]

$$\begin{aligned} \mathrm{DFT}_{km} &= L_k^{km} (I_m \otimes \mathrm{DFT}_k) T_k^{km} L_m^{km} (I_k \otimes \mathrm{DFT}_m) L_k^{km} \\ &= L_k^{km} (I_m \otimes \mathrm{DFT}_k) T_k^{km} (\mathrm{DFT}_m \otimes I_k). \end{aligned} \tag{6.1}$$

6.4. New Fast Algorithms. In this section, we derive novel fast general-radix algorithms for DFT and DCT-4. Each of them requires $O(n \log n)$ operations. To the best of our knowledge, these algorithms have not been reported in the literature.

General-radix Britanak-Rao FFT. In [8], Britanak and Rao derived a fast algorithm for DFT_{2m} that can be written as the factorization

$$\mathrm{DFT}_{2m} = X_m^{2m} \left(I_m \oplus Z_m^{-1} \right) D_m^{2m} \left(\mathrm{DCT\text{-}1}_{m+1} \oplus \mathrm{DST\text{-}1}_{m-1} \right) B_m^{2m}.$$

The matrices D_m^{2m}, B_m^{2m}, and X_m^{2m} are specified in (A.4-A.6) by setting $k = 1$.

In Appendix A, we derive the following general-radix version of this algorithm:

THEOREM 6.1.

$$
\mathrm{DFT}_{2km} = L_k^{2km}\Big(I_{2m}\otimes\mathrm{DFT}_k\Big)X_m^{2km}L_{2m}^{2km}\Big(I_m\oplus Z_m^{-1}\oplus I_{2(k-1)m}\Big)D_m^{2km}
$$
$$
\times\Big(\mathrm{DCT}\text{-}1_{m+1}\oplus\mathrm{DST}\text{-}1_{m-1}\oplus I_{k-1}\otimes(\mathrm{DCT}\text{-}2_m\oplus\mathrm{DST}\text{-}2_m)\Big)B_m^{2km}.
$$

Here, D_m^{2km} is a diagonal matrix, and B_m^{2km} and X_m^{2km} are 2-sparse matrices (that is, each row contains only two non-zero entries) specified in (A.4-A.6).

This factorization is obtained using Theorem 5.1 with subalgebra $\mathcal{B} = \big\langle(x^k + x^{-k})/2\big\rangle$ of the algebra $\mathcal{A} = \mathbb{C}[x]/(x^{2km} - 1)$ and transversal $t_0(x) = 1$, $t_1(x) = (x^k - x^{-k})/2$, $t_{2j}(x) = x^j(x^k + 1)/2$, and $t_{2j+1}(x) = x^j(x^k - 1)/2$ for $1 \le j < k$.

DFT_k requires $O(k\log k)$ operations; $\mathrm{DCT}\text{-}1_{m+1}$, $\mathrm{DST}\text{-}1_{m-1}$, $\mathrm{DCT}\text{-}2_m$, and $\mathrm{DST}\text{-}2_m$ require $O(m\log m)$ operations each [31, 33]. D_m^{2km} requires $n = 2km$ operations and B_m^{2km} and X_m^{2km} each require $3n$ operations. Hence, the algorithm for DFT_n in Theorem 6.1 requires $O(n\log n)$ operations.

General-radix Wang algorithm for DCT-4. In [43], Wang derived a fast algorithm for $\mathrm{DCT}\text{-}4_{2m}$ that can be written as the factorization

$$
\mathrm{DCT}\text{-}4_{2m} = K_2^{2m}\cdot\bigoplus_{j=0}^{m-1}\begin{pmatrix}\cos\frac{2m-2j-1}{8m}\pi & (-1)^j\cos\frac{2j+1-2m}{8m}\pi \\ \cos\frac{2j+1-2m}{8m}\pi & (-1)^{j+1}\cos\frac{2m-2j-1}{8m}\pi\end{pmatrix}
$$
$$
\times(\mathrm{DCT}\text{-}3_m\otimes I_2)(K_2^{2m})^T\begin{pmatrix}1 & & \\ & L_2^{2(m-1)}\cdot I_{m-1}\otimes\mathrm{DFT}_2 & \\ & & 1\end{pmatrix}.
$$

In Appendix B, we derive the following general-radix version of this algorithm:

THEOREM 6.2.

$$
\mathrm{DCT}\text{-}4_{2km} = K_k^{2km}(K_2^{2m}\otimes\mathrm{DCT}\text{-}4_k)Y_m^{2km}\cdot(\mathrm{DCT}\text{-}3_m\otimes L_2^{2k})(K_{2k}^n)^T
$$
$$
\times I_k\otimes\begin{pmatrix}1 & & \\ & L_2^{2(m-1)}\cdot I_{m-1}\otimes\mathrm{DFT}_2 & \\ & & 1\end{pmatrix}(K_{2m}^{2km})^T.
$$

Here, Y_m^{2km} is a 2-sparse matrix specified in (B.4).

