Minimal Realizations of Linear Systems: The "Shortest Basis" Approach

G. David Forney, Jr.[*]

Dedicated to the memory of Ralf Koetter (1963-2009)

Abstract

Given a discrete-time linear system $\mathcal{C}$, a shortest basis for $\mathcal{C}$ is a set of linearly independent generators for $\mathcal{C}$ with the least possible lengths. A basis $\mathcal{B}$ is a shortest basis if and only if it has the predictable span property (*i.e.,* has the predictable delay and degree properties, and is non-catastrophic), or alternatively if and only if it has the subsystem basis property (for any interval $\mathcal{J}$, the generators in $\mathcal{B}$ whose span is in $\mathcal{J}$ is a basis for the subsystem $\mathcal{C}_{\mathcal{J}}$). The dimensions of the minimal state spaces and minimal transition spaces of $\mathcal{C}$ are simply the numbers of generators in a shortest basis $\mathcal{B}$ that are active at any given state or symbol time, respectively. A minimal linear realization for $\mathcal{C}$ in controller canonical form follows directly from a shortest basis for $\mathcal{C}$, and a minimal linear realization for $\mathcal{C}$ in observer canonical form follows directly from a shortest basis for the orthogonal system $\mathcal{C}^{\perp}$. This approach seems conceptually simpler than that of classical minimal realization theory.

Keywords: linear systems, minimal realizations

> It can scarcely be denied that the supreme goal of all theory is to make the irreducible basic elements as simple and as few as possible.— A. Einstein [2][1]

I. Introduction

The minimal realization problem of linear system theory is the problem of finding a state-space realization for a given linear system, often time-invariant, that has the smallest possible state space(s), possibly in some predetermined canonical form. The problem becomes nontrivial in the general case of multivariable and/or time-varying linear systems. The system is usually specified by its impulse response(s), or by some realization that may be nonminimal.

This problem has been studied since the rise of the state-space paradigm in the early 1960s. The classical solution to this problem is usually expressed by the mantra "minimal = controllable + observable." Many concrete algorithms have been developed to solve it, typically making heavy use of linear algebra and matrix manipulations; see *e.g.,* [1].

There is a much simpler approach to the minimal realization problem, at least conceptually; namely, the "shortest basis" approach, as we shall call it here. For linear time-invariant systems,

[*] Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, MA 02139. E-mail: `forneyd@comcast.net`.

[1] In other words, everything should be made as simple as possible, but not simpler.

this approach was developed in [6]. It has been used extensively in the literature of minimal trellis (state-space) realizations of linear block codes [12, 14], where shortest bases are called "trellis-oriented" [7] or "minimum-span" generator matrices. Analogous results are developed in a very general group-theoretic setting in [8]. This paper may be regarded either as a specialization of [8] to the case of linear systems over fields, or, preferably (because all proofs are linear-algebraic), a generalization of [6] to time-varying linear systems, or of [12] to infinite-time-axis linear systems.

Much of this paper is a tutorial overview of known results, aimed particularly at a system-theory audience. The following two results are new, as far as we know:

- $\mathcal{B}$ is a shortest basis if and only if it has the predictable span property;
- $\mathcal{B}$ is a shortest basis if and only if it has the subsystem basis property.

But many of these results are not very well known, at least in system theory, and many of the proofs are new.

II. Preliminaries

We focus on *linear discrete-time systems* over a field $\mathbb{F}$. In system theory, $\mathbb{F}$ is usually the real field $\mathbb{R}$ or the complex field $\mathbb{C}$, whereas in coding theory $\mathbb{F}$ is usually a finite field. The astute reader will notice that most proofs depend only on the group property of linear systems, and therefore apply more generally to group systems. The reader will also observe that our approach is entirely algebraic, and that analytical issues such as stability and convergence play no role.

A discrete-time system has a discrete, ordered *time axis* $\mathcal{I}$, which we take to be the set of integers $\mathbb{Z}$, or a subinterval of $\mathbb{Z}$. We use notation such as $[n, m) = \{k \in \mathbb{Z} : n \leq k < m\}$ for subintervals of $\mathbb{Z}$.

Here, as in behavioral system theory [15], a system will be defined by the set $\mathcal{C}$ of all of its possible *trajectories* $\mathbf{a} = \{a_k : k \in \mathcal{I}\}$ (its "behavior"), where each *symbol* a_k lies in some *alphabet* A_k. If the system is *linear* over a field $\mathbb{F}$, then each alphabet A_k is a vector space over $\mathbb{F}$, assumed to be finite-dimensional, and $\mathcal{C}$ is a subspace of the Cartesian-product vector space $\mathcal{A} = \prod_{k \in \mathcal{I}} A_k$.

If all alphabets A_k are equal to $\mathbb{F}$, then a trajectory $\mathbf{a}$ may be represented by its z-transform $a(z) = \sum_k a_k z^{-k}$, as in linear system theory, or by its D-transform $a(D) = \sum_k a_k D^k$, as in coding theory. The subtle difference (apart from the obvious difference $D = z^{-1}$) is that D is simply an indeterminate, whereas z is often regarded as a complex variable. We shall use both kinds of transforms in this paper, but we shall always regard z as simply an indeterminate.

The *support* of a trajectory $\mathbf{a}$ is the subset of all indices $k \in \mathcal{I}$ such that $a_k \neq 0$. A trajectory is *zero, finite* or *infinite* according to whether the size of its support is zero, finite or infinite.

If the support of a nonzero trajectory $\mathbf{a}$ has a minimum element $k_{\min}$, then $\mathbf{a}$ is called *Laurent*, and $k_{\min}$ is called the *delay* of $\mathbf{a}$, denoted by del $\mathbf{a} = k_{\min}$. By convention, the zero trajectory is defined as Laurent, and its delay is defined as del $\mathbf{0} = +\infty$.

In the body of this paper, we shall require all trajectories to be Laurent, as is common in coding theory. This restriction simplifies our exposition and yields a symmetrical duality theory, but forecloses consideration of uncontrollable systems with autonomous components. In an appendix, we show that the extension of our approach to uncontrollable/autonomous systems is straightforward.

If the support of $\mathbf{a}$ has a maximum element $k_{\max}$, then $k_{\max}$ is called the *degree* of $\mathbf{a}$, denoted by $\deg \mathbf{a} = k_{\max}$. By convention, the degree of the zero trajectory is defined as $\deg \mathbf{0} = -\infty$.

The set of all z-transforms $a(z)$ or D-transforms $a(D)$ of Laurent trajectories $\mathbf{a}$ over $\mathbb{F}$ on the time axis $\mathcal{I} = \mathbb{Z}$ is called the set of all *formal Laurent series* in $\mathbb{F}$ over z^{-1} or D, and is conventionally denoted by $\mathbb{F}((z^{-1}))$ or $\mathbb{F}((D))$, respectively. A nice algebraic property of $\mathbb{F}((z^{-1}))$ or $\mathbb{F}((D))$ is that it forms a field, with multiplication defined by sequence convolution. In particular, every nonzero $a(z) \in \mathbb{F}((z^{-1}))$ has a Laurent inverse $1/a(z)$, which may be computed by long division.

The set of all z-transforms $a(z)$ or D-transforms $a(D)$ of finite trajectories $\mathbf{a}$ over $\mathbb{F}$ with del $\mathbf{a} \geq 0$ is called the set of all *polynomials* in $\mathbb{F}$ over z^{-1} or D, and is denoted by $\mathbb{F}[z^{-1}]$ or $\mathbb{F}[D]$, respectively. For polynomials, our definition of "degree" coincides with the standard definition.

A *linear time-invariant* (LTI) system is a linear system $\mathcal{C}$ whose time axis is $\mathcal{I} = \mathbb{Z}$, whose alphabets A_k are all equal, and which satisfies $D\mathcal{C} = \mathcal{C}$, where D is the *delay operator* that transforms $\mathbf{a} \in \mathcal{C}$ to $D\mathbf{a} = \{a_{k-1} : k \in \mathcal{I}\}$. (This usage of D is compatible with that in D-transforms, since if the D-transform $\mathbf{a}$ is $a(D)$, then that of $D\mathbf{a}$ is $Da(D)$.) This implies that if $\mathbf{a} \in \mathcal{C}$, then every positive or negative shift $D^k\mathbf{a}, k \in \mathbb{Z}$, is in $\mathcal{C}$. Note that the set $\mathbb{F}((D))$ of all formal Laurent series over $\mathbb{F}$ is time-invariant.

It is natural to define a linear system $\mathcal{C}$ by a linearly independent set $\mathbf{g}$ of *generators*, called a *basis*, such that every trajectory in $\mathcal{C}$ is a unique linear (over $\mathbb{F}$) combination of the generators. We say that a generator is *involved in* a linear combination if it has a nonzero coefficient in that combination. For an LTI system, it is natural to choose a basis that consists of all the shifts $D^k\mathbf{g}_j, k \in \mathbb{Z}$, of a set $\{\mathbf{g}_j\}$ of *fundamental generators* $\mathbf{g}_j$.

Example 1 (single-input, single-output LTI system). Consider a real or complex discrete-time linear filter whose impulse response has z-transform $g(z) = 1/(1-\beta z^{-1})$, which denotes the Laurent z-transform $1 + \beta z^{-1} + \beta^2 z^{-2} + \cdots$.[2] What is the set $\mathcal{C}$ of trajectories associated with this filter? We might say that $\mathcal{C}$ is the set of all output sequences of the filter in response to all Laurent input sequences. But then $\mathcal{C}$ would simply be the set of all Laurent sequences, since every Laurent sequence $a(z)$ could be the output sequence if the input were the Laurent sequence $a(z)(1-\beta z^{-1})$; so such a definition would fail to capture the particular characteristics of this filter. Therefore we instead define the set $\mathcal{C}$ of trajectories of this system as the set of all input-output pairs as the input runs through all Laurent sequences:

$$\mathcal{C} = \{(u(z), u(z)g(z)) : u(z) \in \mathbb{F}((z^{-1}))\}.$$

$\mathcal{C}$ is evidently an LTI system. The set of all shifts of the fundamental input-output pair $(1, g(z))$ is a basis for $\mathcal{C}$. □

Example 2 (binary linear block code). The $(8, 4, 4)$ first-order binary Reed-Muller code is the four-dimensional subspace $\mathcal{C}$ of $(\mathbb{F}_2)^8$ that comprises all 16 binary 8-tuples that can be obtained as binary linear combinations of the following four generators:

$$\begin{aligned} \mathbf{g}_1 &= 11110000; \\ \mathbf{g}_2 &= 11001100; \\ \mathbf{g}_3 &= 10101010; \\ \mathbf{g}_4 &= 11111111. \end{aligned}$$

$\mathcal{C}$ may be regarded as a linear system over the binary field $\mathbb{F}_2$ that is defined on the finite time axis $\mathcal{I} = [0, 8)$, with the basis given above. Of course, a system defined on a finite time axis cannot be time-invariant. □

[2] We need not restrict $|\beta| < 1$ if we are not concerned with issues of stability or convergence.

Given a linear system $\mathcal{C} \subseteq \mathcal{A} = \Pi_{k \in \mathcal{I}} A_k$ defined on a time axis $\mathcal{I}$, a (state-space) *realization* of $\mathcal{C}$ (sometimes called a "trellis realization" in coding theory) will be defined in terms of:

- A *state time axis* $\mathcal{I}_S \subseteq \mathbb{Z}$, such that symbol time $k \in \mathcal{I}$ occurs *between* state time $k \in \mathcal{I}_S$ and state time $k+1 \in \mathcal{I}_S$. If $\mathcal{I} = \mathbb{Z}$, we take $\mathcal{I}_S = \mathbb{Z}$; but if $\mathcal{I} = [0, n)$, we take $\mathcal{I}_S = [0, n]$.
- A set of *state spaces* $\Sigma_k, k \in \mathcal{I}_S$.
- For each $k \in \mathcal{I}$, a set $\mathcal{T}_k$ of allowable *transitions* $(\sigma_k, a_k, \sigma_{k+1}) \in \Sigma_k \times A_k \times \Sigma_{k+1}$.

