

Algebraic Signal Processing Theory: Foundation and 1-D Time

Markus Püschel and José M. F. Moura

Abstract—This paper introduces a general and axiomatic approach to *linear signal processing* (SP) that we refer to as the algebraic signal processing theory (ASP). Basic to ASP is the *linear signal model* defined as a triple $(\mathcal{A}, \mathcal{M}, \Phi)$ where familiar concepts like the filter space and the signal space are cast as an algebra \mathcal{A} and a module \mathcal{M} , respectively. The mapping Φ generalizes the concept of a z -transform to bijective linear mappings from a vector space of signal samples into the module \mathcal{M} . Common concepts like filtering, spectrum, or Fourier transform have their equivalent counterparts in ASP. Once these concepts and their properties are defined and understood in the context of ASP, they remain true and apply to specific instantiations of the ASP signal model. For example, to develop signal processing theories for infinite and finite discrete time signals, for infinite or finite discrete space signals, or for multidimensional signals, we need only to instantiate the signal model to one that makes sense for that specific class of signals. Filtering, spectrum, Fourier transform, and other notions follow then from the corresponding ASP concepts. Similarly, common assumptions in SP translate into requirements on the ASP signal model. For example, shift-invariance is equivalent to \mathcal{A} being commutative. For finite (duration) signals shift invariance then restricts \mathcal{A} to polynomial algebras. We explain how to design signal models from the specification of a special filter, the *shift*. The paper illustrates the general ASP theory with the standard *time* shift, presenting a unique signal model for infinite time and several signal models for finite time. The latter models illustrate the role played by boundary conditions and recover the discrete Fourier transform (DFT) and its variants as associated Fourier transforms. Finally, ASP provides a systematic methodology to derive fast algorithms for linear transforms. This topic and the application of ASP to space dependent signals and to multidimensional signals are pursued in companion papers.

Index Terms—Signal model, filter, Fourier transform, boundary condition, signal extension, shift, shift-invariant, z -transform, spectrum, algebra, module, representation theory, irreducible, convolution, polynomial transform

I. INTRODUCTION

Linear signal processing (SP) is built around signals, filters, z -transform, spectrum, Fourier transform, as well as other concepts; it is a well-developed theory for continuous and discrete time. In linear signal processing, signals are modeled as elements of vector spaces over some base field (usually \mathbb{R} or \mathbb{C}) and filters operate as linear mappings on the vector spaces of signals. This paper presents an algebraic signal processing theory (ASP) for *linear* signal processing. ASP starts with three basic objects: 1) an algebra¹ \mathcal{A} of filters,

2) an \mathcal{A} -module \mathcal{M} of signals, and 3) a bijective linear mapping Φ from a coordinate vector space V into \mathcal{M} that generalizes the z -transform. These objects form the triple $(\mathcal{A}, \mathcal{M}, \Phi)$, which we refer to as the *signal model*. In principle, many signal models $(\mathcal{A}, \mathcal{M}, \Phi)$ are possible; knowing which models arise in common SP applications, or which models should be associated with a given linear transform, or how to develop signal models which reflect desired properties are relevant questions. We address these questions by fixing, i.e., choosing, a *shift* operator that generates the algebra \mathcal{A} of filters, and by showing that standard properties in SP translate into corresponding requirements for the signal model. For example, shift-invariance forces the algebra \mathcal{A} to be commutative. If the signals are finite—and for now assuming one dimensional (1-D) signals—this requires \mathcal{A} to be a *polynomial algebra* $\mathbb{C}[x]/p(x)$, which is the space of polynomials modulo the fixed polynomial $p(x)$. Hence, polynomial algebras are a key structure in ASP.

We present the ASP equivalents of filtering, spectrum, Fourier transform, frequency response, and other common signal processing concepts. Once defined and their properties derived in the framework of ASP, it is simple to identify these concepts for concrete examples of ASP signal models. We consider explicitly infinite (duration) and finite (duration) discrete *time* signals. For the corresponding infinite discrete time signal model, the Fourier transform is the discrete time Fourier transform (DTFT). For finite discrete time signals, we can have several signal models; for example, assuming shift-invariance, a common signal model sets $\mathcal{A} = \mathcal{M} = \mathbb{C}[x]/(x^n - 1)$ for which the corresponding Fourier transform is the discrete Fourier transform (DFT). For other finite discrete time models, the Fourier transform becomes the real DFT (RDFT) or the discrete Hartley transform (DHT). In [1], we consider shift-invariant signals indexed by 1-D lattices; we call them 1-D *space* signals. In their signal models, the polynomial $p(x)$ in \mathcal{A} is a Chebychev polynomial and their Fourier transforms are the 16 variants of the discrete trigonometric transforms (DTT), e.g, the discrete cosine transform (DCT) and the discrete sine transform (DST). The ASP framework can be applied to signals in higher dimensions. References [2], [3] instantiate ASP for 2-D signals indexed by the quincunx and hexagonal lattices. The Fourier transforms for these models are novel non-separable 2-D linear transforms.

Besides representing a unifying framework for existing or new signal processing theories in 1-D or higher dimensions, ASP also provides the means to concisely derive fast algorithms for Fourier transforms in its many instantiations. For example, in [4], [5], [6], [7], we derive from a few basic ASP principles many dozens fast algorithms including many new

This work was supported by NSF through awards 9988296, 0310941, and 0634967.

Markus Püschel and José M. F. Moura are with the Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh. E-mail: {pueschel,moura}@ece.cmu.edu. Ph: (412)268-6341; fax: (412)268-3890.

¹The term algebra here is used to describe a specific algebraic structure that is introduced later, and not the mathematical discipline.

ones, such as general-radix Cooley-Tukey type algorithms for various DCTs and DSTs. We also apply the theory in [8] to derive fast algorithms for novel 2-D transforms.

A longer version of this paper is available in [9]. Early work on the algebraic approach to linear transforms appeared in [4].

Related work. To date algebra has not been a mainstream tool in signal processing. However, we can identify two important algebraic research directions in signal processing: the algebraic derivation of fast Fourier transform algorithms (FFT) and Fourier analysis on groups.

The rediscovery of the (standard) FFT by Cooley-Tukey [10], [11] spawned research on the derivation and optimization of DFT algorithms. Key in this work was recognizing the well-known connection between the DFT and the cyclic group, or equivalently the polynomial algebra $\mathbb{C}[x]/(x^n - 1)$, and to use algebra in the algorithm derivation (e.g., [12], [13]). A similar approach underlies Winograd's seminal work on the multiplicative complexity of the DFT, which produced a new class of DFT algorithms [14], [15]. The first book on FFTs by Nussbaumer makes heavy use of the algebraic interpretation of the DFT [16].

Fourier analysis on groups is classic in mathematics, going back to the 19th century [17]. In signal processing, general commutative and finite groups were considered in [18] (including fast algorithms) and are essentially associated with DFTs (of arbitrary dimension). The first proposition of non-commutative groups in SP is due to Karpovsky [19] but it has not found many applications. Notable exceptions include Fourier analysis on the symmetric group to study ranked data [20], on the 2-sphere [21], and on wreath product groups for multi-resolution analysis [22]. Each of these examples is in ASP terms a specific choice of a signal model.

In all this work, groups and group algebras are the algebraic objects of choice. Since shift-invariance requires commutative algebras, as we assert, we need to go beyond group algebras to capture other linear transforms, like the DTTs, within one algebraic framework.

Algebra has played a more significant role in other areas like for example system theory and coding. Algebraic system theory was started in the seminal work of Kalman (see Chapter 10 in [23]) and further developed by others, including [24], [25], [26]. Polynomial algebras play a crucial role but are used differently than in ASP, namely, to study realization, controllability, and observability in linear systems. Similarly, algebraic coding theory is standard [27] and makes heavy use of polynomial algebras. One reason is that finite fields are polynomial algebras over prime-size fields, but polynomial algebra also provide the structure for certain linear codes (e.g., cyclic codes).

Organization. We start by identifying the algebraic structure and basic assumptions underlying SP in Section II and introduce the concept of signal model on which ASP is built. Section III captures and derives basic SP concepts from a given signal model. In Section IV we specialize ASP to finite, shift-invariant SP which means signal models built from polynomial algebras. Section V constructs infinite and finite 1-D time models from basic assumptions and gives detailed insight into possible choices and the need for boundary conditions. We

conclude with Section VI.

II. FOUNDATION: SIGNAL MODEL

As stated in the introduction, by SP we mean *linear* signal processing. In this section, we first explain why SP naturally falls into the framework of algebra and then define the *signal model*. Once a signal model is given, spectrum, Fourier transform, and other SP concepts are automatically defined as we will show in Section III.

A. The Algebraic Structure in Signal Processing

Algebra studies algebraic structures. An algebraic structure is a set (or a collection of sets) with operations (such as addition and multiplication) that satisfy certain properties such as the distributive law. Examples of algebraic structures include groups, rings, fields, and vector spaces. Each one of these spawns its own structure theory. For example, linear algebra is the theory of vector spaces. Hence, to investigate the algebraic structure in SP, we start by identifying the crucial sets and their available operations.

Sets. The basic sets used in SP are the set of signals \mathcal{M} and the set of filters \mathcal{A} .

Operations. The set of signals \mathcal{M} is usually assumed to be a *vector space*: signals can be added and multiplied by a scalar α (from the base field), to yield a new signal. Formally,

$$\begin{aligned} \text{signal} + \text{signal} &= \text{signal}, \\ \alpha \cdot \text{signal} &= \text{signal}. \end{aligned}$$

The structure of a vector space gives access to dimension, basis, linear mapping, subspace, and other related notions.

In SP, signals are processed by linear systems², commonly called *filters*. In block diagram form

$$\text{signal} \longrightarrow \boxed{\text{filter}} \longrightarrow \text{signal} \quad (1)$$

By writing the filter operation formally as multiplication \cdot we can write (1) as

$$\text{filter} \cdot \text{signal} = \text{signal}.$$

Multiplication of a signal in \mathcal{M} by a filter in \mathcal{A} can take different forms depending on the representation of signals and filters, e.g., convolution (in the time domain), standard multiplication (in the z -transform domain), or any other adequate form, as long as certain properties are satisfied, e.g., the distributive law:

$$\begin{aligned} &\text{filter} \cdot (\text{signal} + \text{signal}) \\ &= \text{filter} \cdot \text{signal} + \text{filter} \cdot \text{signal}. \end{aligned}$$

Next, we determine the algebraic structure of the filter space \mathcal{A} . Filters can be added, multiplied, and multiplied by a scalar α from the base field; formally,

$$\begin{aligned} \text{filter} + \text{filter} &= \text{filter} \quad (\text{parallel connection}), \\ \alpha \cdot \text{filter} &= \text{filter} \quad (\text{amplification}), \\ \text{filter} \cdot \text{filter} &= \text{filter} \quad (\text{series connection}) \end{aligned}$$

²We only consider single-input single-output linear (SISO) systems in this paper. Extensions to multiple-input multiple-output (MIMO) systems are under research.

The first two make \mathcal{A} a vector space. In addition, multiplication in \mathcal{A} is defined, which is not the case in \mathcal{M} . Note that multiplication of two filters and multiplication of a filter (element of \mathcal{A}) and a signal (element of \mathcal{M}), though written using the same symbol \cdot , are algebraically different.

Algebraic description. Sets with the above operations are well-known in algebra. The filter space is an *algebra* \mathcal{A} (i.e., a vector space that is also a ring, i.e., with multiplication of its elements defined). It operates on the signal vector space \mathcal{M} , making the signal space \mathcal{M} an \mathcal{A} -*module*. The operation of \mathcal{A} on \mathcal{M} is filtering.

set of filters/linear systems = algebra \mathcal{A} set of signals = \mathcal{A} -module \mathcal{M}

The exact definitions of algebra and module are given in Appendix I. The theory of algebras and associated modules is known as the *representation theory of algebras*. For an introduction to representation theory, we refer to [28], [29], [30].