This factorization is obtained using Theorem 5.1 with subalgebra $\mathcal{B} = \big\langle T_{2k}(x)\big\rangle$ of the algebra $\mathcal{A} = \mathbb{C}[x]/T_{2km}(x)$ with transversal $t_{2j}(x) = V_j(x)$ and $t_{2j+1}(x) = W_j(x)(V_{2k-1}(x) - V_{2k}(x))/2$ for $0 \le j < k$.

$\mathrm{DCT}\text{-}4_k$ requires $O(k\log k)$ operations, and $\mathrm{DCT}\text{-}3_m$ requires $O(m\log m)$ operations [31, 33]. Y_m^{2km} requires $3n$ operations, where $n = 2km$. Hence, the algorithm for $\mathrm{DCT}\text{-}4_n$ in Theorem 6.2 requires $O(n\log n)$ operations.

7. Conclusion. We have introduced a new approach to the factorization of polynomial transforms $\mathcal{P}_{b,\alpha}$ based on the decomposition of the underlying regular module $\mathcal{A} = \mathcal{M} = \mathbb{C}[x]/p(x)$ into an induction. This approach is in its most general form since the underlying Theorem 5.1 allows for arbitrary subalgebras. Not every factorization based on this theorem yields a fast algorithm: it depends on the computational costs of matrices B and M that occur in its recursive application.

However, we have shown that the theorem produces at least two novel general-radix algorithms for the DFT and a DCT. Both algorithms cannot be obtained using

the prior special case Corollary 5.3. In addition, both generalize algorithms from the literature, which now become the special cases of radix 2 and thus also obtain an algebraic explanation. Together with [33, 42], this paper provides a rather complete algebraic theory of Cooley-Tukey type algorithms for trigonometric transforms.

Future work. In addition to the DFT, DCT, and DST, other polynomial transforms have been studied. In particular, polynomial transforms based on orthogonal polynomials have found applications in such areas as function interpolation, data compression, and image processing [22–24]. For practical applications, fast algorithms for this class of polynomial transforms are needed. With the exception of DCT and DST, the fastest algorithms, reported in the literature to date, require $O(n \log^2 n)$ operations (in particular, more than $43n \log_2^2 n$ for $n = 2^k$) [14,28]. The question is whether our approach can improve this bound for some or all of these transforms.

Appendix A. Proof of Theorem 6.1. Consider $\mathcal{A} = \mathcal{M} = \mathbb{C}[x]/(x^{2km} - 1)$, with basis $\{1, x, \ldots, x^{2km-1}\}$ and $\alpha_k = \omega_{2km}^k$. The corresponding polynomial transform is DFT_{2km}.

By Theorem 3.2, the polynomial $r(x) = (x^k + x^{-k})/2$ generates the subalgebra

$$\mathcal{B} = \langle r(x) \rangle \cong \mathbb{C}[y]/2(y^2 - 1)U_{m-1}(y).$$

If we choose $\{T_\ell(y)\}_{0 \leq \ell < m+1}$ as the basis , the polynomial transform is

$$\left[T_\ell(\cos \frac{k\pi}{m})\right]_{0 \leq k, \ell < m+1} = \mathrm{DCT\text{-}1}_{m+1}.$$

By Theorem 4.5, the $\mathcal{B}$-module $(x^k - x^{-k})/2 \cdot \mathcal{B} \cong \mathbb{C}[y]/U_{m-1}(y)$. If we choose the basis $\{U_\ell(y)\}_{0 \leq \ell < m-1}$, then the polynomial transform is

$$\left[U_\ell(\cos \frac{k\pi}{m})\right]_{0 \leq k, \ell < m-1} = \mathrm{diag}\left(1/\sin \frac{(k+1)\pi}{m}\right)_{0 \leq k < m-2} \cdot \mathrm{DST\text{-}1}_{m-1} = \mathrm{DST\text{-}1}'_{m-1}.$$
$$\tag{A.1}$$