The *full behavior* $\mathfrak{B}$ of the realization is then the set of all symbol-state trajectories $(\mathbf{a}, \boldsymbol{\sigma}) \in \mathcal{A} \times \Pi_{k \in \mathcal{I}_S} \Sigma_k$ such that $(\sigma_k, a_k, \sigma_{k+1}) \in \mathcal{T}_k$ for all $k \in \mathcal{I}$. The system $\mathcal{C}$ realized by the realization is the set of all symbol trajectories $\mathbf{a} \in \mathcal{A}$ that appear in some symbol-state trajectory $(\mathbf{a}, \boldsymbol{\sigma}) \in \mathfrak{B}$.

A realization is *linear* if all symbol alphabets A_k and state spaces Σ_k are vector spaces over a field $\mathbb{F}$, and the *transition spaces* $\mathcal{T}_k$ ("local behaviors") are subspaces of the vector spaces $\Sigma_k \times A_k \times \Sigma_{k+1}$ for all $k \in \mathcal{I}$. A realization is *minimal* if the state spaces Σ_k are as small as possible for all $k \in \mathcal{I}_S$. We will see that every linear system $\mathcal{C}$ has a realization that is both linear and minimal.

III. Minimal state and transition spaces

In this section we recapitulate well-known results about minimal state spaces, and less well-known results about minimal transition spaces.

A. Minimal state spaces

A fundamental result of Willems' behavioral system theory [15, 16] is that, given a linear system $\mathcal{C}$, the minimal state space at each possible state time is unambiguously defined.

A state space Σ_k at state time $k \in \mathcal{I}_S$ may be considered to be defined by a *cut* of the symbol time axis $\mathcal{I}$ between symbol time $k-1$ and symbol time k. Such a cut partitions $\mathcal{I}$ into two disjoint subintervals: a *past* $k^- = \{k' \in \mathcal{I} : k' < k\}$ and a *future* $k^+ = \{k' \in \mathcal{I} : k' \geq k\}$.

The fundamental property of states is the *Markov property*: the future should be conditionally independent of the past, given the state. In a state-space realization, this translates to a requirement that two symbol trajectories up to time $k-1$ may arrive at the same state in Σ_k if and only if the sets of their possible future continuations from time k on are identical.[3]

In the linear case, it is easy to identify when this happens. Let the *past subsystem* $\mathcal{C}_{k^-}$ and *future subsystem* $\mathcal{C}_{k^+}$ be defined as the subsets of $\mathcal{C}$ that are all-zero on the future k^+ and the past k^-, respectively. Both $\mathcal{C}_{k^-}$ and $\mathcal{C}_{k^+}$ are evidently linear subsystems of $\mathcal{C}$. Then the *minimal state space* at state time k is the following quotient space:

$$\Sigma_k = \frac{\mathcal{C}}{\mathcal{C}_{k^-} \times \mathcal{C}_{k^+}}.$$

The proof is essentially as follows. The quotient space $\mathcal{C}/(\mathcal{C}_{k^-} \times \mathcal{C}_{k^+})$ is a disjoint union of cosets $\mathbf{a} + (\mathcal{C}_{k^-} \times \mathcal{C}_{k^+})$, where each coset representative $\mathbf{a}$ is a trajectory in $\mathcal{C}$. Define $P_{k^-} : \mathcal{A} \to \mathcal{A}$ and $P_{k^+} : \mathcal{A} \to \mathcal{A}$ as the projection operators onto the past k^- and future k^+, respectively. The coset $\mathbf{a} + (\mathcal{C}_{k^-} \times \mathcal{C}_{k^+})$ is then precisely the Cartesian product

[3] In automata theory, this is called *Nerode equivalence.*

$$\mathbf{a} + (\mathcal{C}_{k^-} \times \mathcal{C}_{k^+}) = (P_{k^-}(\mathbf{a}) + \mathcal{C}_{k^-}) \times (P_{k^+}(\mathbf{a}) + \mathcal{C}_{k^+})\,;$$

i.e., the set of trajectories in $\mathcal{C}$ whose past projections are in the coset $P_{k^-}(\mathbf{a}) + \mathcal{C}_{k^-}$ of $\mathcal{C}_{k^-}$, and whose future projections are in the coset $P_{k^+}(\mathbf{a}) + \mathcal{C}_{k^+}$ of $\mathcal{C}_{k^+}$. Since every such past projection has the same set of future continuations, all of these trajectories may pass through the same state at time k. On the other hand, any past projection in any other coset may not pass through the same state at time k, since it has a disjoint set of future continuations. Thus any minimal state space must be in one-to-one correspondence with this set of cosets; *i.e.,* with Σ_k.

By a simple extension of the above argument, or by an elementary result in group theory (the first theorem about subdirect products in [10]), the minimal state space Σ_k is also isomorphic to the following quotient spaces, called the "past-induced" and "future-induced" state spaces:

$$\Sigma_k \simeq \frac{P_{k^-}(\mathcal{C})}{\mathcal{C}_{k^-}} \simeq \frac{P_{k^+}(\mathcal{C})}{\mathcal{C}_{k^+}},$$

where $P_{k^-}(\mathcal{C})$ and $P_{k^+}(\mathcal{C})$ are the sets of past and future projections of $\mathcal{C}$, respectively.

It is straightforward to define a linear state-space realization of a linear system $\mathcal{C}$ that uses the minimal state spaces Σ_k for every time k. Let each trajectory $\mathbf{a} \in \mathcal{C}$ pass through the sequence of states $\sigma_k(\mathbf{a}) \in \Sigma_k$ for all k that are defined by the natural maps from $\mathcal{C}$ to the quotient spaces $\mathcal{C}/(\mathcal{C}_{k^-} \times \mathcal{C}_{k^+})$. This is called the *canonical realization* of a linear system $\mathcal{C}$. Among other things, the canonical realization shows that there exist linear realizations whose state spaces are minimal at every time $k \in \mathcal{I}_S$.

We shall require that all minimal state spaces Σ_k be finite-dimensional. As we shall see shortly, this condition ensures that only finitely many generators in a shortest basis $\mathcal{B}$ will be "active" at any state time k, which in turn ensures that the number of generators that affect any component a_k of any trajectory $\mathbf{a} \in \mathcal{C}$ will be finite, even when $\mathcal{B}$ is infinite.

B. Minimal transition spaces

We now discuss minimal transition spaces. In coding theory, transition spaces ("branch spaces," "trellis sections," "local constraint codes") have come to be regarded as having importance equal to or possibly even greater than that of state spaces.

Minimal transition spaces are characterized by the following theorem:

Theorem 1 (Minimal transition spaces) *In any minimal realization of a linear system $\mathcal{C}$, for every symbol time $k \in \mathcal{I}$, the set of transitions is in one-to-one correspondence with the following quotient space, called the* minimal transition space *at symbol time k:*

$$\mathcal{T}_k = \frac{\mathcal{C}}{\mathcal{C}_{k^-} \times \mathcal{C}_{(k+1)^+}}.$$

Proof. In a minimal realization, the state spaces Σ_k and Σ_{k+1} are in one-to-one correspondence to $P_{k^-}/\mathcal{C}_{k^-}$ and $P_{(k+1)^+}/\mathcal{C}_{(k+1)^+}$, respectively. The set of all trajectories $\mathbf{a} \in \mathcal{C}$ that pass through a given transition $(\sigma_k, a_k, \sigma_{k+1}) \in \Sigma_k \times A_k \times \Sigma_{k+1}$ is the set that have a past projection $P_{k^-}(\mathbf{a})$ in the coset of $\mathcal{C}_{k^-}$ that corresponds to σ_k, a time-k projection $P_{\{k\}}(\mathbf{a})$ equal to a_k, and a future projection $P_{(k+1)^+}(\mathbf{a})$ in the coset of $\mathcal{C}_{(k+1)^+}$ that corresponds to σ_{k+1}. Thus the trajectories of $\mathcal{C}$ that pass through the same transition at symbol time k are precisely those that lie in the same coset of $\mathcal{C}_{k^-} \times \mathcal{C}_{(k+1)^+}$, so the set of transitions corresponds one-to-one to the set $\mathcal{T}_k$ of cosets of $\mathcal{C}_{k^-} \times \mathcal{C}_{(k+1)^+}$ in $\mathcal{C}$. □

It is easy to see that in a canonical realization, each trajectory $\mathbf{a} \in \mathcal{C}$ passes through the sequence of transitions that are defined by the natural maps from $\mathcal{C}$ to the quotient spaces $\mathcal{C}/(\mathcal{C}_{k^-} \times \mathcal{C}_{k+1^+})$, where $\sigma_k(\mathbf{a})$ and $\sigma_{k+1}(\mathbf{a})$ are identified with past-induced and future-induced states, respectively.

IV. Shortest bases and minimal realizations

It is convenient to have a basis for a linear system $\mathcal{C}$ from which a minimal state-space realization of $\mathcal{C}$ and its parameters can be read directly, "by inspection." In this section we will see that a shortest basis has these properties. In the literature of minimal trellis realizations of linear block codes, such a shortest basis is called a "trellis-oriented" or "minimum-span" generator matrix [12, 14]. In system theory terms, it yields a minimal realization of $\mathcal{C}$ in "controller canonical form" [11].

We first mention some technical "well-behavedness" requirements that we impose on $\mathcal{C}$ for simplicity. Let $\mathcal{C}_{\text{finite}}$ denote the set of all finite trajectories in $\mathcal{C}$. We say that a linear combination of trajectories is *Laurent* if it involves only trajectories whose delays are not less than some minimum delay $k_{\min}$; then the combination is a Laurent trajectory with delay $\geq k_{\min}$. We require that $\mathcal{C}$ be the set of all Laurent linear combinations of $\mathcal{C}_{\text{finite}}$. Then $\mathcal{C}$ is generated by its finite trajectories; such a linear system is called *controllable* [16, 3]. Also, $\mathcal{C}$ is then complete [16] in a Laurent sense; indeed, $\mathcal{C}$ is the Laurent completion of $\mathcal{C}_{\text{finite}}$. For an extension of our development to uncontrollable systems, see the Appendix, or [8].

A. Shortest bases

The *span* of a nonzero finite trajectory $\mathbf{a} \in \mathcal{A}$ is the shortest interval that contains its support, namely $[\text{del}\, \mathbf{a}, \deg \mathbf{a}]$, and the *length* of $\mathbf{a}$ is the size of its span, namely $\deg \mathbf{a} - \text{del}\, \mathbf{a} + 1$.

Loosely, a *shortest basis* $\mathcal{B}$ for a linear system $\mathcal{C}$ will be defined as a basis whose elements are as short as possible. We will see as we proceed that this concept is well defined.