Example: Infinite discrete time. In infinite discrete time SP, the algebra commonly used consists of filters whose z -domain representation has absolute summable coefficient sequences³

$$\mathcal{A} = \{h = \sum_{n \in \mathbb{Z}} h_n z^{-n} \mid \mathbf{h} = (\dots, h_{-1}, h_0, h_1, \dots) \in \ell^1(\mathbb{Z})\}. \quad (2)$$

We use bold-faced symbols like \mathbf{h} to denote coordinate representations, i.e., sequences of scalars from the base field (such as \mathbb{C}). The corresponding element of an algebra (or module below) is written unbolded like h .

The associated module is commonly assumed to be the space of finite energy signals, in the z -domain given by

$$\mathcal{M} = \{s = \sum_{n \in \mathbb{Z}} s_n z^{-n} \mid \mathbf{s} = (\dots, s_{-1}, s_0, s_1, \dots) \in \ell^2(\mathbb{Z})\}. \quad (3)$$

We provide a proof that \mathcal{M} in (3) is indeed an \mathcal{A} -module (i.e., closed under filtering) in [9].

Note that in ASP we consider \mathcal{A} and \mathcal{M} as spaces of series and not immediately as spaces of complex functions. This means that the difference between, e.g., \mathbf{s} and s is that the latter makes a basis explicit for which the former is the coordinate vector.

B. Signal Model

ASP provides an axiomatic approach to SP. It does so by identifying the fundamental objects that are needed to develop an SP theory.

Clearly, we need filter and signal space, i.e., an algebra and an associated module as explained above. However, in SP applications, signals are usually identified as elements of a vector space V and not as elements of modules. For example, in the discrete case, which is the focus of this paper, signals are infinite or finite sequences \mathbf{s} of numbers from the base field (which we assume to be complex for now) over some index

range I : $\mathbf{s} \in \mathbb{C}^I$. For finite $I = \{0, \dots, n-1\}$, $V = \mathbb{C}^I = \mathbb{C}^n$; for $I = \mathbb{N}, \mathbb{Z}$, we usually consider $V = \ell^1(I)$ or $V = \ell^2(I)$.

To define filtering, we need to assign to V a module \mathcal{M} with associated algebra (i.e., filter space). This is done through a bijective linear mapping $\Phi : V \rightarrow \mathcal{M}$. For example, in infinite discrete time SP, Φ is the well-known z -transform

$$\begin{aligned} \Phi : \ell^2(\mathbb{Z}) &\rightarrow \mathcal{M} \\ \mathbf{s} &\mapsto s = S(z) = \sum_{n \in \mathbb{Z}} s_n z^{-n}, \end{aligned} \quad (4)$$

where \mathcal{M} is defined in (3).

As we will show later, the three objects \mathcal{A} , \mathcal{M} , and Φ are indeed sufficient to develop a theory of SP, e.g., to define spectrum, Fourier transforms, and other concepts. Hence we collect these objects in a triple called a *signal model*.

Definition 1 (Linear Signal Model) Let $V \leq \mathbb{C}^I$ be a vector space of complex valued signals over a discrete index domain I . A *discrete linear signal model*, or just signal model, for V is a triple $(\mathcal{A}, \mathcal{M}, \Phi)$, where \mathcal{A} is an algebra of filters, \mathcal{M} is an \mathcal{A} -module of signals with $\dim(\mathcal{M}) = \dim(V)$, and

$$\Phi : V \rightarrow \mathcal{M} \quad (5)$$

is a bijective linear mapping. If \mathcal{A}, \mathcal{M} are clear from the context, we sometimes refer to Φ as the signal model. Further, we transfer properties from \mathcal{M} to the signal model. For example, we say the signal model is finite, if \mathcal{M} is finite-dimensional.

Example: Infinite discrete time model. Continuing the previous example, the signal model usually adopted for infinite discrete time SP is

$$(\mathcal{A}, \mathcal{M}, \Phi) \quad (6)$$

with \mathcal{A} from (2), \mathcal{M} from (3), and Φ from (4).

Remarks on the signal model. If \mathcal{M} is of dimension n with basis⁴ $b = (b_0, \dots, b_{n-1})$ and $\mathbf{s} \in \mathbb{C}^n$, then

$$\Phi(\mathbf{s}) = s = \sum_{i=0}^{n-1} s_i b_i \quad (7)$$

defines a signal model for $V = \mathbb{C}^n$. Conversely, if Φ is any signal model for V with canonical basis \mathbf{e}_i (i th element in \mathbf{e}_i is 1; all other elements are 0), then the list of all $b_i = \Phi(\mathbf{e}_i)$ is a basis of \mathcal{M} (since Φ is bijective) and thus Φ has the form in (7). In other words, the signal model implicitly chooses a basis in \mathcal{M} and Φ is dependent on this basis.

Definition 1 makes it possible to apply different signal models to the same vector of numbers. For example, application of a DFT or a DCT to compute the spectrum of a finite-length vector \mathbf{s} *implicitly adopts different signal models for this vector* (Section V-B and [1]).

We remark that Definition 1 of the signal model and the algebraic theory extend to the case of continuous (index) signals. However, in this paper, we will not pursue this extension and limit ourselves to discrete (index) signals.

³Replacing ℓ^1 with ℓ^2 in (2) destroys the algebra structure: the concatenation or multiplication of two ℓ^2 filters is in general not an ℓ^2 filter.

⁴In this paper b will always denote a basis and b_i always basis elements, i.e., elements (or signals) in \mathcal{M} , which should not be confused with scalars such as s_i, h_i .

III. ALGEBRA AND SIGNAL PROCESSING

We claimed that, given a signal model for a vector space V , the major ingredients for SP on V are automatically defined. This section confirms this claim. We show that signals, filters, convolution, spectrum, Fourier transform, frequency response, shift, shift-invariance have their abstract analogue in ASP and can be derived from the signal model. Understanding and exploiting the benefits of this connection between SP concepts and their algebraic equivalents helps us to develop new SP frameworks, or signal models, different from standard time SP.

In this section we assume a given signal model $(\mathcal{A}, \mathcal{M}, \Phi)$ for a vector space $V \leq \mathbb{C}^I$ with

$$\Phi : V \rightarrow \mathcal{M}, \quad \mathbf{s} \mapsto \sum_{i \in I} s_i b_i. \quad (8)$$

As remarked before, this implies that the b_i form a basis for \mathcal{M} . This basis is automatically fixed by the model. Further, we assume that the base field is \mathbb{C} , i.e., both \mathcal{A} and \mathcal{M} are \mathbb{C} -vector spaces. Other base fields are of course possible.

As a running example, we use the infinite discrete time model in (6).

A. Basic Algebraic Versus SP Concepts

Algebra (filter space). The filters are given by the elements $h \in \mathcal{A}$. Serial and parallel connection of filters are defined through the properties of \mathcal{A} (see Appendix I).

As seen before, in infinite discrete time, \mathcal{A} is given by (2).

Module (signal space). The signals are the elements $s \in \mathcal{M}$. Filtering is automatically defined as the operation of \mathcal{A} on \mathcal{M} and $h \cdot s \in \mathcal{M}$ is ensured by the axioms defining the module.

The basis elements b_i of \mathcal{M} fixed by the model via (8) are the impulses. The impulse response of a filter for this impulse is $hb_i \in \mathcal{M}$.

In infinite discrete time, \mathcal{M} is given by (3). The impulses are the $b_i = z^{-i}$.

Regular module (filter space = signal space). An important module associated with an algebra is the *regular* module which is \mathcal{A} itself: $\mathcal{M} = \mathcal{A}$ with the operation of \mathcal{A} on \mathcal{M} being the multiplication available in \mathcal{A} . We call a signal model with $\mathcal{M} = \mathcal{A}$ a *regular* signal model. Note that even if $\mathcal{A} = \mathcal{M}$ as sets, the algebraic structures of \mathcal{A} and \mathcal{M} (i.e., which operations are allowed) are different.

The infinite discrete time model in (6) is not regular.

Representations (filters as matrices). As a consequence of the module axioms (Appendix I), a fixed filter $h \in \mathcal{A}$ can multiply every signal $s \in \mathcal{M}$ and defines a linear mapping on \mathcal{M} given by

$$s \mapsto h \cdot s. \quad (9)$$

Thus, with respect to the basis $b = (b_i)_{i \in I}$ fixed via (8), every h is expressed by a matrix M_h (possibly, countably infinite if $|I|$ is countably infinite). As usual with linear mappings, M_h is obtained by applying h to each base vector b_i ; the coordinate vector of the result hb_i is the i th column of M_h .

By constructing M_h for every filter $h \in \mathcal{A}$, we obtain a mapping ϕ from the filter algebra \mathcal{A} to the algebra of $|I| \times |I|$ matrices $\mathbb{C}^{|I| \times |I|}$:

$$\phi : \mathcal{A} \rightarrow \mathbb{C}^{|I| \times |I|}, \quad h \mapsto \phi(h) = M_h. \quad (10)$$

The mapping ϕ is a *homomorphism* of algebras, i.e., a mapping that preserves the algebra structure (see Definition 8 in Appendix D). In particular, $\phi(h + h') = \phi(h) + \phi(h')$ and $\phi(hh') = \phi(h)\phi(h')$. The homomorphism ϕ is called the *(matrix) representation of \mathcal{A} afforded by the \mathcal{A} -module \mathcal{M} with basis b* and is fixed by the chosen signal model.

Through the representation, abstract filtering (multiplication of $s \in \mathcal{M}$ by $h \in \mathcal{A}$) becomes in coordinates a matrix-vector multiplication:

$$h \cdot s \Leftrightarrow \phi(h) \cdot \mathbf{s}. \quad (11)$$

This coordinatization of filtering also shows the fundamental difference between signals and filters; namely, in coordinates, signals become vectors, and filters (as linear operators on signals) become matrices.

In the infinite discrete time model, as is well-known, the $\phi(h)$ are infinite Toeplitz matrices.

Irreducible submodule (spectral component). If \mathcal{M} is an \mathcal{A} -module, then a subvector space $\mathcal{M}' \leq \mathcal{M}$ is an \mathcal{A} -submodule of \mathcal{M} if \mathcal{M}' is itself an \mathcal{A} -module, i.e., closed or invariant under the operation of \mathcal{A} . Most subvector spaces fail to be \mathcal{A} -submodules; intuitively, the smaller the vector space \mathcal{M}' is, the harder it is to remain invariant under \mathcal{A} .

A submodule $\mathcal{M}' \leq \mathcal{M}$ is *irreducible* if it contains no proper submodules, i.e., no submodules besides the trivial submodules $\{0\}$ and \mathcal{M}' itself.

In particular, every one-dimensional submodule \mathcal{M}' has to be irreducible and is an eigenspace simultaneously for all filters $h \in \mathcal{A}$; i.e., $hs = \lambda_h s$ for all $s \in \mathcal{M}'$ with a suitable $\lambda_h \in \mathbb{C}$. We call each irreducible module a spectral component of \mathcal{M} and each element in it a *pure frequency* and write f instead of s to emphasize it.

We write the collection of all irreducible submodules as \mathcal{M}_ω , $\omega \in W$, where W is a suitable index domain.

In the infinite discrete time model, there is an irreducible submodule \mathcal{M}_ω of dimension one for every $\omega \in (-\pi, \pi]$, spanned by

$$f_\omega = F_\omega(z) = \sum_{n \in \mathbb{Z}} e^{j\omega n} z^{-n}.$$

Indeed, for arbitrary $h = H(z) \in \mathcal{A}$,

$$hf_\omega = H(e^{j\omega})f_\omega \in \mathcal{M}_\omega, \quad (12)$$

which confirms that \mathcal{M}_ω is an \mathcal{A} -module.⁵

Irreducible representations (frequency response). We choose in each irreducible module, or spectral component \mathcal{M}_ω of \mathcal{M} a basis b_ω . Then \mathcal{M}_ω affords a representation ϕ_ω of \mathcal{A} called irreducible representation:

$$\phi_\omega : \mathcal{A} \rightarrow \mathbb{C}^{d_\omega \times d_\omega}, \quad h \mapsto \phi_\omega(h),$$

⁵To be precise, \mathcal{M}_ω is an \mathcal{A} -module but not a *submodule* of \mathcal{M} since $\mathbf{1}_\omega \notin \ell^2(\mathbb{Z})$ —a problem with infinite index domains. Besides that the theory remains intact.