Similarly, the $\mathcal{B}$-module $x^j(x^k+1)/2 \cdot \mathcal{B} \cong \mathbb{C}[y]/2(y-1)U_{m-1}(y)$ for any $1 \leq j < k$. If we choose the basis $\{V_\ell(y)\}_{0 \leq \ell < m}$, then the polynomial transform is

$$\left[V_\ell(\cos \frac{k\pi}{m})\right]_{0 \leq k, \ell < m} = \mathrm{diag}\left(1/\cos \frac{k\pi}{2m}\right)_{0 \leq k < m} \cdot \mathrm{DCT\text{-}2}_m = \mathrm{DCT\text{-}2}'_m. \tag{A.2}$$

Finally, the $\mathcal{B}$-module $x^j(x^k-1)/2 \cdot \mathcal{B} \cong \mathbb{C}[y]/2(y+1)U_{m-1}(y)$ for any $1 \leq j < k$. If we choose the basis $\{W_\ell(y)\}_{0 \leq \ell < m}$, then the polynomial transform is

$$\left[W_\ell(\cos \frac{(k+1)\pi}{m})\right]_{0 \leq k, \ell < m} = \mathrm{diag}\left(1/\sin \frac{(k+1)\pi}{2m}\right)_{0 \leq k < m} \cdot \mathrm{DST\text{-}2}_m = \mathrm{DST\text{-}2}'_m.$$
$$\tag{A.3}$$

Using Theorem 4.6, we can verify that $t_0(x) = 1$, $t_1(x) = (x^k - x^{-k})/2$, $t_{2j}(x) = x^j(x^k + 1)/2$, and $t_{2j+1}(x) = x^j(x^k - 1)/2$ for $1 \leq j < k$, is a transversal of $\mathcal{B}$ in $\mathcal{A}$. Hence, by Theorem 5.1, we obtain the factorization

$$\mathrm{DFT}_n = M\Big(\mathrm{DCT\text{-}1}_{m+1} \oplus \mathrm{DST\text{-}1}'_{m-1} \oplus I_{k-1} \otimes (\mathrm{DCT\text{-}2}'_m \oplus \mathrm{DST\text{-}2}'_m)\Big) B_m^{2km}.$$

Here, B_m^{2km} is the base change matrix from $\{x^\ell\}_{0\le\ell\le n-1}$ to the concatenation of bases of $t_j(x)\mathcal{B}$, $0\le j<2k$, and by construction

$$B_m^{2km} = \begin{pmatrix} 1 & & & \\ & I_{m-1} & & J_{m-1} \\ & & 1 & \\ & I_{m-1} & & -J_{m-1} \end{pmatrix} \oplus I_{k-1}\otimes \begin{pmatrix} 1 & 1 & & \\ -1 & 1 & I_{m-1} & J_{m-1} \\ & & I_{m-1} & -J_{m-1} \end{pmatrix} \cdot L_k^{2km}. \quad \text{(A.4)}$$

M is constructed as follows. Let

$$M_0 = 1_k \otimes \begin{pmatrix} 1 & & \\ & I_{m-1} & \\ & & 1 \\ & J_{m-1} & \end{pmatrix}.$$

Let $M_0(j_0,\ldots,j_\ell)$ be the subset of columns of M_0 with indices $j_0,\ldots,j_\ell$; and let $D_j = \operatorname{diag}\big(t_j(\alpha_i)\big)_{0\le i<n}$, for $0\le j<2k$. Then

$$M = \big(D_0 M_0 \mid D_1 M_1 \mid D_2 M_2 \mid \cdots \mid D_{2k-1} M_{2k-1}\big),$$

where $M_1 = M_0(1,\ldots,m-1)$; $M_{2j} = M_0(0,\ldots,m-1)$ and $M_{2j+1} = M_0(1,\ldots,m)$ for $1\le j<k$. We can further rewrite M as

$$M = L_k^{2km}(I_{2m}\otimes \operatorname{DFT}_k)X_m^{2km}L_{2m}^{2km}(I_m \oplus Z_m^{-1} \oplus I_{2(k-1)m}).$$