Example 1 (cont.). Recall that the single-input, single-output linear time-invariant system of Example 1 is defined as the set $\mathcal{C}$ of all input-output pairs

$$\mathcal{C} = \{u(z)(1, g(z)) : u(z) \in \mathbb{F}((z^{-1}))\}$$

as the input $u(z)$ runs through all Laurent sequences, where $g(z) = 1/(1 + \beta z^{-1})$. In other words, $\mathcal{C}$ is the set of all multiples of the basic input-output pair $(1, g(z))$ by sequences in the Laurent field $\mathbb{F}((z^{-1}))$. It is easy to see that a nonzero trajectory in $\mathcal{C}$ is finite if and only if the corresponding input sequence $u(z)$ is a finite multiple of $1/g(z) = 1+\beta z^{-1}$. Hence the set $\mathcal{C}_{\text{finite}}$ of finite trajectories in $\mathcal{C}$ is the set of multiples of the finite pair $(1 + \beta z^{-1}, 1)$ by finite Laurent sequences $v(z)$:

$$\mathcal{C}_{\text{finite}} = \{(v(z)(1 + \beta z^{-1}), v(z)) : v(z) \in (\mathbb{F}((z^{-1})))_{\text{finite}}\},$$

From this it is clear that the shortest trajectories in $\mathcal{C}$ have length 2, and that the set of shifts of the length-2 trajectory $(1 + \beta z^{-1}, 1)$ is a shortest basis $\mathcal{B}$ for $\mathcal{C}$. □

Example 2 (cont.). Recall that the $(8, 4, 4)$ binary Reed-Muller code of Example 2 is the set $\mathcal{C}$ of all 16 binary linear combinations of the four generators $(11110000, 11001100, 10101010, 11111111)$. By examining all 16 codewords, we find that the shortest nonzero codewords are the three length-4 8-tuples $11110000, 00111100$ and 00001111, which are evidently independent. The next-shortest codeword that is independent of the previous three is the length-6 8-tuple 01011010. Since the dimension of $\mathcal{C}$ is 4, these four 8-tuples comprise a shortest basis $\mathcal{B}$ for $\mathcal{C}$. □

A shortest basis $\mathcal{B}$ may be found by the following greedy construction. Recall that if $\mathcal{J}$ is a subinterval of the time axis $\mathcal{I}$, then $\mathcal{C}_{\mathcal{J}}$ denotes the *subsystem* of $\mathcal{C}$ consisting of all trajectories $\mathbf{a} \in \mathcal{C}$ whose span is contained in $\mathcal{J}$. First, for every length-1 subinterval $\mathcal{J} \subseteq \mathcal{I}$, find a set of linearly independent length-1 generators for $\mathcal{C}_{\mathcal{J}}$. Next, for every length-2 subinterval $\mathcal{J} \subseteq \mathcal{I}$, find a minimal set of additional independent length-2 generators sufficient (in combination with the previous length-1 generators) to generate all length-2 trajectories in $\mathcal{C}_{\mathcal{J}}$. And so forth.

Assuming that $\mathcal{C}$ is controllable, this algorithm will eventually find a shortest basis $\mathcal{B}$ of finite linearly independent generators for $\mathcal{C}$. Furthermore, it is clear that any shortest basis for $\mathcal{C}$ may be constructed in this way. Since dim $\mathcal{C}_{\mathcal{J}}$ is a parameter of the system $\mathcal{C}$ for every subinterval $\mathcal{J} \subseteq \mathcal{I}$, it follows that the set of lengths of generators in any shortest basis $\mathcal{B}$ for $\mathcal{C}$ is the same.

B. The predictable span property and the subsystem basis property

We now introduce two properties, the predictable span property and the subsystem basis property, and show that a basis $\mathcal{B}$ is a shortest basis if and only if it has either of these properties.

We note that linear independence implies that every trajectory $\mathbf{a} \in \mathcal{C}$ has a unique expression as a (possibly infinite) linear combination of generators in $\mathcal{B}$, so that we may speak of the *generators of* $\mathbf{a}$, meaning the subset $\mathcal{S}(\mathbf{a})$ of generators of $\mathcal{B}$ that are involved in this unique linear combination.

If $\mathcal{S}(\mathbf{a})$ is the set of generators of a trajectory $\mathbf{a} \in \mathcal{C}$, then del $\mathbf{a} \geq k_{\min} = \min_{\mathbf{g} \in \mathcal{S}(\mathbf{a})}$ del $\mathbf{g}$, and $\deg \mathbf{a} \leq k_{\max} = \max_{\mathbf{g} \in \mathcal{S}(\mathbf{a})} \deg \mathbf{g}$, where strict inequality may occur due to cancellations. A basis $\mathcal{B}$ has the **predictable span property** (PSP) if inequality never occurs; *i.e.,* if the span of $\mathbf{a}$ is always equal to $[k_{\min}, k_{\max}]$.

For finite linear combinations, $\mathcal{B}$ evidently has the PSP if and only if it has the *predictable delay property* (*i.e.,* del $\mathbf{a} = k_{\min}$ always) and the *predictable degree property* (*i.e.,* $\deg \mathbf{a} = k_{\max}$ always) [6]. Clearly $\mathcal{B}$ has the predictable delay property if and only if the time-k symbols of the delay-k generators in $\mathcal{B}$ are linearly independent, so cancellation can never occur; similarly $\mathcal{B}$ has the predictable degree property if and only if the time-k symbols of the degree-k generators in $\mathcal{B}$ are linearly independent.

These linear independence properties have an immediate corollary:

Lemma 2 (A finite number of generators start and stop at each time) *If a basis $\mathcal{B}$ for $\mathcal{C}$ has the predictable delay (resp. degree) property, then the number of generators in $\mathcal{B}$ that have delay k (resp. degree k) is not greater than* $\dim A_k$. *In particular, if* $\dim A_k = 1$*, then at most one generator in $\mathcal{B}$ can start or stop at time k.*

Proof. If $\mathcal{B}$ has the predictable delay property, then the set of time-k symbols of delay-k generators in $\mathcal{B}$ is a linearly independent subset of elements of the time-k symbol alphabet A_k; similarly the set of time-k symbols of degree-k generators in $\mathcal{B}$ is a linearly independent subset of A_k. □

Now let us consider infinite Laurent linear combinations. Recall that a linear combination of generators is *Laurent* if it involves only generators whose delays are not less than some finite minimum delay $k_{\min}$. On the other hand, we must have $k_{\max} = \infty$, since an infinite number of generators are involved and there can only be a finite number of each finite degree, under our assumption that $\dim A_k$ is finite. Therefore $\mathcal{B}$ has the PSP for infinite linear combinations if and only if it has the predictable delay property and all infinite linear combinations are infinite. (See Section V for examples of infinite linear combinations that are finite.)

Borrowing a term from coding theory, we say that a basis $\mathcal{B}$ for $\mathcal{C}$ is *catastrophic* if there exists a finite $\mathbf{a} \in \mathcal{C}$ that is equal to an infinite linear combination of generators. Thus, in summary, $\mathcal{B}$ has the PSP if and only if $\mathcal{B}$ has the predictable delay and degree properties, and $\mathcal{B}$ is non-catastrophic.

Secondly, we will say that a basis $\mathcal{B}$ has the **subsystem basis property** (SBP) if for any subinterval $\mathcal{J}$ of the time axis $\mathcal{I}$, the set of generators in $\mathcal{B}$ whose span is contained in $\mathcal{J}$ is a basis for the subsystem $\mathcal{C}_{\mathcal{J}}$. By construction, a shortest basis has this property for all finite $\mathcal{J}$.

Now we show that a basis $\mathcal{B}$ is a shortest basis if and only if it has the PSP, or the SBP:

Theorem 3 (Shortest basis $\Leftrightarrow$ PSP $\Leftrightarrow$ SBP) *For a basis $\mathcal{B}$ of a controllable linear system $\mathcal{C}$, the following are equivalent:*

1. *$\mathcal{B}$ has the predictable span property;*

2. *$\mathcal{B}$ has the subsystem basis property;*

3. *$\mathcal{B}$ is a shortest basis for $\mathcal{C}$.*

Proof. ($1 \Rightarrow 2$) On the one hand, a linear combination of generators in $\mathcal{B}$ whose span is contained in $\mathcal{J}$ must be a trajectory $\mathbf{a} \in \mathcal{C}_{\mathcal{J}}$. On the other hand, if $\mathcal{B}$ has the PSP and $\mathbf{a} \in \mathcal{C}_{\mathcal{J}}$, then the minimum degree of the generators of $\mathbf{a}$ is $\operatorname{del} \mathbf{a} \in \mathcal{J}$, and the maximum degree is $\deg \mathbf{a} \in \mathcal{J}$, so every $\mathbf{a} \in \mathcal{C}_{\mathcal{J}}$ is a linear combination of generators in $\mathcal{B}$ whose span is contained in $\mathcal{J}$.

($2 \Rightarrow 3$) If $\mathcal{B}$ has the SBP, then, for each finite subinterval $\mathcal{J}$, the generators in $\mathcal{B}$ whose span is precisely $\mathcal{J}$ could be chosen in the shortest-basis construction process, so $\mathcal{B}$ is a shortest basis.

($3 \Rightarrow 1$) If $\mathcal{B}$ is a shortest basis for $\mathcal{C}$, then the set of time-k symbols of delay-k generators must be a linearly independent subset of the time-k symbol alphabet A_k, else there would be a finite linear combination $\mathbf{b}$ of delay-k generators with $\operatorname{del} \mathbf{b} > k$, and with $\deg \mathbf{b} \leq k_{\max} = \deg \mathbf{g}$, the degree of a greatest-degree generator $\mathbf{g}$ involved in this linear combination, so $\mathbf{b}$ would be shorter than $\mathbf{g}$, and $\mathbf{b}$ could replace $\mathbf{g}$ in $\mathcal{B}$ to produce a shorter basis $\mathcal{B}'$; contradiction. So $\mathcal{B}$ must have the predictable degree property. Similarly, $\mathcal{B}$ must have the predictable delay property. Finally, by the shortest-basis construction, every finite trajectory $\mathbf{a} \in \mathcal{C}$ is uniquely expressible as a finite linear combination of finite generators in $\mathcal{B}$, so $\mathcal{B}$ must be non-catastrophic. □

C. Dimensions of minimal state and transition spaces

We now show how to determine the dimension of the minimal state space $\Sigma_k = \mathcal{C}/(\mathcal{C}_{k^-} \times \mathcal{C}_{k^+})$ "by inspection" from any shortest basis $\mathcal{B}$ for a linear system $\mathcal{C}$, for any cut of the time axis $\mathcal{I}$ into a past subset k^- and a future subset k^+.

We partition the generators in $\mathcal{B}$ into three subsets: a past subset S_{k^-} consisting of those generators in $\mathcal{B}$ whose support is contained in k^-, a future subset S_{k^+} consisting of those generators in $\mathcal{B}$ whose support is contained in k^+, and a remainder subset R_k consisting of the remaining generators, which we call the *active generators at state time $k \in \mathcal{I}_S$*. By the subsystem basis property of shortest bases, S_{k^-} is a basis for $\mathcal{C}_{k^-}$ and S_{k^+} is a basis for $\mathcal{C}_{k^+}$.

Theorem 4 (Minimal state space dimension) *For any state time $k \in \mathcal{I}_S$, the dimension of the minimal state space Σ_k of a linear system $\mathcal{C}$ is the number of active generators at state time k in any shortest basis $\mathcal{B}$ for $\mathcal{C}$.*

Proof. Since $\mathcal{B}$ is a basis for $\mathcal{C}$, S_{k^-} is a basis for $\mathcal{C}_{k^-}$, and S_{k^+} is a basis for $\mathcal{C}_{k^+}$, the quotient space $\Sigma_k = \mathcal{C}/(\mathcal{C}_{k^-} \times \mathcal{C}_{k^+})$ has a basis consisting of the remaining linearly independent generators in the remainder subset R_k, and thus has dimension $|R_k|$. □

Example 1 (cont.). Recall that a shortest basis for the system $\mathcal{C}$ of Example 1 is the set of shifts of the length-2 trajectory $(1 + \beta z^{-1}, 1)$. For any state time $k \in \mathbb{Z}$, precisely one of these generators is active; for example, at state time 1, only the fundamental generator $(1 + \beta z^{-1}, 1)$ is active, since all of its shifts have supports either in the past $1^- = \{k < 1\}$ or in the future $1^+ = \{k \geq 1\}$. Thus the dimension of the minimal state space Σ_k of $\mathcal{C}$ at any state time $k \in \mathbb{Z}$ is 1.