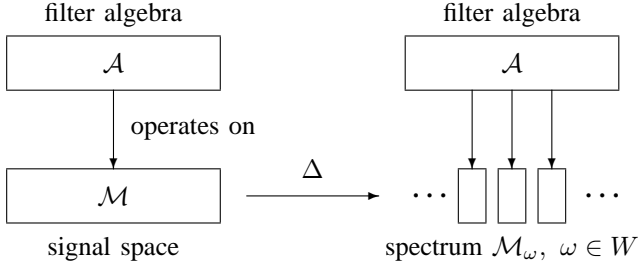


Fig. 1. A visualization of the concept Fourier transform, which decomposes the \mathcal{A} -module \mathcal{M} into a direct sum of irreducible (minimal) \mathcal{A} -invariant subspaces, i.e., \mathcal{A} -submodules. The latter are called the spectrum of \mathcal{M} .

where $d_\omega = \dim(\mathcal{M}_\omega)$. The matrix $\phi_\omega(h)$ is the frequency response of h at frequency ω . The collection of all $\phi_\omega(h)$, $\omega \in W$, is the frequency response of h .

In infinite discrete time, (12) shows that $\phi_\omega(h) = H(e^{j\omega}) \in \mathbb{C}^{1 \times 1} = \mathbb{C}$ as expected.

Module decomposition (spectrum, Fourier transform). It may be possible to decompose the module \mathcal{M} into a direct sum of its irreducible modules. The mapping

$$\begin{aligned} \Delta: \mathcal{M} &\rightarrow \bigoplus_{\omega \in W} \mathcal{M}_\omega, \\ s &\mapsto (s_\omega)_{\omega \in W}. \end{aligned} \quad (13)$$

is then the Fourier transform for the signal model and is invertible.⁶ The existence of such a decomposition, and hence of the Fourier transform, is not guaranteed; it depends on \mathcal{A} and \mathcal{M} . See Fig. 1 for a visualization of the Fourier transform.

With respect to the fixed basis b of \mathcal{M} and chosen bases $b_\omega \in \mathcal{M}_\omega$, we obtain the coordinate form of Δ as

$$\begin{aligned} \mathcal{F}: V &\rightarrow \bigoplus_{\omega \in W} \mathbb{C}^{\dim(\mathcal{M}_\omega)}, \\ \mathbf{s} &\mapsto (\mathbf{s}_\omega)_{\omega \in W}. \end{aligned} \quad (14)$$

In infinite discrete time, for $s = S(z) \in \mathcal{M}$, i.e., $\mathbf{s} \in \ell^2(\mathbb{Z})$, $\dim(\mathcal{M}_\omega) = 1$, $\omega \in (-\pi, \pi]$, i.e., all modules are of dimension 1, and the tuple $(s_\omega)_{\omega \in W}$ is a (scalar) function $\mathcal{F}(\mathbf{s}) = S(e^{j\omega})$, $\omega \in (-\pi, \pi]$. This is in general not the case; different ω may be associated with modules of different dimensions. An example is the real discrete Fourier transform (RDFT) discussed in Section V-C.

The Fourier transform is an \mathcal{A} -module homomorphism (see Definition 9 in Appendix I), which means that $\Delta(h \cdot s) = h \cdot \Delta(s)$ for $h \in \mathcal{A}$, $s \in \mathcal{M}$. In words, this means that filtering in the signal space \mathcal{M} is equivalent to parallel filtering in the spectrum (as visualized in Fig. 1):

$$(h \cdot s)_\omega = h \cdot s_\omega, \quad \text{for all } \omega \in W. \quad (15)$$

$\Delta(h \cdot s) = h \cdot \Delta(s)$ also yields a general convolution theorem:

$$h \cdot s = \Delta^{-1}(h \cdot \Delta(s)). \quad (16)$$

⁶The spectral components s_ω of s should not be confused with the coordinates s_ℓ of s .

B. Shift-Invariance

Section III-A illustrated that once a signal model is given, basic SP concepts are available. From a practical point of view, this means that we can construct a large number of distinct SP frameworks with different notions of filtering, spectrum, and Fourier transform. In this section, we narrow down the choices by imposing shift-invariance on a signal model. For finite (-dimensional) signal models, this will identify polynomial algebras as key structures in SP.

Shifts (generators of filter algebra). The *shift* operator is a special filter, and thus is an element⁷ $x \in \mathcal{A}$. Further, it is common to require that *every* filter $h \in \mathcal{A}$ be expressed as a polynomial or series in the shift operator x . In algebraic terms, this means that the shift operator generates⁸ the algebra \mathcal{A} .

The same holds if multiple shifts are available:

$$\text{shift(s)} = \text{chosen generator(s) of } \mathcal{A}$$

In the infinite discrete time model, the shift is $x = z^{-1}$.

Shift-invariant signal models. A key concept in SP is *shift-invariance*. In ASP this property takes a very simple form. Namely, if x is a shift and h a filter, then h is shift-invariant, if for all signals s , $h(xs) = x(hs)$, which is equivalent to

$$x \cdot h = h \cdot x, \quad \text{for all } h \in \mathcal{A}. \quad (17)$$

Since the shifts generate \mathcal{A} , \mathcal{A} is necessarily commutative in this case.⁹ Conversely, if \mathcal{A} is a commutative algebra then (17) holds:

$$\text{shift-invariant signal model} \Leftrightarrow \mathcal{A} \text{ is commutative}$$

In 1-D SP only one shift is available, in k -D SP k shifts are needed. We focus on the case of one shift and identify possible commutative algebras. The discussion for more shifts is analogous.

Commutative algebras of infinite dimension are spaces of series in x such as \mathcal{A} in (2). Finite-dimensional commutative algebras generated by x are exactly the *polynomial algebras*

$$\mathcal{A} = \mathbb{C}[x]/p(x), \quad p \text{ a polynomial of degree } n.$$

$\mathbb{C}[x]/p(x)$ is the set of all polynomials of degree less than n with addition and multiplication modulo $p(x)$. As a vector space, \mathcal{A} has dimension n .

Thus, imposing only shift-invariance, we have identified one of the key players in ASP, namely polynomial algebras. Indeed, as we will see, they provide the underlying structure for finite time SP and the DFT (Section IV) and for finite space SP and the DCTs/DSTs [1].

⁷We write x instead of z^{-1} to emphasize the abstract nature of the discussion. Later, this will enable us to introduce without additional effort other shifts as well.

⁸This is not entirely correct, as, in a strict sense, one element x can only generate polynomials in x (and x^{-1} if x is invertible), not infinite series. However, by completing the space with respect to some norm the notion of generating can be expanded. We gloss over this detail to focus on the algebraic nature of the discussion.

⁹The requirement of “ x generating \mathcal{A} ” is indeed necessary as there are linear shift-invariant systems that cannot be expressed as convolutions, i.e., as series in x ; see [31].

Further, by allowing more than one shift and hence polynomial algebras in several variables, ASP enables the derivation of 2-D (and higher-dimensional) SP frameworks including nonseparable ones [3], [2].

Finally, we note that noncommutative algebras are allowed in ASP but necessarily yield shift-variant SP. For example, this is the case for Fourier analysis on noncommutative finite groups [32], which, in ASP terms, considers regular signal models with $\mathcal{A} = \mathcal{M} = \mathbb{C}[G]$, the group algebra for a finite group G . Note that the set of polynomial algebras and the set of group algebras are different and intersect only for the case of commutative groups. A more detailed discussion is in [9].

Visualization of a signal model. A given signal model can be visualized by a graph, which provides an intuitive understanding of the model.

Definition 2 (Visualization of Signal Model) Assume that a signal model $(\mathcal{A}, \mathcal{M}, \Phi)$ is given as in (8). Denote the chosen shift operators, i.e., generators, of \mathcal{A} by x_1, \dots, x_n . Further, assume that ϕ is the representation of \mathcal{A} afforded by \mathcal{M} with basis b . Then each $\phi(x_i)$ is an infinite or finite matrix (which we call *shift matrix*) and can be viewed as the adjacency matrix of a weighted graph \mathcal{G}_i . Each of these graphs has the same vertices corresponding to b . Thus we can join these graphs by adding the adjacency matrices of the \mathcal{G}_i to obtain a graph \mathcal{G} . We call this graph the *visualization* of the signal model $(\mathcal{A}, \mathcal{M}, \Phi)$.

Intuitively, the graph provides the topology imposed by the signal model. For example the infinite discrete time model has the visualization shown in Fig. 2. The vertices are the base elements $b_i = x^i = z^{-i}$, the edges show the shift operation.

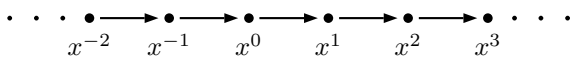


Fig. 2. Visualization of the infinite discrete time model (6).

C. Summary

We summarize the correspondence between algebraic concepts and signal processing concepts in Table I. The signal processing concepts are given in the first column and their algebraic counterparts in the second column. With respect to the basis fixed by the signal model we obtain the corresponding coordinate versions in the third column. In coordinates, the algebraic objects, operations, and mappings become vectors and matrices and thus allow for actual computation. This is the form used in signal processing. However, the coordinate version hides the underlying algebraic structure, which often cannot be easily recovered if it is not known beforehand.

IV. FINITE, SHIFT-INVARIANT, 1-D SIGNAL MODELS

In Section III-B, we have learned that, for finite shift-invariant signal models $(\mathcal{A}, \mathcal{M}, \Phi)$, \mathcal{A} is a polynomial algebra. In particular, in the case of finite 1-D (one shift) signal models, these algebras are necessarily of the form $\mathbb{C}[x]/p(x)$. With this motivation, we investigate what it means to do signal

processing using these algebras. We do this by specializing the general theory from Section III.

The mathematics of polynomial algebras is well-known (e.g., [33]). The purpose of this section is to connect it to SP using the general ASP framework.

We focus on regular models, i.e., $\mathcal{A} = \mathcal{M} = \mathbb{C}[x]/p(x)$. As running example, we will use what we call the *finite discrete time model*. The motivation for this notion will become clear as we proceed.

Polynomial algebras in one variable. Let $p(x)$ be a polynomial of degree $\deg(p) = n$. Then, $\mathcal{A} = \mathbb{C}[x]/p(x) = \{h(x) \mid \deg(h) < n\}$, called the set of residue classes modulo p , is an algebra with respect to the addition of polynomials, and the polynomial multiplication modulo p . We call \mathcal{A} a *polynomial algebra (in one variable)*. \mathcal{A} can be generated by one element, usually chosen to be x .

As an example, consider $p(x) = x^n - 1$, i.e., $\mathcal{A} = \mathbb{C}[x]/(x^n - 1)$. In \mathcal{A} , multiplying, for example, x and x^{n-1} yields $x \cdot x^{n-1} = x^n \equiv 1 \pmod{x^n - 1}$. The last equality is read as “ x^n is congruent 1 modulo $x^n - 1$.” Thus, we do not use “mod” as an operator but to denote equality of two polynomials modulo a third polynomial.