Here, matrix X_m^{2km} has the structure

$$X_m^{2km} = \begin{pmatrix} I_k & & & \\ & \oplus_{j=1}^{m-1}C_j & \oplus_{j=1}^{m-1}D_j & \\ & & & F \\ & \oslash_{j=m+1}^{2m-1}C_j & \oslash_{j=1}^{m-1}D_j & \end{pmatrix}, \quad \text{(A.5)}$$

where

$$C_j = 1 \oplus \operatorname{diag}\big(\omega_{2km}^{j\ell}(\omega_{2m}^j + 1)/2\big)_{1\le\ell<k},$$
$$D_j = \big((\omega_{2m}^j - \omega_{2m}^{-j})/2\big) \oplus \operatorname{diag}\big(\omega_{2km}^{j\ell}(\omega_{2m}^j - 1)/2\big)_{1\le\ell<k},$$
$$F = 1 \oplus \operatorname{diag}\big(-\omega_{2k}^j\big)_{1\le j<k}.$$

After the substitution of DST-$1'_{m-1}$, DCT-$2'_m$, and DST-$2'_m$ with DST-1_{m-1}, DCT-2_m, and DST-2_m using (A.1-A.3), and simplification, we obtain the factorization

$$\operatorname{DFT}_{2km} = L_k^{2km}(I_{2m}\otimes \operatorname{DFT}_k)X_m^{2km}L_{2m}^{2km}(I_m \oplus Z_m^{-1} \oplus I_{2(k-1)m})D_m^{2km}$$
$$\cdot\big(\operatorname{DCT-1}_{m+1} \oplus \operatorname{DST-1}_{m-1} \oplus I_{k-1}\otimes(\operatorname{DCT-2}_m \oplus \operatorname{DST-2}_m)\big)B_m^{2km},$$

where B_m^{2km} and X_m^{2km} are defined in (A.4) and (A.5), and

$$D_m^{2km} = I_{m+1} \oplus \operatorname{diag}\Big(1/\sin\frac{(j+1)\pi}{m}\Big)_{0\le j<m-1}$$
$$\oplus I_{k-1}\otimes\Big(\operatorname{diag}\Big(1/\cos\frac{j\pi}{2m}\Big)_{0\le j<m} \oplus \operatorname{diag}\Big(1/\sin\frac{(j+1)\pi}{2m}\Big)_{0\le j<m}\Big) \quad \text{(A.6)}$$

Appendix B. Proof of Theorem 6.2.

Consider $\mathcal{A} = \mathcal{M} = \mathbb{C}[x]/2T_{2km}(x)$ with basis $\{V_0(x), V_1(x), \ldots, V_{2km-1}(x)\}$. The corresponding polynomial transform is

$$\text{diag}\left(1/\cos\frac{(k+1/2)\pi}{4km}\right)_{0 \le k < 2km} \cdot \text{DCT-4}_{2km} = \text{DCT-4}'_{2km}. \qquad (\text{B.1})$$

By Theorem 3.2, the polynomial $r(x) = T_{2k}(x)$ generates the subalgebra

$$\mathcal{B} = \langle r(x) \rangle \cong \mathbb{C}[y]/2T_m(y).$$

By Theorem 4.5, the $\mathcal{B}$-module $V_j(x)\mathcal{B} \cong \mathbb{C}[y]/2T_m(y)$ for any $0 \le j < k$. If we choose the basis $\{V_\ell(y)\}_{0 \le \ell < m}$, then the polynomial transform is

$$\left[T_\ell(\cos\frac{(k+1/2)\pi}{m})\right]_{0 \le k, \ell < m} = \text{DCT-3}_m.$$

Similarly, the $\mathcal{B}$-module $W_j(x)(V_{2k-1}(x) - V_{2k}(x))/2 \cdot \mathcal{B} \cong \mathbb{C}[y]/2T_m(y)$ for any $0 \le j < k$. If we choose the basis If we choose the basis $\{U_\ell(y)\}_{0 \le \ell < m}$, then the polynomial transform is

$$\left[U_\ell(\cos\frac{(k+1/2)\pi}{m})\right]_{0 \le k, \ell < m-1} = \text{diag}\left(1/\sin\frac{(k+1/2)\pi}{m}\right)_{0 \le k < m} \cdot \text{DST-3}_m = \text{DST-3}'_m.$$
$$(\text{B.2})$$