More generally, let $\mathcal{C}$ be any single-input, single-output LTI system consisting of all input-output trajectories $\{u(z)(1, g(z)) : u(z) \in \mathbb{F}((z^{-1}))\}$, where $g(z)$ is a causal rational impulse response $g(z) = a(z)/b(z)$ with $a(z), b(z)$ being relatively prime polynomials in $\mathbb{F}[z^{-1}]$, with del $a(z) \geq 0$ and del $b(z) = 0$. Then a shortest basis for $\mathcal{C}$ is the set of all shifts of the fundamental input-output trajectory $(b(z), a(z))$, whose delay is 0 and whose degree is $\delta = \max\{\deg b(z), \deg a(z)\}$. Precisely δ of these shifts are active at any state time $k \in \mathbb{Z}$; therefore the dimension of the minimal state space Σ_k of $\mathcal{C}$ at any state time $k \in \mathbb{Z}$ is δ. □

Example 2 (cont.). Recall that the $(8, 4, 4)$ code of Example 2 has the following shortest basis:

$$\begin{aligned} \mathbf{g}_1 &= 11110000; \\ \mathbf{g}_2 &= 00111100; \\ \mathbf{g}_3 &= 00001111; \\ \mathbf{g}_4 &= 01011010. \end{aligned}$$

Notice that the generators in this set "start" at symbol times $0, 1, 2$ and 4, and "stop" at symbol times $3, 5, 6$ and 7. The numbers of generators that are active at state times $0, 1, \ldots, 8$ are therefore $0, 1, 2, 3, 2, 3, 2, 1, 0$, respectively, which are therefore the minimal state space dimensions at these times. We say that the *state-space dimension profile* of $\mathcal{C}$ is $\{0, 1, 2, 3, 2, 3, 2, 1, 0\}$. □

Similarly, from the minimal transition space theorem, we can determine the dimension of the minimal transition space $\mathcal{T}_k$ from any shortest basis $\mathcal{B}$ for a linear system $\mathcal{C}$. We now partition the time axis $\mathcal{I}$ into three subintervals: a past interval k^-, the time $\{k\}$, and a future interval $(k+1)^+$. We partition the generators in $\mathcal{B}$ into three subsets: a past subset S_{k^-} consisting of those generators in $\mathcal{B}$ whose support is contained in k^-, a future subset $S_{(k+1)^+}$ consisting of those generators in $\mathcal{B}$ whose support is contained in $(k+1)^+$, and a remainder subset T_k consisting of the remaining generators, which we call the *active generators at symbol time* $k \in \mathcal{I}$.

Theorem 5 (Minimal transition space dimension) *For any symbol time $k \in \mathcal{I}$, the dimension of the minimal transition space $\mathcal{T}_k$ of a linear system $\mathcal{C}$ is the number of active generators at symbol time k in any shortest basis $\mathcal{B}$ for $\mathcal{C}$.*

Proof. Since $\mathcal{B}$ is a basis for $\mathcal{C}$, S_{k^-} is a basis for $\mathcal{C}_{k^-}$, and $S_{(k+1)^+}$ is a basis for $\mathcal{C}_{(k+1)^+}$, the quotient space $\mathcal{T}_k = \mathcal{C}/(\mathcal{C}_{k^-} \times \mathcal{C}_{(k+1)^+})$ has a basis consisting of the remaining linearly independent generators in the remainder subset T_k, and thus has dimension $|T_k|$. □

Example 1 (cont.). For the system $\mathcal{C}$ of Example 1, we may take $\mathcal{B}$ as the set of shifts of the length-2 trajectory $(1 + \beta z^{-1}, 1)$. For any symbol time $k \in \mathbb{Z}$, precisely two of these generators are active; for example, at symbol time 1, the generators $(1 + \beta z^{-1}, 1)$ and $(z^{-1} + \beta z^{-2}, z^{-1})$ are both active. Thus the dimension of the minimal transition space $\mathcal{T}_k$ of $\mathcal{C}$ at any symbol time $k \in \mathbb{Z}$ is 2.

More generally, let $\mathcal{C}$ be any single-input, single-output LTI system whose shortest-generator set is the set of all shifts of the fundamental input-output trajectory $(b(z), a(z))$, whose delay is 0 and whose degree is $\delta = \max\{\deg b(z), \deg a(z)\}$; then precisely $\delta + 1$ of these shifts are active at any symbol time $k \in \mathbb{Z}$, so the dimension of the minimal transition space $\mathcal{T}_k$ of $\mathcal{C}$ at any symbol time $k \in \mathbb{Z}$ is $\delta + 1$. □

Example 2 (cont.). Given the shortest basis $\{11110000, 00111100, 00001111, 01011010\}$ for the binary code $\mathcal{C}$ of Example 2, we observe that the numbers of generators that are active at symbol times $0, 1, \ldots, 7$ are $1, 2, 3, 3, 3, 3, 2, 1$, respectively. Thus these are the minimal transition space dimensions. We say that the *transition-space dimension profile* of $\mathcal{C}$ is $\{1, 2, 3, 3, 3, 3, 2, 1\}$. □

In coding theory, the transition-space dimension profile of a linear code $\mathcal{C}$ is generally taken as a better measure of the complexity of trellis-based decoding than its state-space dimension profile.

D. Minimal realizations in controller canonical form

Given any shortest basis $\mathcal{B}$ for any linear system $\mathcal{C}$, we can now construct an obvious state-space realization for $\mathcal{C}$, sometimes called the *controller canonical form* [11], which is evidently minimal. For multivariable LTI systems, a construction of a minimal realization in controller canonical form from a shortest ("minimal") basis was given in [6]. In the literature of trellis realizations of block codes, such a construction was first given by Kschischang and Sorokine [12], who introduced the term "atomic."

With each generator $\mathbf{g} \in \mathcal{B}$, we associate an *atomic* state-space realization as follows. Roughly, it involves an "input" $\alpha \in \mathbb{F}$ that occurs at symbol time del $\mathbf{g}$; a "memory element" that stores α during the active state interval $(\text{del}\ \mathbf{g}, \deg \mathbf{g}]$; and an "output" whose value during the active symbol interval $[\text{del}\ \mathbf{g}, \deg \mathbf{g}]$ is $\alpha\mathbf{g}$.

More precisely, if del $\mathbf{g} < \deg \mathbf{g}$, then the state spaces of the atomic realization are equal to $\mathbb{F}$ during the active state interval $(\text{del}\ \mathbf{g}, \deg \mathbf{g}]$, and equal to the trivial space $\{0\}$ otherwise;[4] thus the state space dimension is 1 during the active interval and 0 otherwise. The sets of allowable transitions $\mathcal{T}_k$ are as given below during the active symbol interval $[\text{del}\ \mathbf{g}, \deg \mathbf{g}]$ (otherwise $\mathcal{T}_k = \{(0, 0, 0)\}$):

- For $k = \text{del}\ \mathbf{g}$, $\mathcal{T}_k = \{(0, \alpha g_k, \alpha) : \alpha \in \mathbb{F}\}$;
- For del $\mathbf{g} < k < \deg \mathbf{g}$, $\mathcal{T}_k = \{(\alpha, \alpha g_k, \alpha) : \alpha \in \mathbb{F}\}$;
- For $k = \deg \mathbf{g}$, $\mathcal{T}_k = \{(\alpha, \alpha g_k, 0) : \alpha \in \mathbb{F}\}$;

thus the transition space dimension is 1 during the active interval, and 0 otherwise.

The full behavior of this atomic realization is thus the one-dimensional vector space $\mathfrak{B} = \{(\mathbf{a} = \alpha\mathbf{g}, \boldsymbol{\sigma} = \alpha\mathbf{1}_{(\text{del}\ \mathbf{g}, \deg \mathbf{g}]}) : \alpha \in \mathbb{F}\}$, where $\mathbf{1}_{(\text{del}\ \mathbf{g}, \deg \mathbf{g}]}$ is the indicator function of the state interval $(\text{del}\ \mathbf{g}, \deg \mathbf{g}]$. The system that it realizes is the one-dimensional vector space $\{\alpha\mathbf{g} : \alpha \in \mathbb{F}\}$; *i.e.*, the subsystem of $\mathcal{C}$ that is generated by $\mathbf{g}$.

[4] If del $\mathbf{g} = \deg \mathbf{g}$, then $\Sigma_k = \{0\}$ for all $k \in \mathcal{I}_S$, and $\mathcal{T}_k = \{(0, \alpha g_k, 0) : \alpha \in \mathbb{F}\}$ at symbol time $k = \text{del}\ \mathbf{g} = \deg \mathbf{g}$; otherwise $\mathcal{T}_k = \{(0, 0, 0)\}$.

The whole state-space realization for $\mathcal{C}$ then consists of the aggregate of these atomic realizations for all $\mathbf{g} \in \mathcal{B}$, plus an adder which at each symbol time produces the sum of the outputs of the currently active atomic realizations. The set of all possible output trajectories of the whole realization is thus the set of all linear combinations $\sum_{\mathbf{g} \in \mathcal{B}} \alpha(\mathbf{g})\mathbf{g}$ of generators in $\mathcal{B}$, which is precisely the linear system $\mathcal{C}$. The number of memory elements active at any state time $k \in \mathcal{I}_S$ is the number of active generators at time k, which by the theorem above is the dimension of the minimal state space Σ_k for $\mathcal{C}$. Thus this aggregate "controller canonical form" realization is a minimal (and linear) realization of $\mathcal{C}$.

In a controller canonical realization of a linear time-invariant system, the lengths of the generators $\mathbf{g} \in \mathcal{B}$ are sometimes called the *controllability indices* of $\mathcal{C}$. Thus in a linear time-varying system, the lengths of the generators may be regarded as generalized controllability indices.

E. New information, and forgetting information

Further important quantities in a linear system $\mathcal{C}$ are the amount of information that enters or "drives" the system at each time, and also the amount that is "forgotten" at each time.

We define the *in-space* I_k at symbol time $k \in \mathcal{I}$ as the quotient space $\mathcal{C}_{k^+}/\mathcal{C}_{(k+1)^+}$; *i.e.,* the set of trajectories in $\mathcal{C}$ that start at time k or later, modulo those that start at time $k+1$ or later.

If $\mathcal{B}$ is a shortest basis for $\mathcal{C}$, then $\mathcal{C}_{k^+}$ is generated by the elements of $\mathcal{B}$ that have delay k or more, and $\mathcal{C}_{(k+1)^+}$ is generated by the elements of $\mathcal{B}$ that have delay $k+1$ or more; therefore:

Theorem 6 (In-space dimension) *For any symbol time $k \in \mathcal{I}$, the dimension of the in-space I_k of a linear system $\mathcal{C}$ is the number of delay-k generators in any shortest basis $\mathcal{B}$ for $\mathcal{C}$.*

As we have seen previously, the time-k symbols of delay-k generators in a shortest basis $\mathcal{B}$ must be linearly independent, so their number must satisfy $0 \leq \dim I_k \leq \dim A_k$.