A. Signal Model

General case. We consider $\mathcal{A} = \mathcal{M} = \mathbb{C}[x]/p(x)$ with $\deg(p) = n$, and choose a basis $b = (p_0, \dots, p_{n-1})$ of \mathcal{M} . This defines a signal model for $V = \mathbb{C}^n$; namely, for $\mathbf{s} = (s_0, \dots, s_{n-1})^T \in \mathbb{C}^n$, we can define the bijective linear mapping Φ as

$$\Phi : \mathbb{C}^n \rightarrow \mathcal{M}, \mathbf{s} \mapsto \sum_{0 \leq \ell < n} s_\ell p_\ell. \quad (18)$$

Φ in (18) is the equivalent of the z -transform for this model. Filtering in this model is the multiplication $h(x)s(x) \pmod{p(x)}$ for $h \in \mathcal{A}$ and $s \in \mathcal{M}$. The shift in this model is $x \in \mathcal{A}$. The basis elements p_i are the unit impulses in \mathcal{M} , i.e., \mathbf{p}_i is a canonical base vector. The impulse response of a filter $h \in \mathcal{A}$ for the impulse p_i is $hp_i \in \mathcal{M}$.

Example. Our running example will be the finite discrete time model defined as

$$\begin{aligned} \mathcal{A} = \mathcal{M} &= \mathbb{C}[x]/(x^n - 1), \\ \Phi : \mathbb{C}^n \rightarrow \mathcal{M}, \mathbf{s} &\mapsto \sum_{0 \leq \ell < n} s_\ell x^\ell. \end{aligned} \quad (19)$$

We call Φ the *finite z -transform*. It fixes the basis $b = (1, x, \dots, x^{n-1})$ in \mathcal{M} .

B. Filtering

General case. As said above, filtering in the signal model defined in (18) is the multiplication of polynomials (filter h and signal s) modulo p . In coordinates, filtering becomes the matrix-vector multiplication

$$hs \in \mathcal{M} \leftrightarrow \phi(h) \cdot \mathbf{s} \in \mathbb{C}^n, \quad (20)$$

where $\phi(h) \in \mathbb{C}^{n \times n}$. The i th column of $\phi(h)$ is exactly the coordinate vector of the impulse response hp_i . The representation of \mathcal{A} associated with the signal model is $\phi : \mathcal{A} \rightarrow \mathbb{C}^{n \times n}$.

We call the $\phi(h)$ filter matrices; $\phi(x)$ is the *shift matrix*.

TABLE I
CORRESPONDENCE BETWEEN DISCRETE SIGNAL PROCESSING CONCEPTS AND ALGEBRAIC CONCEPTS.

signal processing concept	algebraic concept (coordinate free)	in coordinates
filter	$h \in \mathcal{A}$ (algebra)	$\phi(h) \in \mathbb{C}^{I \times I}$
signal	$s = \sum s_i b_i \in \mathcal{M}$ (\mathcal{A} -module)	$\mathbf{s} = (s_i)_{i \in I} \in \mathbb{C}^I$
filtering	$h \cdot s$	$\phi(h) \cdot \mathbf{s}$
impulse	base vector $b_i \in \mathcal{M}$	$\mathbf{b}_i = (\dots, 0, 1, 0, \dots)^T \in \mathbb{C}^I$
impulse response of $h \in \mathcal{A}$	$h \cdot b_i \in \mathcal{M}$	$\phi(h) \cdot \mathbf{b}_i \in \mathbb{C}^I$
Fourier transform	$\Delta : \mathcal{M} \rightarrow \bigoplus_{\omega \in W} \mathcal{M}_\omega$	$\mathcal{F} : \mathbb{C}^I \rightarrow \bigoplus_{\omega \in W} \mathbb{C}^{d_\omega} \Leftrightarrow \phi \rightarrow \bigoplus_{\omega \in W} \phi_\omega$
spectrum of signal	$\Delta(s) = (s_\omega)_{\omega \in W}$	$\mathcal{F}(\mathbf{s}) = (\mathbf{s}_\omega)_{\omega \in W}$
frequency response of $h \in \mathcal{A}$	n.a.	$(\phi_\omega(h))_{\omega \in W}$
shift(s)	generator(s) x of \mathcal{A}	$\phi(x)$
shift-invariance	\mathcal{A} is commutative	n.a.

Example. In our example, the filter matrix for a generic filter $\sum_{0 \leq k < n} h_k x^k$ is readily computed as

$$\phi(h) = \begin{bmatrix} h_0 & h_{n-1} & h_{n-2} & \dots & h_1 \\ h_1 & h_0 & h_{n-1} & \dots & h_2 \\ h_2 & h_1 & h_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & h_{n-1} \\ h_{n-1} & \dots & h_2 & h_1 & h_0 \end{bmatrix}. \quad (21)$$

Hence, the filter matrices in this model are precisely the circulant matrices. Filtering in coordinates, $\phi(h)\mathbf{s}$, is exactly circular convolution.

C. Visualization

General case. The visualization of the signal model $(\mathcal{A}, \mathcal{M}, \Phi)$ with Φ in (18) is the graph with n vertices that has the shift matrix $\phi(x)$ as adjacency matrix (see Definition 2). In the general case the graph has no apparent structure.

Example. In our example (19), the shift matrix $\phi(x)$ is a special case of (21), namely the cyclic shift

$$\phi(x) = \begin{bmatrix} 0 & & & & 1 \\ 1 & 0 & & & \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & 0 \end{bmatrix}, \quad (22)$$

This yields the visualization as a circle shown in Fig. 3.

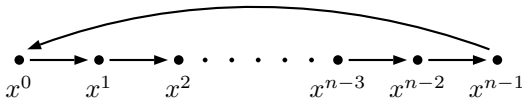


Fig. 3. Visualization of the finite discrete time model in (19).

D. Spectrum and Fourier Transform

General case. We assume that $p(x)$ has pairwise distinct zeros:

$$p(x) = \prod_{k=0}^{n-1} (x - \alpha_k), \quad \alpha_k \neq \alpha_\ell, \text{ for } k \neq \ell,$$

and set $\alpha = (\alpha_0, \dots, \alpha_{n-1})$.

The Fourier transform, or spectral decomposition, of the regular module $\mathcal{M} = \mathbb{C}[x]/p(x)$ is given by the Chinese remainder theorem (CRT; stated in Theorem 10 in Appendix I).

In coordinate-free form, the Fourier transform is given by the mapping

$$\Delta : \mathbb{C}[x]/p(x) \rightarrow \mathbb{C}[x]/(x - \alpha_0) \oplus \dots \oplus \mathbb{C}[x]/(x - \alpha_{n-1}), \\ s = s(x) \mapsto (s(\alpha_0), \dots, s(\alpha_{n-1})). \quad (23)$$

Each $\mathcal{M}_k = \mathbb{C}[x]/(x - \alpha_k)$ is of dimension 1. So the elements of $\mathbb{C}[x]/(x - \alpha_k)$ are polynomials of degree 0, i.e., scalars $c \in \mathbb{C}$. Further, each \mathcal{M}_k is an \mathcal{A} -module, since for $h = h(x) \in \mathcal{A}$ and $c \in \mathcal{M}_k$,

$$h(x) \cdot c \equiv h(\alpha_k) \cdot c \pmod{(x - \alpha_k)},$$

i.e., the result is again in \mathcal{M}_k . Since \mathcal{M}_k is of dimension 1, it is irreducible.

The scalars $s(\alpha_k)$ in (23) are the spectral components of s . The mapping in (23) simultaneously projects a signal (i.e., polynomial) $s \in \mathbb{C}[x]/p(x)$ into the modules $\mathbb{C}[x]/(x - \alpha_k)$. This projection is precisely the evaluation

$$s(x) \equiv s(\alpha_k) \pmod{(x - \alpha_k)}.$$

The set of the one-dimensional irreducible modules $\mathcal{M}_k = \mathbb{C}[x]/(x - \alpha_k)$, $0 \leq k < n$, is the *spectrum* of the signal space \mathcal{M} . Each \mathcal{M}_k is an eigenspace simultaneously for all filters (or linear systems) in \mathcal{A} . The spectrum of a signal $s \in \mathcal{M}$ is the vector $\Delta(s) = (s(\alpha_0), \dots, s(\alpha_{n-1}))$.

The pure frequencies f_k associated with \mathcal{M}_k are those elements of \mathcal{M} that are mapped to a canonical base vector: $\Delta(f_k) = e_k$. This implies $f_k(\alpha_i) = 1$ for $i = k$ and $= 0$ for $i \neq k$. This is an interpolation problem, and the solution is well known and given by the Lagrange polynomial [33]

$$f_k = \prod_{i \neq k} (x - \alpha_i) / \prod_{i \neq k} (\alpha_k - \alpha_i). \quad (24)$$

With this we see that Δ enables us to express a signal s as a linear combination of pure frequencies, namely $s = \sum_{0 \leq k < n} s(\alpha_k) f_k$.

Example. In our example, $x^n - 1 = 0$ has pairwise distinct zeros $\alpha_k = \omega_n^k$ with $\omega_n = e^{-2\pi j/n}$. Thus, spectrum and

Fourier transform of the model (19) are given by

$$\begin{aligned} \Delta : \mathbb{C}[x]/(x^n - 1) &\rightarrow \bigoplus_{0 \leq k < n} \mathbb{C}[x]/(x - \omega_n^k) \\ s = s(x) &\mapsto (s(\omega_n^0), \dots, s(\omega_n^{n-1})). \end{aligned} \quad (25)$$

The pure frequency f_k is given by

$$f_k = \prod_{i \neq k} (x - \omega_n^i) / \prod_{i \neq k} (\omega_n^k - \omega_n^i). \quad (26)$$

This expression can be simplified as explained later.

E. Frequency Response

General case. Filtering in the regular module $\mathcal{M} = \mathbb{C}[x]/p(x)$ becomes parallel filtering in the frequency domain, i.e., on the irreducible \mathcal{A} -modules \mathcal{M}_k . Namely, let $h \in \mathcal{A}$ be any filter and let $s(\alpha_k) \in \mathcal{M}_k$ be a spectral component of the signal s . Then filtering by h yields

$$h(x)s(\alpha_k) \equiv h(\alpha_k)s(\alpha_k) \pmod{(x - \alpha_k)}.$$

This shows that \mathcal{M}_k affords the irreducible representation

$$\phi_k : h = h(x) \mapsto h(\alpha_k). \quad (27)$$

The collection of the $\phi_k(h)$, namely, $(h(\alpha_0), \dots, h(\alpha_{n-1}))$ is the frequency response of the filter h . This means that the k th spectral component $s(\alpha_k)$ of a signal $s = s(x)$ is obtained in the same way as the frequency response $h(\alpha_k)$ at α_k , namely by evaluating polynomials. This is a special property of polynomial algebras.

Example. In our example (19), the frequency response of $h \in \mathcal{A}$ is the collection $h(\omega_n^k)$, $0 \leq k < n$.

F. Fourier Transform as Matrix

General case. The Fourier transform Δ in (23) is a linear mapping, which is expressed by a matrix \mathcal{F} after bases are chosen. We will call this matrix also a Fourier transform for \mathcal{M} . To compute this matrix, we choose the basis $b = (p_0, \dots, p_{n-1})$ in \mathcal{M} , fixed by the signal model (18), and the basis $b_k = (1)$ (the list containing the polynomial $x^0 = 1$) for each summand $\mathbb{C}[x]/(x - \alpha_k)$. The columns of \mathcal{F} are precisely the coordinate vectors of $\Delta(p_\ell)$, $0 \leq \ell < n$. Since $p_\ell(x) \equiv p_\ell(\alpha_k) \pmod{(x - \alpha_k)}$, we get

$$\mathcal{F} = \mathcal{P}_{b,\alpha} = [p_\ell(\alpha_k)]_{0 \leq k, \ell < n}. \quad (28)$$

We call $\mathcal{P}_{b,\alpha}$ a *polynomial transform*. It is uniquely determined by the signal model.

This definition coincides with the notion of a polynomial transform in [34], [35] and is related but different from the use in [36]. In [37], polynomial transforms are called polynomial Vandermonde matrices.

Note that $\mathcal{P}_{b,\alpha}$ can have entries equal to zero, but, as an isomorphism (as stated by the CRT), it is necessarily invertible.