We can verify using Theorem 4.6 that $t_{2j} = V_j(x)$ and $t_{2j+1} = W_j(x)(V_{2k-1}(x) - V_{2k}(x))/2$ for $0 \le j < k$, is a transversal of $\mathcal{B}$ in $\mathcal{A}$. Hence, by Theorem 5.1, we obtain the decomposition

$$\text{DCT-4}'_{2km} = M\left(I_k \otimes (\text{DCT-3}'_m \oplus \text{DST-3}'_m)\right)B.$$

Here, B is the base change matrix from $\{x^\ell\}_{0 \le \ell \le n-1}$ to the concatenation of bases of $t_j(x)\mathcal{B}$, $0 \le j < 2k$, and by construction

$$B = I_k \otimes \begin{pmatrix} 1 & & \\ & L_2^{2(m-1)} \cdot I_{m-1} \otimes \text{DFT}_2 & \\ & & 1 \end{pmatrix} (K_{2m}^{2km})^T.$$

M is constructed as follows. Let

$$M_0 = 1_k \otimes \begin{pmatrix} I_m \\ J_m \end{pmatrix}.$$

Let $D_j = \text{diag}\left(t_j(\alpha_i)\right)_{0 \le i < n}$ for $0 \le j < 2k$. Then

$$M = \left(D_0 M_0 \mid D_1 M_0 \mid D_2 M_0 \mid \cdots \mid D_{2k-1}M_0\right).$$

We can simplify matrix M. Let us introduce matrices

$$X_k^{(C4)}(r) = \begin{pmatrix} c_0 & & & s_{k-1} \\ & \ddots & \ddots & \\ & \ddots & \ddots & \\ s_0 & & & c_{k-1} \end{pmatrix}, \quad X_k^{(S4)}(r) = \begin{pmatrix} c_0 & & & -s_{k-1} \\ & \ddots & \ddots & \\ & \ddots & \ddots & \\ -s_0 & & & c_{k-1} \end{pmatrix}. \quad (\text{B.3})$$

Here, $c_\ell = \cos \frac{(1-2r)(2\ell+1)\pi}{4k}$ and $s_\ell = \sin \frac{(1-2r)(2\ell+1)\pi}{4k}$. These matrices are used for the so-called *skew* DCT and DST [33]. Further, let us define $r^{(i)} = (2i+1)/(4m)$ and

$$r_j^{(i)} = \begin{cases} \frac{r^{(i)}+2j}{k}, & \text{if } j \text{ is even} \\ \frac{2-r^{(i)}+2j}{k}, & \text{if } j \text{ is odd} \end{cases}$$

for $0 \le j < \lfloor \frac{k}{2} \rfloor$. In case k is odd, we also define $r_{k-1}^{(i)} = \frac{r^{(i)}-1}{k} + 1$. Finally, let us define diagonal matrices

$$D_k^{(C4)}(r^{(i)}) = \text{diag}\left(1/\cos\left(r_j^{(i)}\pi/2\right)\right)_{0 \le j < k},$$

$$D_k^{(S4)}(r^{(i)}) = \text{diag}\left(\sin\left(2kr_j^{(i)}\pi\right)/\cos\left(r_j^{(i)}\pi/2\right)\right)_{0 \le j < k}.$$

Then $M = K_k^n \widehat{M} L_{2m}^n$, where $\widehat{M} =$

$$\begin{pmatrix} \oplus_{i=0}^{m-1} D_k^{(C4)}(r^{(i)}) \, \text{DCT-4}_k(r^{(i)}) X_k^{(C4)}(r^{(i)}) & \oplus_{i=0}^{m-1} D_k^{(S4)}(r^{(i)}) \, \text{DST-4}_k(r^{(i)}) X_k^{(S4)}(r^{(i)}) \\ \oslash_{i=m}^{2m-1} D_k^{(C4)}(r^{(i)}) \, \text{DCT-4}_k(r^{(i)}) X_k^{(C4)}(r^{(i)}) & \oslash_{i=m}^{2m-1} D_k^{(S4)}(r^{(i)}) \, \text{DST-4}_k(r^{(i)}) X_k^{(S4)}(r^{(i)}) \end{pmatrix}.$$