Now if we compare the minimal state space $\Sigma_k = \mathcal{C}/(\mathcal{C}_{k^-} \times \mathcal{C}_{k^+})$ to the minimal transition space $\mathcal{T}_k = \mathcal{C}/(\mathcal{C}_{k^-} \times \mathcal{C}_{(k+1)^+})$, we see that

$$\dim \mathcal{T}_k = \dim \Sigma_k + \dim I_k.$$

In words, if we regard one element of the field $\mathbb{F}$ as one unit of information, then in a minimal realization of $\mathcal{C}$ the transition at symbol time k is completely determined by $\dim \Sigma_k$ units of state information at state time k, plus $\dim I_k$ new units of information at symbol time k. Indeed, in the controller canonical realization, we see explicitly that the system transition at symbol time k is completely determined by the coefficients of the $\dim \Sigma_k$ generators that are active at state time k, plus the $\dim I_k$ generators that start at symbol time k.

As an obvious corollary, if the minimal state spaces Σ_k and the symbol alphabets A_k are finite-dimensional, then the minimal transition spaces $\mathcal{T}_k$ are finite-dimensional.

Symmetrically, we may define the *out-space* O_k at symbol time $k \in \mathcal{I}$ as the quotient space $\mathcal{C}_{(k+1)^-}/\mathcal{C}_{k^-}$; then the dimension of O_k is the number of degree-k generators in any shortest basis $\mathcal{B}$ for $\mathcal{C}$, and we have $\dim \mathcal{T}_k = \dim \Sigma_{k+1} + \dim O_k$, where $0 \leq \dim O_k \leq \dim A_k$. In words, we may interpret $\dim O_k$ as the number of units of information that are "forgotten" at symbol time k, as may be seen explicitly in the controller canonical realization.[5]

[5] Alternatively, if we were to run the system in the reverse-time direction, then $\dim O_k$ and $\dim I_k$ would reverse roles and become the amounts of "new" and "forgotten" information, respectively.

V. Minimal realizations of multivariable LTI systems

We now consider minimal realizations of general Laurent LTI systems, which for brevity we simply call *multivariable LTI systems*. The material in this section is well known; our purpose is to let the reader see its connections with the "shortest basis" approach.

As usual, we make no distinction between $(\mathbb{F}((z^{-1})))^n$ and $\mathbb{F}^n((z^{-1}))$.

A multivariable LTI system is usually defined (as in Example 1) by an $n \times k$ rational *generator matrix* $G(z) = \{g_{ij}(z) : 1 \le i \le n, 1 \le j \le k\}$, where each element $g_{ij}(z)$ is a rational Laurent sequence. A Laurent sequence in $\mathbb{F}((z^{-1}))$ is *rational* if it can be expressed in the form $a(z)/b(z)$, where $a(z)$ and $b(z)$ are polynomial sequences in $\mathbb{F}[z^{-1}]$ with $b(z) \neq 0$. The set of all rational Laurent sequences is denoted by $\mathbb{F}(z^{-1})$, and forms a field; in particular, the multiplicative inverse of a nonzero rational sequence $a(z)/b(z)$ is $b(z)/a(z)$.

The system $\mathcal{C}$ is then the set of all n-tuples of Laurent sequences $\mathbf{y}(z) = G(z)\mathbf{u}(z)$ as $\mathbf{u}(z)$ ranges through all k-tuples of Laurent sequences:

$$\mathcal{C} = \{\mathbf{y}(z) = G(z)\mathbf{u}(z) : \mathbf{u}(z) \in (\mathbb{F}((z^{-1})))^k\}.$$

(Notice that the component sequences $y_i(z)$ of $\mathbf{y}(z)$ may represent either "inputs" or "outputs," as for example in Example 1.) It follows that such an LTI system $\mathcal{C}$ is a subspace of the n-dimensional vector space $(\mathbb{F}((z^{-1})))^n$ of all n-tuples of Laurent sequences over the Laurent field $\mathbb{F}((z^{-1}))$. Thus without loss of generality we may assume that $k \le n$, and that $G(z)$ has full rank k.

We now give an "algorithm" to find a shortest basis $\mathcal{B}$ for $\mathcal{C}$. The correctness of this approach is proved in [4], using the invariant factor theorem (IFT), and again in [6], without using the IFT. The "shortest basis" approach gives a nice motivation for this development.

We first find a set of k independent finite generators whose shifts generate $\mathcal{C}$, by finding the shortest finite trajectories in the k 1-dimensional subsystems $\mathcal{C}_j$ that are generated by the k rational generators $\mathbf{g}_j(z) = \{g_{ij}(z) = a_{ij}(z)/b_{ij}(z) : 1 \le i \le n\}$. We observe (as in Example 1) that $u_j(z)\mathbf{g}_j(z)$ is finite if and only if $u_j(z)$ is a finite multiple of $\lambda_j(z)/\gamma_j(z)$, where $\lambda_j(z)$ is the least common multiple of the denominators $b_{ij}(z)$, and $\gamma_j(z)$ is the greatest common divisor of the numerators $a_{ij}(z)$. The shortest finite trajectories in $\mathcal{C}_j$ are therefore the shifts of $\mathbf{g}'_j(z) = \lambda_j(z)\mathbf{g}_j(z)/\gamma_j(z)$. Since we may take any shift of $\mathbf{g}'_j(z)$, we may assume without loss of generality that the delay of $\mathbf{g}'_j(z)$ is zero. Then the polynomial matrix $G'(z) = \{\mathbf{g}'_j(z) : 1 \le j \le k\}$ is a basis for $\mathcal{C}$.

We note in passing that this construction shows that any LTI system $\mathcal{C}$ that is generated by a rational generator matrix $G(z)$ is controllable; *i.e.,* generated by its finite trajectories.

Now we ask whether there exists any finite linear combination $G'(z)\mathbf{u}(z)$ of the polynomial generators $\mathbf{g}'_j(z)$ that produces a finite sequence that is shorter than any generator involved in this combination. As we saw earlier, this can happen if and only if the set of shifts of the $\{\mathbf{g}'_j(z)\}$ does not have the predictable delay property or the predictable degree property.

1. The set of shifts of the $\{\mathbf{g}'_j(z)\}$ does not have the predictable delay property if and only if there exists a linear combination $\mathbf{g}''(z)$ of the delay-0 generators $\mathbf{g}'_j(z)$ that has delay greater than zero. This occurs if and only if the delay-0 coefficient n-tuples $\mathbf{g}'_{j,0}$ are linearly dependent over $\mathbb{F}$, which occurs if and only if the $k \times k$ minors (determinants of $k \times k$ submatrices) of the $n \times k$ matrix $G'(z)$ all have delay greater than zero. In this case we can obtain a shorter set of generators by substituting the linear combination $\mathbf{g}''(z)$ for a longest generator $\mathbf{g}'_j(z)$ that is involved in the combination.

2. The set of shifts of the $\{\mathbf{g}'_j(z)\}$ does not have the predictable degree property if and only if there exists a linear combination $\mathbf{g}''(z)$ of the degree-0 shifts $D^{-\deg \mathbf{g}'_j(z)}\mathbf{g}'_j(z)$ of the generators $\mathbf{g}'_j(z)$ that has degree less than zero. This occurs if and only if the high-order coefficient n-tuples $\mathbf{g}'_{j,\deg \mathbf{g}'_j}$ are linearly dependent over $\mathbb{F}$, which occurs if and only if the $k \times k$ minors of $G'(z)$ all have degree less than their expected degree $\mu = \sum_{j=1}^{k} \deg \mathbf{g}'_j(z)$. In this case we can obtain a shorter set of generators by substituting the delay-0 shift of the linear combination $\mathbf{g}''(z)$ for a longest generator $\mathbf{g}'_j(z)$ that is involved in the combination.

Finally, we ask whether the set of shifts of the $\{\mathbf{g}'_j(z)\}$ is catastrophic— *i.e.,* whether there exists any infinite linear combination $\mathbf{y}(z) = G'(z)\mathbf{u}(z)$ of the polynomial generators $\mathbf{g}'_j(z)$ that produces a finite sequence $\mathbf{y}(z)$. As shown in [4, 6], this occurs if and only if there is some polynomial $p(z) \in \mathbb{F}[z^{-1}]$ other than z^{-1} and some finite k-tuple $\mathbf{u}(z)$ such that $\mathbf{g}''(z) = \mathbf{y}(z)/p(z) = G'(z)(\mathbf{u}(z)/p(z))$ is finite, whereas $\mathbf{u}(z)/p(z)$ is infinite. This occurs if and only if the matrix $G'(z) \bmod p(z)$ has less than full rank, which occurs if and only if the $k \times k$ minors of $G'(z)$ are all divisible by $p(z)$. Then we can obtain a shorter set of generators by substituting the delay-0 shift of the linear combination $\mathbf{g}''(z)$ for a longest generator $\mathbf{g}'_j(z)$ that is involved in the combination.

To detect this situation, we can in principle compute the $k \times k$ minors of $G'(z)$, and see whether they have any common factor $p(z)$. It turns out that $p(z)$ is an invariant factor of $G'(z)$ [4], so any efficient algorithm for finding invariant factors of polynomial matrices may be used to find $p(z)$. Then there exists some linear combination of the generators $\mathbf{g}'_j(z)$ that equals zero modulo $p(z)$; *i.e.,* is divisible by $p(z)$. Dividing this combination by $p(z)$, we obtain our shorter generator $\mathbf{g}''(z)$.

Example 3. Consider the multivariable LTI system $\mathcal{C}$ over any field $\mathbb{F}$ generated by the 3×2 matrix

$$G(z) = \begin{bmatrix} 1 & 1 - \alpha z^{-1} \\ 1 - \beta z^{-1} & 1 \\ 1 - \gamma z^{-1} & 1 - \delta z^{-1} \end{bmatrix},$$

The 2×2 minors of $G(z)$ are $(\alpha+\beta)z^{-1} - \alpha\beta z^{-2}$, $(\alpha+\gamma-\delta)z^{-1} - \alpha\gamma z^{-2}$, and $(\gamma-\beta-\delta)z^{-1} + \beta\delta z^{-2}$. Since all have delay greater than zero (or, alternatively, since all have a common divisor $p(z) = z^{-1}$), the set of shifts of $\mathbf{g}_1(z) = (1, 1-\beta z^{-1}, 1-\gamma z^{-1})$ and $\mathbf{g}_2(z) = (1-\alpha z^{-1}, 1, 1-\delta z^{-1})$ does not have the predictable delay property. Indeed, the linear combination $\mathbf{g}_1(z) - \mathbf{g}_2(z) = (\alpha z^{-1}, -\beta z^{-1}, (\delta-\gamma)z^{-1})$ has delay 1 and length 1, and its delay-0 shift $(\alpha, -\beta, (\delta-\gamma))$ (obtained by dividing out the common divisor $p(z) = z^{-1}$) may replace of $\mathbf{g}_1(z)$ or $\mathbf{g}_2(z)$ as a shorter fundamental generator. □

As this development suggests, the predictable delay, predictable degree, and non-catastrophic properties may be seen as special cases of the "no common divisor" property, for the cases of $p(z) = z^{-1}$, $p(z) = z$, and all other polynomials, respectively; see the appendix of [6].

When the ground field $\mathbb{F}$ is the complex field $\mathbb{C}$, then the minors of $G'(z)$ have no common divisor $p(z) \in \mathbb{C}[z^{-1}]$ if and only if they have no common degree-1 divisor $z^{-1} - \alpha$ for any $\alpha \in \mathbb{C}$. As Example 3 illustrates, the case $\alpha = 0$ corresponds to a test of the predictable delay property; by interchanging z and z^{-1} we can see that the case $\alpha = \infty$ ($\alpha^{-1} = 0$) corresponds to a test of the predictable degree property. Since $G'(z) \bmod z^{-1} - \alpha$ is the complex matrix obtained by "evaluating" $G'(z)$ at $z^{-1} = \alpha$, this ultimately implies that $G'(z)$ is a set of shortest fundamental generators for $\mathcal{C}$ if and only if $G'(z)$ has full rank when evaluated at $z^{-1} = \alpha$ for all $\alpha \in \mathbb{C} \cup \infty$. In system theory, this property is sometimes expressed in terms like the following: "The matrix $G'(z)$ has no zeroes anywhere in the complex plane, including at zero and at infinity."