Let $s = s(x) = \sum s_\ell p_\ell(x) \in \mathcal{M}$ be a signal. Then, in coordinates, Δ in (23) becomes a matrix-vector product:

$$\Delta(s) \Leftrightarrow \mathcal{P}_{b,\alpha} \cdot \mathbf{s} = (s(\alpha_0), \dots, s(\alpha_{n-1}))^T \in \mathbb{C}^n. \quad (29)$$

The matrix form \mathcal{F} of Δ in (23) is not uniquely determined. The degree of freedom is in the choice of bases in the

irreducible modules $\mathcal{M}_k = \mathbb{C}[x]/(x - \alpha_k)$. If we choose generic bases $b_k = (a_k)$, $a_k \neq 0$, in \mathcal{M}_k , $0 \leq k < n$, then the Fourier transform \mathcal{F} becomes the *scaled* polynomial transform

$$\text{diag}(1/a_0, \dots, 1/a_{n-1}) \cdot \mathcal{P}_{b,\alpha}.$$

Once \mathcal{F} is chosen, the coordinate vectors \mathbf{f}_k of the pure frequencies in (24) are the $\mathcal{F}^{-1}\mathbf{e}_k$, i.e., the columns of \mathcal{F}^{-1} .

Example. In our example, the (polynomial) Fourier transform associated with (25) is computed as

$$\mathcal{P}_{b,\alpha} = [\omega_n^{k\ell}]_{0 \leq k, \ell < n} = \text{DFT}_n, \quad (30)$$

i.e., it is precisely the discrete Fourier transform, which supports that we call (19) finite discrete time model and Φ in (19) finite z -transform. It also follows that the k th column of DFT_n^{-1} is the coordinate vector \mathbf{f}_k of f_k in (26).

G. Diagonalization Properties and Convolution Theorems

General case. The diagonalization property of any Fourier transform \mathcal{F} of the regular module $\mathcal{M} = \mathbb{C}[x]/p(x)$ is a consequence of the CRT.

Theorem 3 (Diagonalization Properties) Let \mathcal{F} be a Fourier transform for the regular signal model in (18). Then

$$\mathcal{F} \cdot A \cdot \mathcal{F}^{-1} = \text{diag}(a_0, \dots, a_{n-1}), \quad (31)$$

if and only if $A = \phi(h)$ for a filter $h \in \mathcal{A}$. In this case, $a_k = h(\alpha_k)$, $0 \leq k < n$, is the frequency response of h .

In particular, \mathcal{F} diagonalizes the shift matrix $\phi(x)$, and the shift operator x has the frequency response $(\alpha_0, \dots, \alpha_{n-1})$.

Proof: Let $A = \phi(h)$. Then $\mathcal{F}\phi(h)\mathcal{F}^{-1}$ is diagonal, since it is the coordinate representation of the filter h in the frequency domain, which is the diagonal matrix with the frequency response on the diagonal.

Conversely, the set of diagonal matrices $\text{diag}(a_0, \dots, a_{n-1})$ is an n -dimensional vector space. Since \mathcal{F} is invertible, the set of matrices A diagonalized by \mathcal{F} is also n -dimensional. Since \mathcal{A} is of dimension n , and ϕ is injective, the set of all matrices $\phi(h)$ is a vector space of dimension n and thus the set of all matrices diagonalized by \mathcal{F} . ■

We also note that, using Theorem 3, we get immediately the characteristic polynomial, trace, and determinant for every matrix $\phi(h)$, since it is similar to the diagonal matrix $\text{diag}(h(\alpha_0), \dots, h(\alpha_{n-1}))$. In particular, the characteristic polynomial of $\phi(x)$ is $p(\lambda)$.

Theorem 3 is the convolution theorem for the signal model under consideration. Namely, it states that filtering $\phi(h)\mathbf{s}$ in the signal domain becomes pointwise multiplication by the frequency response $\text{diag}(h(\alpha_k))(\mathcal{F}\mathbf{s})$ in the spectral domain.

Example. For our example (19), Theorem 3 yields the well-known fact that the DFT_n diagonalizes the circulant matrices.

V. 1-D TIME MODELS

We presented two signal models as examples of the general algebraic theory: the infinite time model in (6) and the finite time model in (19). The former bore no surprises, but the latter is, as formulated, non-standard in SP and ASP produced

a first small benefit: the proper notion of a finite z -transform. To develop new SP frameworks, not directly related to standard time SP, we present in this section a methodology to derive signal models from basic principles, namely, from the shift operator. This will further shed light on why, for example, the time models look exactly as in (6) and, in particular, as in (19). In the process, we get a deeper appreciation of the difference between the filter and signal spaces (a difference that follows from the axioms of ASP). We also understand the necessity for boundary conditions, the impact of different choices, and how they relate to the problem of signal extension. We use this methodology to derive 1-D and 2-D space signal models in [1] and [3].

For notational convenience, we set as before¹⁰ $x = z^{-1}$. The construction of the infinite and finite time models follows three basic steps: definition of the shift, linear extension, and realization.

A. Constructing the Infinite Time Model

Definition of the shift. Following Kalman [23], when considering discrete time, we need two ingredients: *time marks* t_n and a *shift operator* q .

The time marks are symbolic independent variables $t_n, n \in \mathbb{Z}$; t_n is associated to “time n .” However, time marks alone capture neither the equidistance of the time points nor the directed nature of time. This problem is resolved by the shift operator q and the shift operation \diamond defined as

$$q \diamond t_n = t_{n+1}, \quad n \in \mathbb{Z}. \quad (32)$$

Fig. 4 shows a graphical representation of the time shift.

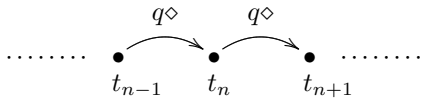


Fig. 4. The time shift $q \diamond t_n$.

Next, we extend the operator domain from the shift operator q to k -fold shift operators q_k , defined by

$$q_k \diamond t_n = t_{n+k}.$$

Clearly, $q_k = q^k$.

At this point of the construction, working only with t_n and q_k , there is no notion of linearity.

Linear extension. To obtain a *linear* signal model, we consider two extensions: 1) we extend linearly the operation \diamond of the shift operator q from the set of the t_n to the set of all formal sums $\sum s_n t_n$: $q \diamond s = \sum s_n (q \diamond t_n)$; and 2) we extend linearly the set of k -fold shift operators q^k to the set of all formal sums $\sum h_k q^k$. The first set will become the module of signals, while the second set will become the algebra of

¹⁰Note that the choice of z^{-1} instead of z in the definition (4) is a convention, not a mathematical necessity; choosing z leads to equivalent properties and an equivalent theory for the z -transform. In fact, the choice of z^{-1} in SP is in contrast to the original mathematical work on Laurent series. The reason may lie on the fact that the shift operator z^{-1} causes a delay of the signal. However, z^{-1} *advances* what we call below the time marks.

TABLE II
REALIZATION OF THE ABSTRACT TIME MODEL.

concept	abstract	realized
shift operator	q	x
shift operation	\diamond	\cdot
time mark	t_n	x^n
k -fold shift operator	$q_k = q^k$	x^k
shift	$q \diamond t_n = t_{n+1}$	$x \cdot x^n = x^{n+1}$
signal	$\sum s_n t_n$	$\sum s_n x^n$
filter	$\sum h_k q^k$	$\sum h_k x^k$

filters. Convergence of the filter operation is handled as part of the next step.

Realization. To obtain the signal model, we first consider the “realization” of the abstract model. We replace the abstract objects t_n and q and the operation \diamond by objects we can compute with. To this end, we choose a variable x and set $q = x$, and $\diamond = \cdot$, the ordinary multiplication of series. Then, (32) becomes

$$t_{n+1} = x \cdot t_n. \quad (33)$$

This two-term recurrence, when started with $t_0 = 1$, has the unique solution

$$t_n = x^n. \quad (34)$$

In other words, the realization is essentially (up to a common scaling factor for all x^n) unique.

As a result, we obtain $\mathcal{M} = \{s = \sum s_n x^n\}$ and $\mathcal{A} = \{h = \sum h_k x^k\}$. Since the series are infinite, we have to ensure convergence as part of the realization; namely, that filtering, the operation of \mathcal{A} on \mathcal{M} , is well-defined. This is achieved, for example, by requiring $\mathbf{s} \in \ell^2(\mathbb{Z})$ and $\mathbf{h} \in \ell^1(\mathbb{Z})$, as explained in Section III-A.

Table II shows the correspondence between the abstract and the realized concepts. Note that signals and filters are conceptually different (as pointed out several times before) but *look the same (both are Laurent series in x) because the realization maps both q^n and t_n to x^n .*

Resulting signal model. As a result of the above procedure, we obtain the infinite discrete time model in (6).

B. Constructing the Finite Time Model

In real applications, usually only a finite subsequence $\mathbf{s} = (s_0, \dots, s_{n-1})$ is available, not the entire (sampled) sequence $(s_k)_{k \in \mathbb{Z}}$. Thus, for time SP, the question arises how to construct a *finite* time model $(\mathcal{A}, \mathcal{M}, \Phi)$. Here ASP and in particular polynomial algebras provide a very detailed insight into the possible choices.

For our investigation we first need a formal notion of *signal extension*.

Definition 4 (Signal Extension) Let $\mathbf{s} = (s_k)_{k \in I}$ be a signal given on an index set $I \subset \mathbb{Z}$. A (linear) signal extension of \mathbf{s} is the sequence of linear combinations (only finitely many summands are nonzero)

$$s_k = \sum_{i \in I} \beta_{k,i} s_i, \quad \text{for } k \notin I.$$

The signal extension is called *monomial*, if, for each k , the sum has only one summand.

In other words, in a monomial signal extension, every signal value outside the signal scope I is assumed to be a multiple of a signal value inside the signal scope. For example, the periodic signal extension is monomial.

Note that we consider only *linear* signal extensions (e.g., polynomial signal extensions are excluded). The reason is that with nonlinear signal extensions it is not possible to maintain filtering as a linear operation. Thus, we are outside linear SP, and hence outside ASP as developed here.

Shift, linear extension, realization. To construct a finite time signal model, we follow the exact same steps as in Section V-A, but start from a *finite* set of time marks t_0, \dots, t_{n-1} .

The construction seems to lead to the following definition of a “finite” z -transform, which maps $\mathbf{s} \in \mathbb{C}^n$ to

$$s = s(x) = \sum_{0 \leq k < n} s_k x^k,$$

Clearly, the set $\mathbb{C}_n[x]$ of the polynomials $s(x)$ of degree less than n is a vector space with the natural basis $b = (x^0, \dots, x^{n-1})$. The problem, however, arises from the operation of the (realized) time shift x : the set of polynomials of degree less than n is *not closed* under multiplication by x . More precisely, the root of the problem is

$$x \cdot x^{n-1} = x^n \notin \mathbb{C}_n[x], \quad (35)$$

and, if x is invertible,

$$x^{-1} \cdot x^0 = x^{-1} \notin \mathbb{C}_n[x]. \quad (36)$$

Thus, the time shift as defined is not a valid operation on $\mathbb{C}_n[x]$, which implies that we cannot define filtering in $\mathbb{C}_n[x]$, or, algebraically, $\mathbb{C}_n[x]$ is not a module. Without filtering, there is also no notion of spectrum or Fourier transform. To resolve this, we need to take care of the problems raised by (35) and (36), which we do now by introducing boundary conditions.

Boundary conditions and signal extension. To remedy the first problem (35), we have to make sure that x^n can again be expressed as a polynomial of degree $n-1$. This is achieved by introducing an equation

$$x^n = r(x) = \sum_{0 \leq k < n} \beta_k x^k, \quad \text{or} \quad x^n - r(x) = 0. \quad (37)$$

This equation implicitly defines the right boundary condition $s_n = \sum_{0 \leq k < n} \beta_k s_k$. Further, (37) determines the entire right signal extension obtained by reducing x^{n+k} , $k \geq 0$, modulo $x^n - r(x)$:

$$x^{n+k} \equiv r_k(x) \pmod{(x^n - r(x))}. \quad (38)$$

Algebraically, the boundary condition replaces the vector space $\mathbb{C}_n[x]$ by the vector space $\mathcal{M} = \mathbb{C}[x]/(x^n - r(x))$, which is of the same dimension, but *closed* under multiplication by the time shift operator x and thus a module. The corresponding algebra \mathcal{A} , generated by x , is identical to \mathcal{M} . The remaining question to consider is (36). There are two cases.