We can further simplify (B.1) by substituting DCT-$4'_{2km}$ and DST-$3'_m$ with DCT-4_{2km} DST-3_m using (B.1) and (B.2). Then we use the equalities

$$X_k^{(C4)}(r) = X_k^{(S4)}(1-r),$$

$$\text{DST-3}_m = \text{diag}\left((-1)^j\right)_{0 \le j < m} \cdot \text{DCT-3}_m \cdot J_m,$$

$$\text{DST-4}_k = \text{diag}\left((-1)^j\right)_{0 \le j < k} \cdot \text{DCT-4}_k \cdot J_k,$$

to obtain the decomposition

$$\text{DCT-4}_{2km} = K_k^{2km}(K_2^{2m} \otimes \text{DCT-4}_k)Y_m^{2km}(\text{DCT-3}_m \otimes L_2^{2k})(K_{2k}^{2km})^T$$

$$\cdot I_k \otimes \begin{pmatrix} 1 & & \\ & L_2^{2(m-1)} \cdot I_{m-1} \otimes \text{DFT}_2 & \\ & & 1 \end{pmatrix} (K_{2m}^{2km})^T,$$

where

$$Y_m^{2km} = \bigoplus_{j=0}^{m-1} \begin{pmatrix} X_k^{(C4)}(r^{(j)}) & (-1)^j \cdot J_k \cdot X_k^{(C4)}(1-r^{(j)}) \\ X_k^{(C4)}(1-r^{(j)}) & (-1)^{j+1} \cdot J_k \cdot X_k^{(C4)}(r^{(j)}) \end{pmatrix} \qquad \text{(B.4)}$$

and $X_k^{(C4)}(r)$ is defined in (B.3).

REFERENCES

[1] L. AUSLANDER, E. FEIG, AND S. WINOGRAD, *Abelian semi-simple algebras and algorithms for the discrete Fourier transform*, Advances in Applied Mathematics, 5 (1984), pp. 31–55.

[2] ——, *The multiplicative complexity of the discrete Fourier transform*, Advances in Applied Mathematics, 5 (1984), pp. 87–109.

[3] G. D. BERGLAND, *Numerical analysis: A fast Fourier transform algorithm for real-valued series*, Communications ACM, 11 (1968), pp. 703–710.

[4] Th. Beth, *Verfahren der Schnellen Fouriertransformation [Methods for the Fast Fourier Transform]*, Teubner, 1984.

[5] ———, *On the computational complexity of the general discrete Fourier transform*, Theoretical Computer Science, 51 (1987), pp. 331–339.

[6] J. P. Boyd, *Chebyshev and Fourier Spectral Methods*, Dover, 2nd ed., 2001.

[7] R. N. Bracewell, *The fast Hartley transform*, Proc. IEEE, 72 (1984), pp. 1010–1018.

[8] V. Britanak and K. R. Rao, *The fast generalized discrete Fourier transforms: A unified approach to the discrete sinusoidal transforms computation*, Signal Processing, 79 (1999), pp. 135–150.

[9] M. Clausen, *Beiträge zum Entwurf schneller Spektraltransformationen (Habilitationsschrift)*, Univ. Karlsruhe, 1988.

[10] M. Clausen and U. Baum, *Fast Fourier Transforms*, BI-Wiss.-Verl., 1993.

[11] J. W. Cooley and J. W. Tukey, *An algorithm for the machine calculation of complex Fourier series*, Math. of Computation, 19 (1965), pp. 297–301.

[12] W. C. Curtis and I. Reiner, *Representation Theory of Finite Groups*, Interscience, 1962.

[13] P. Diaconis and D. Rockmore, *Efficient computation of the Fourier transform on finite groups*, Amer. Math. Soc., 3(2) (1990), pp. 297–332.

[14] J. R. Driscoll, D. M. Healy Jr., and D. Rockmore, *Fast discrete polynomial transforms with applications to data analysis for distance transitive graphs*, SIAM Journal Computation, 26 (1997), pp. 1066–1099.

[15] P. Duhamel, *Implementation of "split-radix" FFT algorithms for complex, real, and real-symmetric data*, IEEE Trans. ASSP, 34 (1986), pp. 285–295.

[16] D. S. Dummit and R. M. Foote, *Abstract Algebra*, Wiley, 3rd ed., 2003.

[17] P. A. Fuhrman, *A Polynomial Approach to Linear Algebra*, Springer Verlag, New York, 1996.

[18] M. T. Heideman and C. S. Burrus, *On the number of multiplications necessary to compute a length-2^n DFT*, IEEE Trans. Acoust., Speech, Signal Proc., ASSP-34 (1986), pp. 91–95.

[19] H. W. Johnson and C. S. Burrus, *On the structure of efficient DFT algorithmss*, IEEE Trans. Acoust., Speech, Signal Proc., ASSP-33 (1985), pp. 248–254.