VI. Duality

An alternative way of defining a linear system $\mathcal{C}$ is via a set of generators for its orthogonal system $\mathcal{C}^\perp$. In linear system theory, such a representation of $\mathcal{C}$ is sometimes called a *kernel representation*, whereas a representation in terms of generators for $\mathcal{C}$ is called an *image representation*.

If $\mathcal{B}^\perp$ is a shortest basis for $\mathcal{C}^\perp$, then $\mathcal{C}$ is the set of all trajectories that are orthogonal to all trajectories in $\mathcal{B}^\perp$. A fundamental duality result is that any minimal state space for $\mathcal{C}^\perp$ has the same dimension as the corresponding minimal state space for $\mathcal{C}$. These results lead to a minimal realization for $\mathcal{C}$ in "observer canonical form" [11]. We also determine the dimensions of the minimal transition spaces of $\mathcal{C}^\perp$.

A. Orthogonal systems

Each symbol alphabet A_k is a finite-dimensional vector space over $\mathbb{F}$, and therefore has a dual space $\hat{A}_k$ of the same dimension such that for all $a_k \in A_k, \hat{a}_k \in \hat{A}_k$ there is a well-defined inner product $\langle a_k, \hat{a}_k \rangle \in \mathbb{F}$. Commonly A_k is the set $\mathbb{F}^n$ of n-tuples over $\mathbb{F}$; then $\hat{A}_k$ may also be taken as $\mathbb{F}^n$, with the inner product being defined in standard componentwise fashion.

If $\mathcal{A} = \prod_{k \in \mathcal{I}} A_k$ is the set of all Laurent trajectories, then its dual space $\hat{\mathcal{A}} = \prod_{k \in \mathcal{I}} \hat{A}_k$ is the set of all anti-Laurent trajectories (*i.e.,* all nonzero trajectories with finite degree, plus $\mathbf{0}$). The inner product between a trajectory $\mathbf{a} \in \mathcal{A}$ and a dual trajectory $\hat{\mathbf{a}} \in \hat{\mathcal{A}}$ may then be defined by $\langle \mathbf{a}, \hat{\mathbf{a}} \rangle = \sum_{k \in \mathcal{I}} \langle a_k, \hat{a}_k \rangle$; this sum is well defined if $\mathbf{a}$ is Laurent and $\hat{\mathbf{a}}$ is anti-Laurent, because then only a finite number of terms in the sum are nonzero.

The *orthogonal system* $\mathcal{C}^\perp$ is then defined as set of all trajectories $\hat{\mathbf{a}} \in \hat{\mathcal{A}}$ whose inner product with all trajectories $\mathbf{a} \in \mathcal{C}$ is zero. $\mathcal{C}^\perp$ is linear, and its orthogonal system $\mathcal{C}^{\perp\perp}$ is $\mathcal{C}$. Therefore $\mathcal{C}$ may be characterized as the set of all $\mathbf{a} \in \mathcal{A}$ that are orthogonal to a basis $\mathcal{B}^\perp$ for $\mathcal{C}^\perp$.

Example 2 (cont.). The orthogonal code $\mathcal{C}^\perp$ to the code $\mathcal{C}$ of Example 2 is $\mathcal{C}$ itself. Thus an 8-tuple $\mathbf{a} \in (\mathbb{F}_2)^8$ is in $\mathcal{C}$ if and only if it is orthogonal to the four generators $\mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3, \mathbf{g}_4$. □

If a linear system $\mathcal{C}$ is Laurent complete (the Laurent completion of its finite subcode), then $\mathcal{C}^\perp$ is anti-Laurent complete, so there is a nice symmetry between a system and its orthogonal system.[6]

An LTI system $\mathcal{C}$ over a field $\mathbb{F}$ is invariant both under multiplication by elements of $\mathbb{F}$ and under time shifts, and therefore is invariant under multiplication by Laurent sequences in $\mathbb{F}((D))$ or $\mathbb{F}((z^{-1}))$, where multiplication of Laurent trajectories by Laurent sequences is defined by sequence convolution. Thus we usually prefer to regard an LTI system as a linear system over $\mathbb{F}((D))$ or $\mathbb{F}((z^{-1}))$. In this case the orthogonal code $\mathcal{C}^\perp$ is defined by an inner product in $\mathbb{F}((D))$ or $\mathbb{F}((z^{-1}))$, and is also linear over $\mathbb{F}((D))$ or $\mathbb{F}((z^{-1}))$. It is easy to see that the orthogonal code $\mathcal{C}^\perp$ so defined is the time reversal of the orthogonal code according to the earlier definition using an inner product over $\mathbb{F}$. Thus we use slightly different definitions of orthogonality for LTI and for non-LTI systems.[7]

Example 1 (cont.). The linear time-invariant system $\mathcal{C}$ of Example 1 may be regarded as the one-dimensional subspace of the two-dimensional vector space $(\mathbb{F}((z^{-1})))^2$ that is generated by $(1, g(z))$. The orthogonal code $\mathcal{C}^\perp$ is then the orthogonal one-dimensional subspace, which is generated by $(g(z), -1)$. In other words, a pair $(u(z), y(z))$ is in $\mathcal{C}$ if and only if $u(z)g(z) - y(z) = 0$. □

[6] This symmetry can be improved by reversing the time axis of the orthogonal code.

[7] As noted in the previous footnote, it would be better conceptually if we always reversed the time axis of the orthogonal system $\mathcal{C}^\perp$, but in the general case the notation then becomes cumbersome.

B. Dual minimal state and transition spaces

It is well known that the minimal state spaces $\hat{\Sigma}_k$ of the orthogonal system $\mathcal{C}^\perp$ have the same dimensions as the corresponding minimal state spaces Σ_k of $\mathcal{C}$. This follows from:

- The fact that Σ_k is isomorphic to the past-induced state space $P_{k^-}(\mathcal{C})/\mathcal{C}_{k^-}$, or equivalently to the quotient space $R_{k^-}(\mathcal{C})/R_{k^-}(\mathcal{C}_{k^-})$, where the restriction R_{k^-} maps a trajectory $\mathbf{a} = \{a_{k'} : k' \in \mathcal{I}\}$ defined on $\mathcal{I}$ to a restricted trajectory $R_{k^-}(\mathbf{a}) = \{a_{k'}, : k' \in k^-\}$ defined on k^-.

- The fact that restricted systems and subsystems are duals, in the sense that $R_{k^-}(\mathcal{C}^\perp) = (R_{k^-}(\mathcal{C}_{k^-}))^\perp$ and $R_{k^-}((\mathcal{C}^\perp)_{k^-}) = (R_{k^-}(\mathcal{C}))^\perp$. This follows from the fact that $(R_{k^-}(\mathbf{a}), R_{k^+}(\mathbf{a}))$ is orthogonal to $(R_{k^-}(\mathbf{b}), R_{k^+}(\mathbf{0}))$ if and only if $R_{k^-}(\mathbf{a})$ is orthogonal to $R_{k^-}(\mathbf{b})$.

- The fact that if B is a subspace of A, then $A^\perp$ is a subspace of $B^\perp$, and the quotient spaces A/B and $B^\perp/A^\perp$ are dual spaces, with the same dimension. Consequently $R_{k^-}(\mathcal{C})/R_{k^-}(\mathcal{C}_{k^-}) \simeq \Sigma_k$ and $R_{k^-}(\mathcal{C}^\perp)/R_{k^-}((\mathcal{C}^\perp)_{k^-}) \simeq \hat{\Sigma}_k$ are dual spaces, and $\dim \Sigma_k = \dim \hat{\Sigma}_k$.

Is there a corresponding duality result for minimal transition spaces? A little-known fact, apparently first discovered by Mittelholzer [13], and proved in a more general context in [9], is that whereas Σ_k and $\hat{\Sigma}_k$ are dual spaces, if $\mathcal{T}_k \subseteq \Sigma_k \times A_k \times \Sigma_{k+1}$ is a minimal transition space of $\mathcal{C}$, then the corresponding minimal transition space of $\mathcal{C}^\perp$ is the orthogonal space $(\mathcal{T}_k)^\perp$ to $\mathcal{T}_k$ in the dual space $\hat{\Sigma}_k \times \hat{A}_k \times \hat{\Sigma}_{k+1}$, where orthogonality is defined with respect to the following bilinear form:

$$\langle (\sigma_k, a_k, \sigma_{k+1}), (\hat{\sigma}_k, \hat{a}_k, \hat{\sigma}_{k+1}) \rangle = \langle \sigma_k, \hat{\sigma}_k \rangle + \langle a_k, \hat{a}_k \rangle - \langle \sigma_{k+1}, \hat{\sigma}_{k+1} \rangle.$$

Thus the dimensions of the minimal transition spaces of $\mathcal{C}$ and $\mathcal{C}^\perp$ are in general related as follows:

$$\dim \mathcal{T}_k + \dim (\mathcal{T}_k)^\perp = \dim \Sigma_k + \dim A_k + \dim \Sigma_{k+1}.$$

The in-space of $\mathcal{C}^\perp$ at time k is in some sense the dual to the out-space of $\mathcal{C}$ at time k, and *vice versa*, as can be seen from the following relations. Since $\dim \Sigma_k = \dim \hat{\Sigma}_k$ and $\dim \mathcal{T}_k = \dim \Sigma_k + \dim I_k = \dim \Sigma_{k+1} + \dim O_k$, we have

$$\dim (\mathcal{T}_k)^\perp = \dim \hat{\Sigma}_k + \dim A_k - \dim O_k = \dim \hat{\Sigma}_{k+1} + \dim A_k - \dim I_k.$$

Thus if $\hat{I}_k$ and $\hat{O}_k$ are the in-space and out-space of $\mathcal{C}^\perp$ at symbol time k, then

$$\begin{aligned} \dim \hat{I}_k &= \dim A_k - \dim O_k; \\ \dim \hat{O}_k &= \dim A_k - \dim I_k. \end{aligned}$$

In particular, when symbols are simply elements of $\mathbb{F}$ so that $\dim A_k = 1$, then $\dim \hat{O}_k = 0$ if $\dim I_k = 1$ and *vice versa*.