Case 1: $x \mid r(x)$. Then also $x \mid (x^n - r(x))$, and thus x (the shift operator) is not invertible¹¹ in $\mathcal{A} = \mathbb{C}[x]/(x^n - r(x))$ and (36) does not need to be considered: the signal has no left boundary, since “the past” is not accessible without an invertible x .

Case 2: $x \nmid r(x)$. Then, from (37), we get

$$x^{-1} = -\frac{1}{\beta_0}(\beta_1 + \beta_2 x + \dots + \beta_{n-1} x^{n-2} - x^{n-1}),$$

which is the left boundary condition. Similar to above, the left signal extension can be determined by multiplying by x^{-k} and reducing modulo $x^n - r(x)$. Thus, the signal extension in *both* directions is determined by *one* equation (37), which provides the left and the right boundary condition:

boundary condition \Rightarrow right and left signal extension.

By assuming the generic boundary condition $x^n = r(x)$, we obtain a valid signal model. However, the corresponding signal extension (38) has in general no simple structure. To obtain a module that is reasonable for applications, we thus require

- the shift operator $x \in \mathcal{A}$ to be invertible; and
- the signal extension to be monomial (see Definition 4).

These requirements lead to the signal model for the DFT in the *finite time* case (explained below) and for the 16 DCTs and DSTs in the *finite space* case [1].

We can now explicitly determine the polynomials $x^n - r(x)$ that satisfy the above two conditions.

Lemma 5 The boundary condition $x^n = r(x)$ makes $\mathcal{A} = \mathbb{C}[x]/(x^n - r(x))$ an algebra in which x is invertible and determines a monomial signal extension in $\mathcal{M} = \mathcal{A}$, if and only if the polynomial $r(x)$ is a nonzero constant, i.e., $r(x) = a \neq 0$. The signal extension in this case is given by $s_k = a^{k_2} s_{k_1}$, where $k \in \mathbb{Z}$ is expressed as $k = k_1 + k_2 n$, with $0 \leq k_1 < n$.

Proof: Let $r(x) = a$, $a \neq 0$, and let $k \in \mathbb{Z}$. We write $k = k_1 + k_2 n$, with $0 \leq k_1 < n$, and thus $x^k \equiv a^{k_2} x^{k_1} \pmod{(x^n - a)}$, which is a monomial signal extension. Conversely, let $x^n = r(x)$ determine a monomial signal extension. This implies $x^n = a x^\ell$, for some $0 \leq \ell < n$. Since x is by assumption invertible modulo $x^n - a x^\ell$, it follows $\ell = 0$ and $a \neq 0$ as desired. ■

Resulting signal model. In summary, the signal model obtained is for $V = \mathbb{C}^n$ and given by

$$\mathcal{A} = \mathcal{M} = \mathbb{C}[x]/(x^n - a), \quad \Phi: \mathbf{s} \mapsto \sum_{0 \leq k < n} s_k x^k \in \mathcal{M}. \quad (39)$$

For $a = 1$, this is exactly the finite model in (19), which we studied in Section IV.

For other values of a , it is an easy exercise to specialize the general results from Section IV. In short, the visualization is as in Fig. 3 with the backwards edge weighted with a , the filter

¹¹A polynomial $q(x)$ is invertible in $\mathbb{C}[x]/p(x)$ if and only if $\gcd(q(x), p(x)) = 1$, since in this case there are polynomials $r(x), s(x)$ such that $1 = s(x)q(x) + r(x)p(x)$, which implies that $s(x) \equiv q(x)^{-1} \pmod{p(x)}$.

matrices are skew-circulant matrices, filtering is hence skew-circular convolution, and the polynomial Fourier transform has the form $\text{DFT}_n \cdot D$, with a suitable diagonal matrix D [9].

In particular, this class includes the generalized DFTs from [38], [39] defined as

$$\mathcal{F}_{c,d} = [\omega_n^{(k+c)(\ell+d)}]_{0 \leq k, \ell < n},$$

where $c, d \in \mathbb{R}$. We briefly investigate the 4 special cases given by $c, d \in \{0, 1/2\}$, which in [39] are called DFTs of types 1–4, written as DFT-1, \dots , DFT-4. Namely,

$$\text{DFT-1}_n = \mathcal{F}_{0,0} = \text{DFT}_n, \quad (40)$$

$$\text{DFT-2}_n = \mathcal{F}_{0,1/2} = \text{diag}_{0 \leq k < n}(\omega_n^{k/2}) \text{DFT}_n, \quad (41)$$

$$\text{DFT-3}_n = \mathcal{F}_{1/2,0}, \quad (42)$$

$$\text{DFT-4}_n = \mathcal{F}_{1/2,1/2} = \text{diag}_{0 \leq k < n}(\omega_n^{k/2}) \text{DFT-3}_n. \quad (43)$$

We identify the signal models for which these transforms are Fourier transforms. The DFT-1 $_n = \text{DFT}_n$ is, as seen above, a polynomial transform for $\mathbb{C}[x]/(x^n - 1)$. The DFT-2 $_n$ in (41) is also a Fourier transform, but not the polynomial transform, for $\mathbb{C}[x]/(x^n - 1)$. The DFT-3 $_n$ in (42) is the polynomial transform for $\mathbb{C}[x]/(x^n + 1)$, since $\omega_n^{k+1/2}$, $0 \leq k < n$, are precisely the zeros of $x^n + 1$. Finally, the DFT-4 $_n$ in (43) is also a Fourier transform, but not the polynomial transform, for $\mathbb{C}[x]/(x^n + 1)$. This means that these DFTs cover the two important cases of boundary conditions $s_n = \pm s_0$ or $p(x) = x^n \mp 1$.

Other boundary conditions and effect on spectrum. At this point it is instructive to investigate what problems arise if we slightly relax the conditions in Lemma 5 by dropping the requirement of monomial signal extension or the requirement that the shift operator x is invertible in the resulting algebra.

If we allow *any* signal extension and hence $p(x)$, we obtain the *generic* finite time model

$$\mathcal{A} = \mathcal{M} = \mathbb{C}[x]/p(x), \quad \Phi : \mathbf{s} \mapsto \sum_{0 \leq k < n} s_k x^k.$$

If $p(x)$ has pairwise distinct zeros, then the polynomial transform is precisely a Vandermonde matrix and the shift matrix $\phi(x)$ is the transpose of the companion matrix of p .

If we require a monomial signal extension, but allow for a non-invertible shift, then the proof of Lemma 5 shows that necessarily $p(x) = x^n - ax^\ell$. A simple choice is $a = 0$ yielding $\mathcal{A} = \mathcal{M} = \mathbb{C}[x]/x^n$, which realizes a right zero extension ($x^n = 0$ implies $x^{n+k} = 0$ for $k \geq 0$). The problem with this model is that it does not permit spectral analysis: $\mathbb{C}[x]/x^n$ cannot be decomposed by the Chinese Remainder Theorem (CRT). This can also be seen from the shift matrix $\phi(x)$, which is the lower Jordan block (and hence cannot be block-diagonalized)

$$\phi(x) = \begin{bmatrix} 0 & & & & \\ 1 & 0 & & & \\ & \ddots & \ddots & & \\ & & & 1 & 0 \end{bmatrix}.$$

Another simple choice is the symmetric boundary condition $x^n = x^{n-1}$, i.e., $p(x) = x^n - x^{n-1}$. This choice implies

a constant right signal extension, since $x^n = x^{n-1}$ implies $x^{n+k} = x^{n-1}$ for all $k \geq 0$. In this case, the CRT yields

$$\mathbb{C}[x]/(x^n - x^{n-1}) \cong \mathbb{C}[x]/(x - 1) \oplus \mathbb{C}[x]/x^{n-1},$$

and the rightmost module, of dimension $n - 1$, is again indecomposable. In contrast, in [1] we will see that finite space models (which have DCTs/DST as Fourier transforms) do permit symmetric boundary conditions.

If we relax the requirement of a monomial signal extension and only require that the Fourier transform approaches the DTFT as $n \rightarrow \infty$, then choices nontrivially different from the DFT are indeed possible [40].

C. Real Finite Time Model

ASP naturally extends to base fields other than \mathbb{C} and gives insight into the necessary changes in the SP concepts associated with a signal model. As an example, we consider *real* finite time models in this section. In particular, we will explain why the real DFTs (RDFTs) or discrete Hartley transforms (DHTs) are now the associated Fourier transforms.

The algebraic interpretation of the DHT in this section is equivalent to recognizing the DHT as a special case of an ADFT (algebraic discrete Fourier transform), a general concept introduced in [41], [42] and rediscovered (using a different name) in [43].

Real finite time model. If only real signals and filters are to be considered and all the computations are in \mathbb{R} then we simply replace \mathbb{C} by \mathbb{R} in a given signal model. For example, the real equivalent of (19) for $V = \mathbb{R}^n$ is given by

$$\mathcal{M} = \mathcal{A} = \mathbb{R}[x]/(x^n - 1), \quad \Phi : \mathbf{s} \mapsto \sum_{0 \leq k < n} s_k x^k \in \mathcal{M}. \quad (44)$$

Compared to its complex counterpart in (19), (44) has the same notions of filtering (only restricted to \mathbb{R}), visualization, and signal extension.

Spectrum and Fourier transform. The difference arises when computing the spectrum. Since only real numbers are available, and the roots of $x^n - 1$ are complex, \mathcal{M} cannot be decomposed into one-dimensional irreducible modules.¹² Over \mathbb{R} , the irreducible factors of $x^n - 1$ are polynomials of degree 1 or 2. Namely, if $\omega_n^k, \omega_n^{n-k}$, $k \neq 0, n/2$, are conjugated complex roots of $x^n - 1$, then

$$(x - \omega_n^k)(x - \omega_n^{n-k}) = x^2 - 2c_{k,n}x + 1,$$

with $c_{k,n} = \cos(2k\pi/n)$ is irreducible over \mathbb{R} .

Hence the spectral decomposition is now given by

$$\Delta : \mathbb{R}[x]/(x^n - 1) \rightarrow \mathbb{R}[x]/(x - 1) \oplus \bigoplus_{1 \leq k < n/2} \mathbb{R}[x]/(x^2 - 2c_{k,n}x + 1) \oplus \mathbb{R}[x]/(x + 1), \quad (45)$$

where the last summand appears only for even n ($-1 = \omega_n^{n/2}$).