[20] Th. Kailath and V. Olshevsky, *Displacement structure approach to polynomial Vandermonde and related matrices*, Linear Algebra and Applications, 261 (1997), pp. 49–90.

[21] S. Mallat, *A Wavelet Tour of Signal Processing*, Academic Press, 1999.

[22] G. Mandyam and N. Ahmed, *The discrete Laguerre transform: Derivation and applications*, IEEE Trans. on Signal Processing, 44 (1996), pp. 2925–2931.

[23] J.-B. Martens, *The Hermite transform—applications*, IEEE Trans. on Acoustics, Speech, and Signal Processing, 38 (1990), pp. 1607–1618.

[24] ———, *The Hermite transform—theory*, IEEE Trans. on Acoustics, Speech, and Signal Processing, 38 (1990), pp. 1595–1605.

[25] J. C. Mason and D. C. Handscomb, *Chebyshev polynomials*, Chapman and Hall/CRC, 2002.

[26] P. J. Nicholson, *Algebraic theory of finite Fourier transforms*, Journal of Computer and System Sciences, 5 (1971), pp. 524–547.

[27] H. J. Nussbaumer, *Fast Fourier Transformation and Convolution Algorithms*, Springer, 2nd ed., 1982.

[28] D. Potts, G. Steidl, and M. Tasche, *Fast algorithms for discrete polynomial transforms*, Mathematics of Computation, 67 (1998), pp. 1577–1590.

[29] M. Püschel, *Decomposing monomial representations of solvable groups*, Journal of Symbolic Computation, 34 (2002), pp. 561–596.

[30] M. Püschel and J. M. F. Moura, *Algebraic signal processing theory*. available at http://arxiv.org/abs/cs.IT/0612077, parts of this manuscript appeared as [34] and [32].

[31] ———, *The algebraic approach to the discrete cosine and sine transforms and their fast algorithms*, SIAM Journal of Computing, 32 (2003), pp. 1280–1316.

[32] ———, *Algebraic signal processing theory: 1-D space*, IEEE Transactions on Signal Processing, 56 (2008), pp. 3586–3599.

[33] ———, *Algebraic signal processing theory: Cooley-Tukey type algorithms for DCTs and DSTs*, IEEE Transactions on Signal Processing, 56 (2008), pp. 1502–1521.

[34] ———, *Algebraic signal processing theory: Foundation and 1-D time*, IEEE Transactions on Signal Processing, 56 (2008), pp. 3572–3585.

[35] K. R. RAO AND P. YIP, *Discrete Cosine Transform: Algorithms, Advantages, Applications*, Academic Press, 1990.

[36] D. ROCKMORE, *Efficient computation of Fourier inversion for finite groups*, Assoc. Comp. Mach., 41 (1994), pp. 31–66.

[37] H. V. SORENSEN, D. L. JONES, C. S. BURRUS, AND M. T. HEIDEMAN, *On computing the discrete Hartley transform*, IEEE Trans. on Acoustics, Speech, and Signal Processing, ASSP-33 (1985), pp. 1231–1238.

[38] G. STEIDL, *Fast radix-p discrete cosine transform*, Appl. Algebra Engrg. Comm. Comp., 3 (1992), pp. 39–46.

[39] G. STEIDL AND M. TASCHE, *A polynomial approach to fast algorithms for discrete Fourier-cosine and Fourier-sine transforms*, Mathematics of Computation, 56 (1991), pp. 281–296.

[40] R. TOLIMIERI, M. AN, AND C. LU, *Algorithms for Discrete Fourier Transforms and Convolution*, Springer, 2nd ed., 1997.

[41] C. VAN LOAN, *Computational Framework of the Fast Fourier Transform*, Siam, 1992.

[42] Y. VORONENKO AND M. PÜSCHEL, *Algebraic signal processing theory: Cooley-Tukey type algorithms for real DFTs*, IEEE Trans. Signal Proc., 57 (2009), pp. 205–222.

[43] Z. WANG, *Fast algorithms for the discrete W transform and for the discrete Fourier transform*, IEEE Trans. on Acoustics, Speech, and Signal Processing, ASSP-32 (1984), pp. 803–816.

[44] S. WINOGRAD, *On the multiplicative complexity of the discrete Fourier transform*, Advances in Mathematics, 32 (1979), pp. 83–117.