Example 1 (cont.). Let $\mathcal{C}$ be any single-input, single-output linear time-invariant system, whose shortest basis is the set of all shifts of the fundamental input-output trajectory $(b(z), a(z))$, whose delay is 0 and whose degree is $\delta = \max\{\deg b(z), \deg a(z)\}$. Then a shortest basis for the orthogonal system $\mathcal{C}^\perp$ is the set of all shifts of the fundamental input-output trajectory $(a(z), -b(z))$. Thus the minimal state spaces of $\mathcal{C}$ and $\mathcal{C}^\perp$ both have dimension δ, and the minimal transition spaces of $\mathcal{C}$ and $\mathcal{C}^\perp$ both have dimension $\delta + 1$. Also, all in-spaces and out-spaces have dimension 1. Since $\dim A_k = 2$, it is easy to check all that the relations above are satisfied. □

Example 2 (cont.). The binary code $\mathcal{C}$ of Example 2 is generated by the shortest basis $\{11110000, 00111100, 00001111, 01011010\}$, and has state-space dimension profile $\{0,1,2,3,2,3,2,1,0\}$ and transition-space dimension profile $\{1,2,3,3,3,3,2,1\}$. The orthogonal code $\mathcal{C}^\perp$ is the same code, and thus has the same profiles. One may check that the relations above are satisfied at all times; for example, at symbol time 0, $\dim I_0 = \dim \hat{I}_0 = 1, \dim O_0 = \dim \hat{O}_0 = 0$ and $\dim \mathcal{T}_0 = \dim(\mathcal{T}_0)^\perp = 1$. Note that since $\dim A_k = 1$ and $\mathcal{C} = \mathcal{C}^\perp$, we must have $\dim O_k = 0$ if $\dim I_k = 1$, and *vice versa*; thus $\dim I_k = 1$ for $k = 0,1,2,4$, while $\dim O_k = 1$ for $k = 3,5,6,7$. □

Example 3 (cont.). The system $\mathcal{C}$ of Example 3 is a two-dimensional subspace of $(\mathbb{F}((z^{-1})))^3$, and has a shortest basis consisting of the shifts of the two delay-0 generators $\mathbf{g}'_1(z) = (\alpha, -\beta, (\delta-\gamma))$ and $\mathbf{g}_2(z) = (1-\alpha z^{-1}, 1, 1-\delta z^{-1})$, which have degrees 0 and 1, respectively. Thus the minimal state spaces of $\mathcal{C}$ have dimension 1, and its minimal transition spaces have dimension 3. The orthogonal system $\mathcal{C}^\perp$ must thus be a one-dimensional subspace of $(\mathbb{F}((z^{-1})))^3$, and must be generated by the shifts of a delay-0, degree-1 generator $\mathbf{h}(z)$. Thus its minimal state spaces have dimension 1, and its minimal transition spaces have dimension 2. □

More generally, as we have seen, a multivariable LTI system $\mathcal{C}$ has a polynomial $n \times k$ generator matrix $G'(z) = \{\mathbf{g}'_j(z) : 1 \le j \le k\}$, whose $k \times k$ minors have no common polynomial factors, and have maximum degree $\mu = \sum_{j=1}^k \deg \mathbf{g}'_j(z)$; then the shifts of the fundamental generators $\mathbf{g}'_j(z)$ form a shortest basis for $\mathcal{C}$. It turns out that the orthogonal LTI system $\mathcal{C}^\perp$ has a polynomial $n \times (n-k)$ generator matrix $H(z) = \{\mathbf{h}_j(z) : 1 \le j \le n-k\}$ whose $(n-k) \times (n-k)$ minors are the same (up to sign) as the complementary $k \times k$ minors of $G'(z)$ [5], such that the shifts of the fundamental generators $\mathbf{h}_j(z)$ form a shortest basis for $\mathcal{C}^\perp$. Since the in-spaces and out-spaces of $\mathcal{C}$ have dimension k, and those of $\mathcal{C}^\perp$ have dimension $n-k$, it follows that the dimensions of the minimal state spaces of $\mathcal{C}$ and $\mathcal{C}^\perp$ are both equal to μ, that the dimensions of the minimal transition spaces of $\mathcal{C}$ are $\mu + k$, and that the dimensions of the minimal transition spaces of $\mathcal{C}^\perp$ are $\mu + n - k$.

Example 3 (cont.). For the system $\mathcal{C}$ of Example 3, the 2×2 minors of $G'(z)$ are $\alpha + \beta - \alpha\beta z^{-1}$, $\alpha + \gamma - \delta - \alpha\gamma z^{-1}$, and $\gamma - \beta - \delta + \beta\delta z^{-1}$. It follows that these are also the 1×1 minors of the generator matrix $H(z)$ of $\mathcal{C}^\perp$, up to sign; indeed, the fundamental generator of $H(z)$ is $\mathbf{h}(z) = (\gamma - \beta - \delta + \beta\delta z^{-1}, -\alpha - \gamma + \delta + \alpha\gamma z^{-1}, \alpha + \beta - \alpha\beta z^{-1})$. □

C. Minimal realizations in observer canonical form

Given a shortest basis $\mathcal{B}^\perp$ for the orthogonal system $\mathcal{C}^\perp$ to a linear system $\mathcal{C}$, we can give a straightforward state-space realization for $\mathcal{C}$, sometimes called the *observer canonical form* [11], whose state-space dimensions are minimal at all times. Indeed, this realization may be obtained by dualizing the controller canonical form realization of $\mathcal{C}^\perp$.

With each generator $\mathbf{h} \in \mathcal{B}^\perp$, we associate a one-dimensional atomic "checker" as follows. Roughly, for an arbitrary trajectory $\mathbf{a} \in \mathcal{A}$, the realization accumulates the partial sums of the inner product $\langle \mathbf{a}, \mathbf{h} \rangle = \sum_{k \in [\mathrm{del}\ \mathbf{h}, \deg \mathbf{h}]} \langle a_k, h_k \rangle$ in an "accumulator." The trajectory "checks" (is valid) with respect to $\mathbf{h}$ if the final sum in the accumulator is 0.

More precisely, if del $\mathbf{h} < \deg \mathbf{h}$, then the state spaces of the atomic checker are equal to $\mathbb{F}$ during the active state interval $(\mathrm{del}\ \mathbf{h}, \deg \mathbf{h}]$, and equal to the trivial space $\{0\}$ otherwise;[8] thus the state space dimension is 1 during the active interval and 0 otherwise. The sets of allowable transitions

[8] If del $\mathbf{h} = \deg \mathbf{h}$, then $\hat{\Sigma}_k = \{0\}$ for all $k \in \mathcal{I}_S$, and $\mathcal{T}_k = \{(0, a_k, 0) : \langle a_k, h_k \rangle = 0\}$ at symbol time $k = \mathrm{del}\ \mathbf{h} = \deg \mathbf{h}$; otherwise $\mathcal{T}_k = \{(0,0,0)\}$.

$\mathcal{T}_k$ are as given below during the active symbol interval $[\mathrm{del}\,\mathbf{h}, \deg \mathbf{h}]$ (otherwise $\mathcal{T}_k = \{(0,0,0)\}$):

- For $k = \mathrm{del}\,\mathbf{h}$, $\mathcal{T}_k = \{(0, a_k, \sigma_{k+1} = \langle a_k, h_k \rangle) : a_k \in A_k\}$;
- For $\mathrm{del}\,\mathbf{h} < k < \deg \mathbf{h}$, $\mathcal{T}_k = \{(\sigma_k, a_k, \sigma_{k+1} = \sigma_k + \langle a_k, h_k \rangle) : a_k \in A_k\}$;
- For $k = \deg \mathbf{h}$, $\mathcal{T}_k = \{(-\langle a_k, h_k \rangle, a_k, 0) : a_k \in A_k\}$.

(It is easily checked that these are the orthogonal transition spaces under the bilinear form given above to those defined in Section IV-D for the controller canonical form, if $\mathbf{h}$ is substituted for $\mathbf{g}$.) Evidently $\sigma_k = \sum_{k'<k} \langle a_{k'}, h_{k'} \rangle$ for $k \le \deg \mathbf{h}$, and a trajectory $\mathbf{a} \in \mathcal{A}$ has a corresponding state sequence $\boldsymbol{\sigma}(\mathbf{a})$ such that $(\mathbf{a}, \boldsymbol{\sigma}(\mathbf{a}))$ is a valid symbol-state trajectory if and only if

$$\sigma_{\deg \mathbf{h}} = \sum_{k \in [\mathrm{del}\ \mathbf{h}, \deg \mathbf{h})} \langle a_k, h_k \rangle = -\langle a_{\deg \mathbf{h}}, h_{\deg \mathbf{h}} \rangle;$$

i.e., if and only if $\langle \mathbf{a}, \mathbf{h} \rangle = 0$.

The whole realization for $\mathcal{C}$ then consists of the aggregate of these atomic "checkers" for all $\mathbf{h} \in \mathcal{B}^\perp$. The set of all $\mathbf{a} \in \mathcal{A}$ that have a compatible state sequence $\boldsymbol{\sigma}(\mathbf{a})$ in all "checkers" is the set of all $\mathbf{a} \in \mathcal{A}$ that are orthogonal to all $\mathbf{h} \in \mathcal{B}^\perp$, which is precisely the linear system $\mathcal{C}$. The number of memory elements active at any state time $k \in \mathcal{I}_S$ is the number of active $\mathbf{h} \in \mathcal{B}^\perp$ at time k, which is the dimension of the minimal state space $\hat{\Sigma}_k$ for $\mathcal{C}^\perp$, which equals $\dim \Sigma_k$. Thus this aggregate "observer canonical form" realization is a minimal (and linear) realization of $\mathcal{C}$.

In an observer canonical realization of a linear time-invariant system, the lengths of the dual generators $\mathbf{h} \in \mathcal{B}^\perp$ are sometimes called the *observability indices* of $\mathcal{C}$. Thus the observability indices of $\mathcal{C}$ are the controllability indices of $\mathcal{C}^\perp$, and *vice versa.*

VII. Conclusion

The "shortest basis" approach describes a linear system $\mathcal{C}$ by a shortest basis $\mathcal{B}$ that transparently characterizes the controllability properties of $\mathcal{C}$, or by a shortest basis $\mathcal{B}^\perp$ for $\mathcal{C}^\perp$ that similarly characterizes the observability properties of $\mathcal{C}$. In particular, $\mathcal{B}$ and $\mathcal{B}^\perp$ lead directly to minimal linear realizations of $\mathcal{C}$ in controller and observer canonical form, respectively.

In this paper, we have not carried this approach through to the development of actual algorithms for computing minimal realizations, given a description of a linear system $\mathcal{C}$. When the time axis $\mathcal{I}$ is finite, then there exist straightforward algorithms for reducing a given basis $\mathcal{B}$ to a shortest basis by detecting and correcting any failure of $\mathcal{B}$ to have the predictable span property; see [14]. When the time axis is infinite, we need also to detect and correct catastrophicity. For LTI systems, this is essentially a matter of finding and eliminating invariant polynomial factors, as discussed in Section V. For linear time-varying systems, detecting catastrophicity is in general an open question, depending on how the system is described.

As shown in [8], this approach generalizes naturally to discrete-time group systems. As shown in [9], it further generalizes to linear and group systems defined on cycle-free graphs, rather than on a standard discrete time axis, and to some extent to general graphs. Such generality suggests that the "shortest basis" approach is rather fundamental.

Acknowledgments

I have benefitted greatly from interactions with many colleagues over the very many years during which I have been interested in these topics, including particularly F. Fagnani, R. Johannesson, T. Kailath, R. Koetter, F. R. Kschischang, H.-A. Loeliger, J. L. Massey, T. Mittelholzer, S. Mitter, J. Rosenthal, M. D. Trott, A. Vardy, J. C. Willems, and S. Zampieri.

For comments on earlier versions of this paper, I am grateful to H. Gluesing-Luerssen, F. R. Kschischang, M. Kuijper, and the reviewers.

Appendix. The shortest basis approach for complete systems

In this Appendix, we relax the restriction that trajectories $\mathbf{a} \in \mathcal{A} = \prod_{k \in \mathcal{I}} A_k$ must be Laurent. This allows us to consider uncontrollable systems $\mathcal{C} \subset \mathcal{A}$, which in general will have autonomous components. The theory is a straightforward extension of the approach developed for controllable systems in the main body of the paper, but now a shortest basis $\mathcal{B}$ may include infinite generators. However, we will see that the duality theory becomes less symmetrical, since the dual space $\hat{\mathcal{A}}$ now consists of only the finite trajectories in $\prod_{k \in \mathcal{I}} \hat{A}_k$.