We want to compute the matrix form \mathcal{F} of (45). The situation is slightly outside the scope of Section IV; in particular there is no notion of polynomial transform. Still, the theory

¹²In algebraic terms, \mathbb{R} is not a *splitting field* for the \mathcal{A} -module \mathcal{M} .

is readily extended. To compute \mathcal{F} , we choose a basis in each spectral component. It turns out that the natural choice is $(1, \frac{1}{s_{k,n}}(x - c_{k,n}))$, $s_{k,n} = \sin(2k\pi/n)$. Namely, this choice associates the matrix $\begin{bmatrix} 1 & j \\ 1 & -j \end{bmatrix}$ with the decomposition

$$\mathbb{C}[x]/(x^2 - 2c_{k,n} + 1) \rightarrow \mathbb{C}[x]/(x - \omega_n^k) \oplus \mathbb{C}[x]/(x - \omega_n^{n-k})$$

and hence shows that the coordinates of the real spectrum are the real and imaginary parts of the complex spectrum. Further, the irreducible representation (i.e., frequency response) ϕ_k afforded by a two-dimensional spectral component in (45) maps the shift to a rotation:

$$\phi_k : \mathcal{A} \rightarrow \mathbb{R}^{2 \times 2}, \quad x \mapsto \begin{bmatrix} c_{k,n} & -s_{k,n} \\ s_{k,n} & c_{k,n} \end{bmatrix},$$

and hence, as a homomorphism, $\phi_k(h(x)) = h(\phi_k(x))$. The matrix \mathcal{F} is now computed by reducing x^ℓ modulo $x - 1$, $x^2 - 2c_{k,n} + 1$, and $x + 1$. Further, to precisely match the common definition of the real DFT, we order the spectral basis such that first come all the 1's (bases of the one-dimensional components) and then the remaining. The result is

$$\mathcal{F} = \text{RDFT}_n = [r_{k\ell}]_{0 \leq k, \ell < n}$$

with

$$r_{k\ell} = \begin{cases} \cos \frac{2\pi k\ell}{n}, & 0 \leq k \leq n/2, \\ -\sin \frac{2\pi k\ell}{n}, & n/2 < k < n. \end{cases}$$

From the above it follows that

$$\text{DFT}_n = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & & & j \\ \vdots & & \ddots & \ddots & \\ \vdots & & \ddots & \ddots & \\ 0 & 1 & & & -j \end{bmatrix} \cdot \text{RDFT}_n. \quad (46)$$

Since the only degree of freedom is in choosing a spectral basis in (45), a generic real DFT has the form

$$\mathcal{F} = X_n \cdot \text{RDFT}_n,$$

where X_n is any invertible matrix with the same x-shaped pattern as the matrix in (46). An example is

$$\begin{aligned} \text{DHT}_n &= [\cos \frac{2k\ell\pi}{n} + \sin \frac{2k\ell\pi}{n}]_{0 \leq k, \ell, n} \\ &= [\text{cas} \frac{2k\ell\pi}{n}]_{0 \leq k, \ell, n}, \end{aligned}$$

where $\text{cas}(x) = \cos(x) + \sin(x)$. Obviously,

$$\text{DHT}_n = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & & & 1 \\ \vdots & & \ddots & \ddots & \\ \vdots & & \ddots & \ddots & \\ 0 & 1 & & & -1 \end{bmatrix} \cdot \text{RDFT}_n. \quad (47)$$

Both transforms, the RDFT and the DHT, are special among the class of all possible real DFTs. The RDFT appears to have the lowest arithmetic complexity¹³ and the DHT is equal to its inverse (up to a scaling factor).

¹³We do not have a proof. The assertion is based on the best known algorithms.

The above derivation extends to the DFTs of type 1–4 in (40)–(43) and allows us to define DHTs and RDFTs of type 1–4 in parallel to (40)–(43). Namely, the types $t = 1, 2, 3, 4$ correspond, respectively, to the parameters $(c, d) = (0, 0), (0, 1/2), (1/2, 0), (1/2, 1/2)$ in the following definitions.

$$\text{RDFT-t} = [r_{k,\ell}]_{0 \leq k, \ell < n}$$

with

$$r_{k\ell} = \begin{cases} \cos \frac{2\pi(k+c)(\ell+d)}{n}, & 0 \leq k \leq m, \\ -\sin \frac{2\pi(k+c)(\ell+d)}{n}, & m < k < n, \end{cases}$$

where $m = n/2$ for $t = 1, 2$ and $m = (n-1)/2$ for $t = 3, 4$.

$$\text{DHT-t}_n = [\text{cas} \frac{2(k+d)(\ell+c)\pi}{n}]_{0 \leq k, \ell, n}.$$

The relations (46) and (47) hold for all four types.

The four transforms DHT-t were introduced (in their orthogonal form) in [44], [45], [46], [47], where they were called discrete W transforms (DWTs) of type 1–4. We suggest to rename these transforms to DHTs of type 1–4 since: 1) the name DHT (for type 1) is much more commonly used than DWT, and the types 2–4 are just variants; and 2) even though the DHT and the DWT were introduced at about the same time ([48] and [47]), the continuous counterpart was introduced by Hartley much earlier in 1942 [49].

Diagonalization properties. The above discussion gives immediately the “diagonalization” properties of the RDFT and DHT. We use double quotes, since these properties are not actually a diagonalization. If $h \in \mathcal{A} = \mathbb{R}[x]/(x^n - 1)$ is any filter, then $\phi(h)$ is a real circulant matrix, i.e., of the form (21) with $a = 1$. Then

$$\text{RDFT}_n \phi(h) \text{RDFT}_n^{-1} = X, \quad (48)$$

where X is real and has the same x-shaped structure as the matrix in (46). Convolution theorems can be similarly derived.

Finally, we note that other basefields than \mathbb{C} and \mathbb{R} can be considered. For example, the rational finite time model can be studied by decomposing $x^n - 1$ over \mathbb{Q} . Interestingly, this yields the rationalized Haar transform as one possible Fourier transform choice. See [9] for further details.

D. Overview of Finite Time Models

In Table III we list the finite time models that we introduced in this paper, and their associated Fourier transforms. The table is divided into complex and real time models. In each row we list in the first two columns the signal model $(\mathcal{A}, \mathcal{M}, \Phi)$, in the third column the associated unique polynomial Fourier transform, and in the fourth column other possible relevant Fourier transforms for the model. Note that the notion of polynomial transform does not exist for the real time models since the spectral components are not all one-dimensional.

VI. CONCLUSIONS

We presented the algebraic signal processing theory (ASP), a new approach to linear signal processing.

ASP is an axiomatic theory of SP. It is developed from the concept of the signal model, the triple $(\mathcal{A}, \mathcal{M}, \Phi)$. We

TABLE III

OVERVIEW OF FINITE TIME MODELS AND ASSOCIATED FOURIER TRANSFORMS DISCUSSED IN THIS PAPER.

Complex finite z-transform			
$\mathcal{A} = \mathcal{M}$	Φ	$\mathcal{F} = \mathcal{P}_{b,\alpha}$	other \mathcal{F}
$\mathbb{C}[x]/(x^n - a)$	$\mathbf{s} \mapsto \sum s_k x^k$	DFT $_n \cdot D$	—
$\mathbb{C}[x]/(x^n - 1)$	$\mathbf{s} \mapsto \sum s_k x^k$	DFT $_n = \text{DFT-}1_n$	DFT- 2_n
$\mathbb{C}[x]/(x^n + 1)$	$\mathbf{s} \mapsto \sum s_k x^k$	DFT- 3_n	DFT- 4_n
Real finite z-transform			
$\mathcal{A} = \mathcal{M}$	Φ	\mathcal{F}	
$\mathbb{R}[x]/(x^n - 1)$	$\mathbf{s} \mapsto \sum s_k x^k$	RDFT- $1/2_n$, DHT- $1/2_n$	
$\mathbb{R}[x]/(x^n + 1)$	$\mathbf{s} \mapsto \sum s_k x^k$	RDFT- $3/4_n$, DHT- $3/4_n$	

showed that basic concepts such as filtering, spectrum, Fourier transform, shift, and shift-invariance can be defined (if they exist) for any signal model, just like basis, dimension, and linear mapping can be defined for any vector space.

ASP is a very general platform for SP. In this paper, we focused on capturing time SP in ASP; reference [1] presents ASP for space dependent signals.

ASP gives deep insight into the structure and choices in SP. For example, for finite time SP, we derived the periodic boundary condition from basic principles but also showed that other choices are possible. We also considered DFT variants and showed that they are Fourier transforms in ASP for a properly chosen signal model. This understanding is crucial when we leave the familiar domain of time SP.

ASP is constructive. For example, we showed how to derive the time signal models from the shift operation. This enables the derivation of novel signal models for other, non-standard shifts. Further, in [5], [7] we use ASP to present concise derivations of existing and new fast algorithms for linear transforms.

Besides the derivation of other SP frameworks, or signal models, a future research direction is to capture “advanced” SP concepts abstractly within ASP including sampling, down-sampling, filter banks, multiresolution analysis, frames, and others.

REFERENCES

[1] M. Püschel and J. M. F. Moura, “Algebraic signal processing theory: 1-D space,” *IEEE Trans. on Signal Processing*, to appear.

[2] M. Püschel and M. Rötteler, “Fourier transform for the spatial quincunx lattice,” in *Proc. International Conference on Image Processing (ICIP)*, 2005, vol. 2, pp. 494–497.

[3] M. Püschel and M. Rötteler, “Algebraic signal processing theory: 2-D hexagonal spatial lattice,” *IEEE Trans. on Image Processing*, vol. 16, no. 6, pp. 1506–1521, 2007.

[4] M. Püschel and J. M. F. Moura, “The algebraic approach to the discrete cosine and sine transforms and their fast algorithms,” *SIAM Journal of Computing*, vol. 32, no. 5, pp. 1280–1316, 2003.

[5] M. Püschel and J. M. F. Moura, “Algebraic signal processing theory: Cooley-Tukey type algorithms for DCTs and DSTs,” *IEEE Trans. on Signal Processing*, vol. 56, no. 4, pp. 1502–1521, 2008.

[6] Y. Voronenko and M. Püschel, “Algebraic derivation of general radix Cooley-Tukey algorithms for the real discrete Fourier transform,” in *Proc. International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, 2006, vol. 3, pp. 876–879.

[7] Y. Voronenko and M. Püschel, “Algebraic signal processing theory: Cooley-Tukey type algorithms for real DFTs,” *IEEE Trans. on Signal Processing*, to appear.

[8] M. Püschel and M. Rötteler, “Algebraic signal processing theory: Cooley-Tukey type algorithms on the 2-D spatial hexagonal lattice,” *Applicable Algebra in Engineering, Communication and Computing, special issue “in memoriam Thomas Beth”*, 2008, to appear.

[9] M. Püschel and J. M. F. Moura, “Algebraic signal processing theory,” [Online]. Available: <http://arxiv.org/abs/cs.IT/0612077>.

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

[11] M. T. Heideman, D. H. Johnson, and C. S. Burrus, “Gauss and the history of the fast Fourier transform,” *Archive for History of Exact Sciences*, vol. 34, pp. 265–277, 1985.

[12] P. J. Nicholson, “Algebraic theory of finite Fourier transforms,” *Journal of Computer and System Sciences*, vol. 5, pp. 524–547, 1971.

[13] L. Auslander, E. Feig, and S. Winograd, “Abelian semi-simple algebras and algorithms for the discrete Fourier transform,” *Advances in Applied Mathematics*, vol. 5, pp. 31–55, 1984.

[14] S. Winograd, “On computing the discrete Fourier transform,” *Mathematics of Computation*, vol. 32, pp. 175–199, 1978.

[15] S. Winograd, “On the multiplicative complexity of the discrete Fourier transform,” *Advances in Mathematics*, vol. 32, pp. 83–117, 1979.

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

[17] W. Rudin, *Fourier Analysis on Groups*, Number 12 in Interscience tracts in pure and applied mathematics. Interscience, New York, 1962.

[18] G. G. Apple and P. A. Wintz, “Calculation of Fourier transforms on finite Abelian groups,” *IEEE Trans. on Information Theory*, vol. IT-16, pp. 233–234, 1970.

[19] M. G. Karpovsky, “Fast Fourier transforms on finite non-Abelian groups,” *IEEE Trans. on Computers*, vol. C-26, pp. 1028–1030, 1977.

[20] P. Diaconis, “A generalization of spectral analysis with applications to ranked data,” *Annals of Statistics*, vol. 17, pp. 949–979, 1989.

[21] J. R. Driscoll and D. M. Healy Jr., “Computing Fourier transforms and convolutions on the 2-sphere,” *Advances in Applied Mathematics*, vol. 15, pp. 203–250, 1994.

[22] R. Foote, G. Mirchandi, D. Rockmore, D. Healy, and T. Olson, “A wreath product approach to signal and image processing: Part I—multiresolution analysis,” *IEEE Trans. on Signal Processing*, vol. 48, no. 1, pp. 102–132, 2000.

[23] R. E. Kalman, P. L. Falb, and M. A. Arbib, *Topics in Mathematical System Theory*, McGraw-Hill, 1969.

[24] J. C. Willems and S. K. Mitter, “Controllability, observability, pole allocation, and state reconstruction,” *IEEE Transactions on Automatic Control*, vol. 16, pp. 582–595, 1971.

[25] Adrian E. Eckberg, *Algebraic System Theory with Applications to Decentralized Control*, Ph.D. thesis, Massachusetts Institute of Technology, Cambridge, MA, 1973.

[26] Paul A. Fuhrman, “Algebraic system theory: An analyst’s point of view,” *Journal of the Franklin Institute*, vol. 301, pp. 521–540, 1976.

[27] E. R. Berlekamp, *Algebraic Coding Theory*, Aegean Park Press, 1984.

[28] N. Jacobson, *Basic Algebra I*, W. H. Freeman and Co., 1974.

[29] G. James and M. Liebeck, *Representations and Characters of Groups*, Cambridge Univ. Pr., 1993.

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

[31] Irwin W. Sandberg, “A representation theorem for linear systems,” *IEEE Trans. on Circuits and Systems—1: Fundamental Theory and Applications*, vol. 45, no. 5, pp. 578–580, 1998.

[32] D. Rockmore, “Some applications of generalized FFT’s,” in *Proceedings of DIMACS Workshop in Groups and Computation*, 1995, vol. 28, pp. 329–370.

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

[34] 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*, vol. 26, pp. 1066–1099, 1997.

[35] D. Potts, G. Steidl, and M. Tasche, “Fast algorithms for discrete polynomial transforms,” *Mathematics of Computation*, vol. 67, no. 224, pp. 1577–1590, 1998.

[36] Henri J. Nussbaumer and Philippe Quandalle, “Fast computation of discrete Fourier transforms using polynomial transforms,” *IEEE Trans. on Acoustics, Speech, and Signal Processing*, vol. ASSP-27, no. 2, pp. 169–181, 1979.

- [37] Th. Kailath and V. Olshevsky, "Displacement structure approach to polynomial Vandermonde and related matrices," *Linear Algebra and Applications*, vol. 261, pp. 49–90, 1997.
- [38] G. Bongiovanni, P. Corsini, and G. Frosini, "One-dimensional and two-dimensional generalized discrete Fourier transform," *IEEE Trans. on Acoustics, Speech, and Signal Processing*, vol. ASSP-24, no. 2, pp. 97–99, 1976.
- [39] V. Britanak and K. R. Rao, "The fast generalized discrete Fourier transforms: A unified approach to the discrete sinusoidal transforms computation," *Signal Processing*, vol. 79, pp. 135–150, 1999.
- [40] D. Balcan, A. Sandryhaila, J. Gross, and M. Püschel, "Alternatives to the discrete Fourier transform," in *Proc. International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, 2008.
- [41] Th. Beth, *Verfahren der Schnellen Fouriertransformation [Methods for the Fast Fourier Transform]*, Teubner, 1984.
- [42] Th. Beth, W. Fumy, and W. Mühlfeld, "Zur algebraischen diskreten Fourier-Transformation [on the algebraic discrete Fourier transform]," *Archiv der Mathematik*, vol. 6, no. 3, pp. 238–244, 1983.
- [43] J. Hong, M. Vetterli, and P. Duhamel, "Basefield transforms with the convolution property," *Proceedings of the IEEE*, vol. 82, no. 3, pp. 400–412, 1994.
- [44] Z. Wang, "Harmonic analysis with a real frequency function. I. aperiodic case," *Appl. Math. Comput.*, vol. 9, pp. 53–73, 1981.
- [45] Z. Wang, "Harmonic analysis with a real frequency function. II. periodic and bounded cases," *Appl. Math. Comput.*, vol. 9, pp. 153–163, 1981.
- [46] Z. Wang, "Harmonic analysis with a real frequency function. III. data sequence," *Appl. Math. Comput.*, vol. 9, pp. 245–255, 1981.
- [47] Z. Wang and B. R. Hunt, "The discrete W transform," *Applied Mathematics and Computation*, vol. 16, pp. 19–48, 1985.
- [48] R. N. Bracewell, "Discrete Hartley transform," *J. Optical Society America*, vol. 73, no. 12, pp. 1832–1835, 1983.
- [49] R. V. L. Hartley, "A more symmetrical Fourier analysis applied to transmission problems," *Proc. IRE*, vol. 30, pp. 144–150, 1942.

APPENDIX I ALGEBRAIC BACKGROUND

We provide here formal definitions for the most important algebraic concepts used in this paper. For an introduction to algebra we refer to [28].

Definition 6 (Algebra) A \mathbb{C} -algebra \mathcal{A} is a \mathbb{C} -vector space that is also a ring (multiplication is defined and the distributive law holds), such that the addition in the ring and the addition in the vector space coincide. Further, for $\alpha \in \mathbb{C}$ and $g, h \in \mathcal{A}$: $\alpha(gh) = (\alpha g)h = g(\alpha h)$.

Definition 7 (Module) Let \mathcal{A} be a \mathbb{C} -algebra. A (left) \mathcal{A} -module is a \mathbb{C} -vector space \mathcal{M} with operation

$$\mathcal{A} \times \mathcal{M} \rightarrow \mathcal{M}, \quad (a, m) \mapsto am,$$

which satisfies, for $a, b, 1 \in \mathcal{A}$ and $m, n \in \mathcal{M}$,

$$\begin{aligned} a(m+n) &= am + an & (ab)m &= a(bm) \\ (a+b)m &= am + bm & 1m &= m \end{aligned}$$

Definition 8 (Homomorphism of algebras) Let \mathcal{A}, \mathcal{B} be \mathbb{C} -algebras. A homomorphism of algebras is a mapping $\phi : \mathcal{A} \rightarrow \mathcal{B}$ that satisfies, for $a, b \in \mathcal{A}$, $\alpha \in \mathbb{C}$:

$$\phi(a+b) = \phi(a) + \phi(b), \quad \phi(ab) = \phi(a)\phi(b), \quad \phi(\alpha a) = \alpha\phi(a).$$

An isomorphism is a bijective homomorphism.

Definition 9 (Homomorphism of modules) Let \mathcal{M}, \mathcal{N} be \mathcal{A} -modules. An \mathcal{A} -module homomorphism is a mapping $\phi : \mathcal{M} \rightarrow \mathcal{N}$ that satisfies, for $a \in \mathcal{A}$, $m, n \in \mathcal{M}$,

$$\phi(m+n) = \phi(m) + \phi(n) \quad \text{and} \quad \phi(am) = a\phi(m).$$

We denote with $\mathbb{Z}/n\mathbb{Z}$ the ring of integers $\{0, \dots, n-1\}$ with addition and multiplication modulo n . The Chinese remainder theorem (CRT) for integers states that if $n = pq$ and $\gcd(p, q) = 1$, then

$$\phi : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}, \quad k \mapsto (k \bmod p, k \bmod q).$$

is a ring isomorphism. In words, the CRT states that "computing (addition and multiplication) modulo n is equivalent to computing in parallel modulo p and modulo q ."

The CRT also holds for polynomials. In this case, $\mathbb{C}[x]/p(x)\mathbb{C}[x] = \mathbb{C}[x]/p(x)$ is the ring (even algebra) of polynomials of degree less than $n = \deg(p)$ with addition and multiplication modulo $p(x)$. These *polynomial algebras* are discussed in detail in Section IV.

Theorem 10 (CRT for polynomials) Let $p(x) \in \mathbb{C}[x]$ be a polynomial that factorizes as $p(x) = r(x)s(x)$ with $\gcd(r(x), s(x)) = 1$. Then

$$\begin{aligned} \phi : \mathbb{C}[x]/p(x) &\rightarrow \mathbb{C}[x]/r(x) \oplus \mathbb{C}[x]/s(x), \\ s(x) &\mapsto (q(x) \bmod r(x), q(x) \bmod s(x)) \end{aligned}$$

is an isomorphism of algebras. Note that we write \oplus instead of \times in this case, since the rings also carry the vector space structure.



Markus Püschel (M'99–SM'05) is an Associate Research Professor of Electrical and Computer Engineering at Carnegie Mellon University (CMU). He received his Diploma (M.Sc.) in Mathematics and his Doctorate (Ph.D.) in Computer Science, in 1995 and 1998, respectively, both from the University of Karlsruhe, Germany. From 1998–1999 he was a Postdoctoral Researcher at Mathematics and Computer Science, Drexel University, Philadelphia. Since 2000 he has been with CMU. He is an Associate Editor for the *IEEE Transactions on Signal Processing*, and was an Associate Editor for the *IEEE Signal Processing Letters*, a Guest Editor of the *Journal of Symbolic Computation*, and the *Proceedings of the IEEE*. He holds the title of Privatdozent of Applied Informatics at the Department of Computer Science, University of Technology, Vienna, Austria and was awarded (with J. Moura) the CMU College of Engineering Outstanding Research Award. His research interests include signal processing theory/software/hardware, scientific computing, compilers, applied mathematics and algebra.



José M. F. Moura (S'71–M'75–SM'90–F'94) received the engenheiro electrotécnico degree in 1969 from Instituto Superior Técnico (IST), Lisbon, Portugal, and the M.Sc., E.E., and D.Sc. degrees in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology (M.I.T.), Cambridge, in 1973 and 1975, respectively.

He is a Professor of Electrical and Computer Engineering and, by courtesy, of Biomedical Engineering at Carnegie Mellon University (CMU) where he is a founding co-director of the Center for Sensed Critical Infrastructures Research (CenSCIR). He was on the faculty at IST (1975-84) and has held visiting faculty appointments at MIT (1984-86, 1999-00, 2006-07) and as a research scholar at USC (summers of 1978-81). In 2006, he founded the Information and Communications Technologies Institute, a joint venture between CMU and Portugal, that he co-Directs, and that manages the CMU-Portugal education and research program, www.icti.cmu.edu.

His research interests include statistical and algebraic signal processing, image, bioimaging, and video processing, and digital communications. He has published over 300 technical Journal and Conference papers, is the co-editor of two books, holds six patents on image and video processing, and digital communications with the US Patent Office, and has given numerous invited seminars at US and European Universities and industrial and government Laboratories.

Dr. Moura is the *President Elect* (2006-07) for the *IEEE Signal Processing Society* (SPS), which he has served as *Vice-President for Publications* (2000-02), *Editor in Chief* for the *IEEE Transactions in Signal Processing* (1975-99), interim *Editor in Chief* for the *IEEE Signal Processing Letters* (December 2001-May 02), founding member of the *Bioimaging and Signal Processing* (BISP) Technical Committee, and member of several other Technical Committees. He was *Vice-President for Publications* for the *IEEE Sensors Council* (2000-02) and is or was on the *Editorial Board* of several Journals, including the *IEEE Proceedings*, the *IEEE Signal Processing Magazine*, and the *ACM Transactions on Sensor Networks*. He chaired the *IEEE TAB Transactions Committee* (2002-03) that joins the more than 80 Editors in Chief of the *IEEE Transactions* and served on the *IEEE TAB Periodicals Review Committee* (2002-06). He is on the *International Conference on Information Processing and Sensor Networks* (IPSN) and was on the *International Symposium on Bioimaging* (ISBI) Steering Committees and has been on the program committee of over 35 Conferences and Workshops. He was on the *IEEE Press Board* (1991-95).

Dr. Moura is a *Fellow* of the *IEEE*, a *Fellow* of the *American Association for the Advancement of Science* (AAAS), and a corresponding member of the *Academy of Sciences of Portugal* (Section of Sciences). He was awarded the 2003 *IEEE Signal Processing Society Meritorious Service Award*, in 2000 the *IEEE Millennium Medal*, in 2006 an *IBM Faculty Award*, and in 2007 the CMU College of Engineering *Outstanding Research Award* (with Püschel). He is affiliated with several IEEE societies, Sigma Xi, AMS, AAAS, IMS, and SIAM.