We correspondingly relax the restriction that linear combinations must be Laurent. Thus, if $\mathcal{B}$ is a basis for $\mathcal{C}$, then $\mathcal{C}$ is the set of *all* linear combinations of generators in $\mathcal{B}$. This implies that $\mathcal{C}$ is "complete," not just "Laurent complete."

We continue to define a system $\mathcal{C}$ as *controllable* if it is generated by its finite trajectories, where "generated" is now understood in the sense of unrestricted linear combinations. A complete LTI system need not be controllable, as is shown by the following simple example.

Example A (repetition system). Over any field $\mathbb{F}$, the repetition system $\mathcal{C}$ is defined as the set of all bi-infinite trajectories $\mathbf{a} \in \mathbb{F}^{\mathbb{Z}}$ such that $a_k = \alpha$ for all $k \in \mathbb{Z}$, for some $\alpha \in \mathbb{F}$. $\mathcal{C}$ is evidently a linear time-invariant system, and indeed a one-dimensional subspace of $\mathbb{F}^{\mathbb{Z}}$ that is generated by the bi-infinite all-one trajectory $\mathbf{1} \in \mathbb{F}^{\mathbb{Z}}$. Since the only finite trajectory in $\mathcal{C}$ is the all-zero trajectory $\mathbf{0}$, $\mathcal{C}$ is uncontrollable. □

The controllable subsystem of a linear system $\mathcal{C}$ is defined as the subsystem $\mathcal{C}^c$ generated by all finite trajectories of $\mathcal{C}$. The uncontrollable component of $\mathcal{C}$ may be defined abstractly as the quotient space $\mathcal{C}/\mathcal{C}^c$.

As is well known, the minimal state space theorem continues to hold for uncontrollable systems, and it is easy to see that the minimal transition space theorem does also. Furthermore, Theorems 4 and 5 continue to hold; *i.e.,* the minimal state space (resp. transition space) dimension at state (resp. symbol) time k is the number of active generators at time k. Thus if we continue to require that minimal state spaces be finite-dimensional, then the dimension of $\mathcal{C}^u$ must be finite. Thus $\mathcal{C}^u$ must have a basis $\mathcal{B}^u$ consisting of a finite set of infinite trajectories in $\mathcal{C}$ (*e.g.,* the all-one trajectory $\mathbf{1}$ in Example A).

For the controllable subsystem $\mathcal{C}^c$, the "shortest basis" approach of the main body of the text goes through without significant change. In particular, we may still obtain a basis $\mathcal{B}^c$ for $\mathcal{C}^c$ by our greedy construction. This construction may be continued to construct a shortest basis $\mathcal{B}^u$ for $\mathcal{C}^u$ consisting of a finite set of infinite generators. Together, $\mathcal{B}^c$ and $\mathcal{B}^u$ form a shortest basis $\mathcal{B}$ for $\mathcal{C}$.

Minimal linear realizations in controller canonical form may be constructed as before, with the only difference being that some of the atomic generators may be active for an infinitely long time.

Example A (cont.). For a repetition system $\mathcal{C}$, the subsystems $\mathcal{C}_{k^-}$ and $\mathcal{C}_{k^+}$ are trivial at all times $k \in \mathbb{Z}$, so the minimal state space and transition space have dimension 1 at all times. Any nonzero trajectory in $\mathcal{C}$ may be taken as the single generator in a shortest basis $\mathcal{B}$; such a generator is active at all times. A minimal realization of $\mathcal{C}$ in controller canonical form is given by the one-dimensional atomic realization whose transition space is $\mathcal{T}_k = \{(\alpha, \alpha, \alpha) : \alpha \in \mathbb{F}\}$ at all times. □

It turns out that the dual space to the complete space $\prod_{k \in \mathcal{I}} A_k$ is the space $\hat{\mathcal{A}}$ consisting of the finite trajectories in $\prod_{k \in \mathcal{I}} \hat{A}_k$. This ensures that the inner product $\langle \mathbf{a}, \hat{\mathbf{a}} \rangle$ of a trajectory $\mathbf{a} \in \mathcal{A}$ and a trajectory $\hat{\mathbf{a}} \in \hat{\mathcal{A}}$ is well defined, since such an inner product is a sum of only finitely many nonzero terms $\langle a_k, \hat{a}_k \rangle$. Linear combinations in $\hat{A}$ are restricted to finite linear combinations.

Consequently, the orthogonal system $\mathcal{C}^\perp \subseteq \hat{\mathcal{A}}$ to a complete system $\mathcal{C} \subseteq \mathcal{A}$ is a finite system; *i.e.,* a system all of whose trajectories are finite. Such a system is necessarily controllable— *i.e.,* generated as the set of all finite linear combinations of its (finite) elements. Therefore the shortest basis approach of the main body of this paper applies directly to $\mathcal{C}^\perp$.

Example A (cont.). The orthogonal system $\mathcal{C}^\perp$ to a repetition system $\mathcal{C}$ is the set of all finite trajectories $\hat{\mathbf{a}} \in \mathbb{F}^{\mathbb{Z}}$ that are orthogonal to the all-one trajectory $\mathbf{1}$; *i.e.,* the set of all finite trajectories $\hat{\mathbf{a}} \in \mathbb{F}^{\mathbb{Z}}$ whose components sum to zero: $\sum_{k \in \mathcal{I}} \hat{a}_k = 0$. Note that $\mathcal{C}^\perp$ is also a time-invariant system.

Since a zero-sum trajectory cannot have length 1, the shortest nonzero trajectories in $\mathcal{C}^\perp$ have length 2 and are of the form $\alpha(D^k - D^{k+1})$ for some $\alpha \in \mathbb{F}$ and $k \in \mathbb{Z}$. The set of all shifts of the fundamental generator $1 - D$ generates $\mathcal{C}^\perp$, and is therefore a shortest basis $\mathcal{B}$ for $\mathcal{C}^\perp$. □

Our duality results for minimal state spaces and transition spaces of $\mathcal{C}^\perp$ continue to hold. From a shortest basis for $\mathcal{C}^\perp$, we can construct a minimal realization of $\mathcal{C}^\perp$ in controller canonical form, or a minimal realization of $\mathcal{C}$ in observer canonical form.

Example A (cont.). The elements $D^k - D^{k+1}$ of a shortest basis $\mathcal{B}$ for $\mathcal{C}^\perp$ all have length 2. One is active at each state time, and two are active at each symbol time. Therefore the minimal state space dimension is 1 at each time, the same as the minimal state space dimension for $\mathcal{C}$, and the minimal transition space dimension is 2, which equals

$$\dim \Sigma_k + \dim A_k + \dim \Sigma_{k+1} - \dim \mathcal{T}_k = 1 + 1 + 1 - 1.$$

The in-space and out-space dimensions of $\mathcal{C}$ are 0 at all times, and those of $\mathcal{C}^\perp$ are 1 at all times.

A minimal realization for $\mathcal{C}^\perp$ in controller canonical form may be constructed from an infinite set of one-dimensional atomic realizations, one for each $k \in \mathbb{Z}$, of which the kth produces an output sequence $\alpha(D^k - D^{k+1})$ and is active only at one state time, namely $k + 1$. Similarly, a minimal realization for $\mathcal{C}$ in observer canonical form may be constructed from an infinite set of one-dimensional atomic checkers, one for each $k \in \mathbb{Z}$, of which the kth checks that the inner product of $\mathbf{a}$ with $D^k - D^{k+1}$ is zero, and is active only at state time $k + 1$. □

In summary, the shortest basis approach applies equally well to complete systems.

References

[1] B. De Schutter, "Minimal state-space realization in linear system theory: An overview," *J. Comp. Appl. Math.*, vol. 121, pp. 331–354, Sept. 2000.

[2] A. Einstein, "On the method of theoretical physics," The Herbert Spencer Lecture, Oxford, England, June 10, 1933; republished in *Philosophy of Science*, vol. 1, pp. 163–169, April 1934.

[3] F. Fagnani, "Shifts on compact and discrete Lie groups: Algebraic-topological invariants and classification problems, *Adv. Math.*, vol. 127, pp. 283–306, 1997.

[4] G. D. Forney, Jr., "Convolutional codes I: Algebraic structure," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 720–738, Nov. 1970.

[5] G. D. Forney, Jr., "Structural analysis of convolutional codes via dual codes," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 512–518, July 1973.

[6] G. D. Forney, Jr., "Minimal bases of rational vector spaces, with applications to multivariable linear systems," *SIAM J. Control*, vol. 13, pp. 493–520, 1975.

[7] G. D. Forney, Jr., "Coset codes— Part II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152–1187, Sept. 1988.

[8] G. D. Forney, Jr. and M. D. Trott, "The dynamics of group codes: State spaces, trellis diagrams, and canonical encoders," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1491–1513, Sept. 1993.

[9] G. D. Forney, Jr., "Codes on graphs: Normal realizations," *IEEE Trans. Inform. Theory*, vol. 47, pp. 520–548, Feb. 2001.

[10] M. Hall, Jr., *The Theory of Groups*. New York: MacMillan, 1959.

[11] T. Kailath, *Linear Systems*. Englewood Cliffs, NJ: Prentice-Hall, 1980.

[12] F. R. Kschischang and V. Sorokine, "On the trellis structure of block codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1924–1937, Nov. 1995.

[13] T. Mittelholzer, "Convolutional codes over groups: A pragmatic approach," in *Proc. 33d Allerton Conf. Communication, Control and Computers*, Allerton, IL, Sept. 1995, pp. 380–381.

[14] A. Vardy, "Trellis structure of codes," in *Handbook of Coding Theory* (V. Pless and C. Huffman, eds.), pp. 1989–2118. New York: Elsevier, 1998.

[15] J. C. Willems, "From time series to linear systems, Parts I–III," *Automatica*, vol. 22, pp. 561–580 and 675–694, 1986; vol. 23, pp. 87–115, 1987.

[16] J. C. Willems, "Models for dynamics," *Dynamics Reported*, vol. 2, pp. 171–269, 1989.

Author biography

G. David Forney, Jr. received the B.S.E. degree in electrical engineering from Princeton University, Princeton, NJ, in 1961, and the M.S. and Sc.D. degrees in electrical engineering from the Massachusetts Institute of Technology, Cambridge, MA, in 1963 and 1965, respectively.

From 1965-99 he was with the Codex Corporation, which was acquired by Motorola, Inc. in 1977, and its successor, the Motorola Information Systems Group, Mansfield, MA. Since 1996, he has been an Adjunct Professor at M.I.T.

Dr. Forney was Editor of the IEEE Transactions on Information Theory from 1970 to 1973. He has been a member of the Board of Governors of the IEEE Information Theory Society during 1970-76, 1986-94, and 2004-10, and was President in 1992 and 2008. He has been awarded the 1970 IEEE Information Theory Group Prize Paper Award, the 1972 IEEE Browder J. Thompson Memorial Prize Paper Award, the 1990 and 2009 IEEE Donald G. Fink Prize Paper Awards, the 1992 IEEE Edison Medal, the 1995 IEEE Information Theory Society Claude E. Shannon Award, the 1996 Christopher Columbus International Communications Award, and the 1997 Marconi International Fellowship. In 1998 he received an IT Golden Jubilee Award for Technological Innovation, and two IT Golden Jubilee Paper Awards. He received an honorary doctorate from EPFL, Lausanne, Switzerland in 2007. He was elected a Fellow of the IEEE in 1973, a member of the National Academy of Engineering (U.S.A.) in 1983, a Fellow of the American Association for the Advancement of Science in 1993, an honorary member of the Popov Society (Russia) in 1994, a Fellow of the American Academy of Arts and Sciences in 1998, and a member of the National Academy of Sciences (U.S.A.) in 2003.