INFORMATION AND CONTROL 37, 23–33 (1978)

On Split Realizations of Response Maps over Rings

EDUARDO D. SONTAG*

Department of Mathematics, Rutgers University, New Brunswick, New Jersey 08903

This paper deals with observability properties of realizations of linear response maps defined over commutative rings. A characterization is given for those maps which admit realizations which are simultaneously reachable and observable in a strong sense. Applications are given to delay–differential systems.

INTRODUCTION

Observability is one of the central concepts of system theory (see Kalman, Arbib and Falb, 1969). We study here some aspects of observability in linear dynamical systems defined over commutative rings. For motivation and for a survey of results on systems over rings, the reader is referred to Sontag (1976); for an elementary mathematical introduction the reader is referred to Eilenberg (1974, Chapter XVI).

Let R denote a commutative ring.

Consider a linear system

$$\Sigma = \begin{cases} x(t+1) = Fx(t) + Gu(t), \\ y(t) = Hx(t), \qquad t = 0, 1, 2,..., \end{cases}$$

where $x(t)$ is in $X = R^n$ (n-vectors over R), $u(t)$ is an m-vector and $y(t)$ is a p-vector for $t = 0, 1, 2,...$, and where F, G, H are matrices of the appropriate sizes.

Intuitively, observability means the existence of a procedure for determining the state $x(0)$ of Σ from data obtained by experiments of the type: "apply an input sequence $u(0), u(1), u(2),...$ beginning in state $x(0)$ and observe the corresponding output sequence $y(0), y(1), y(2),...$". Since Σ is a linear system, the effect of nonzero inputs can be substracted from the output sequence. Thus we may restrict ourselves to those experiments in which $u(t) = 0$ for all $t \geqslant 0$.

* This research was supported in part by US Air Force Grant 72-2268 through the Center for Mathematical System Theory, University of Florida, Gainesville, Florida 32611.

0019-9958/78/0371–0023$02.00/0

Let $\mathbf{O}(x)$ denote the output sequence $Hx, HFx, HF^2x, \ldots$. Then for linear systems we have the following characterization of

(a) *Observability*: each state x in X can be uniquely determined from $\mathbf{O}(x)$.

This question was studied in Kalman (1968, Definition 10.1) for the case $R =$ field. In this case, (a) is equivalent to the possibility of determining x via linear data processing schemes. In other words, for each x' in X' (where X' denotes the set of *costates*, i.e., the dual of the state-space X) there exists an R-linear procedure $\gamma_{x'}$ (i.e., an R-linear map from the set of output sequences into R) such that for all states x in X,

$$x'(x) = \gamma_{x'}(\mathbf{O}(x)), \tag{*}$$

(see Kalman, 1969, Definition 10.2 and Theorem 10.10). Because of finite dimensionality, condition (*) can be also expressed as

(b) *R-linear observability*: for every x' in X', there exists $\gamma_{x'}$ in $(R^{np})'$ such that $x' = \gamma_{x'} \circ \mathbf{O}_n$.

[Here $\mathbf{O}_n : X \to R^{np}$ is given by

$$x \to \begin{bmatrix} Hx \\ HFx \\ \vdots \\ HF^{n-1}x \end{bmatrix}.]$$

The equivalence (a) $\Leftrightarrow$ (b) breaks down when R is an arbitrary ring. Consider for instance a system over $R := \mathbb{Z}$ with $n = p = 1, F = 0, G =$ arbitrary and $H := 2$. The system will be observable in the sense of (a), since the state x can be recovered from the knowledge of the corresponding output $y = 2x$. On the other hand, observability in the sense of (b) does not hold, because division by 2 cannot be performed when operating over $\mathbb{Z}$. Similar differences among (a) and (b) when $R =$ ring arise in continuous-time situations (for example, for delay-differential systems).

The case $R \neq$ field is further complicated by the fact that canonical realizations are not always *free*, (unless $R =$ principal ideal domain) i.e., the state space cannot be described by independent coordinate functions. We take the position that some notion of coordinate system is needed in order for the above problems to be manageable. Therefore, we shall only consider response maps for which the canonical state space admits (nonindependent) coordinates (projective modules).

Condition (b) is related to such important system-theoretic questions as the existence of observers with arbitrary dynamics and the problem of regulation. Accordingly, we propose to study in this paper *conditions under which the canonical realization of a given response map is observable in the (strong) sense of* (b).

For integral domains, this is achieved in Theorem (2.1), which gives a necessary and sufficient condition stated in elementary terms. For rings with zero-divisors, a similar condition is given in (3.1). The proofs rely heavily on known realization results on systems over rings together with some results from commutative algebra and an apparently new criterion for the projectivity of the column-module of a matrix.

The results of this paper have applications in the theory of regulation of delay-differential systems; we illustrate how this application comes about through an example, a more complete discussion having been already given by the author in Sontag (1976, Section 3.D). Consider a delay-differential system with equations

$$\begin{aligned} \dot{x}_1(t) &= 2x_1(t-1) + x_1(t) + x_2(t) + u(t), \\ \dot{x}_2(t) &= x_1(t-1) - 3x_2(t-5) + u(t-1), \\ y(t) &= x_1(t) - x_2(t-1). \end{aligned} \tag{a}$$

If we introduce the delay operator σ defined by

$$\sigma(x)(t) := x(t-1),$$

we can rewrite (a) in matrix form as

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 2\sigma + 1 & 1 \\ \sigma & -3\sigma^5 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} 1 \\ \sigma \end{bmatrix} u$$

$$y = [1 \; -\sigma] \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

We see then that (a) can be expressed in a form very similar to the ordinary finite-dimensional constant linear systems of control theory, the only difference being that the matrices (F, G, H) now have polynomial instead of real valued entries. When all the delays a_i, b_j, c_k in (*) are integral multiples of a fixed delay λ, we can apply the same procedure as above, taking now for σ a shift of λ seconds. If, instead, the delays in (*) are not commensurable, we need to define a finite set of delay operators $\sigma_1, \ldots, \sigma_r$ and then consider systems whose matrices have entries in the ring of polynomials in $\sigma_1, \ldots, \sigma_r$, denoted by $\mathbb{R}[\sigma_1, \ldots, \sigma_r]$.

A Luenberger observer, or deterministic Kalman filter, can be constructed for (*) formally as in the case of finite-dimensional linear systems, with arbitrary convergence rates, *precisely* when the system (*) (with R = polynomial ring) is observable in the sense of (b). Given a delay-differential system described in the input/output sense, the standard construction of a regulator (observer + state-feedback) is possible if and only if the canonical realization (in the ring-sense) is observable in the sense of (b). In the case of finite-dimensional systems such a property is always true; in the delay-differential case a most natural necessary and sufficient condition is given by (2.1) applied to R = polynomial ring. It is interesting to remark that the notions of *projective* and *free* module *coincide* in this case (Serre's conjecture/Quillen's theorem), so the notion of a "split realization" is very strong here; the application of (2.1) to delay-differential systems results then in a result of high intuitive significance whose proof depends on rather sophisticated algebra.

1. Definitions and Notational Conventions

We shall assume throughout this paper that R is a (commutative) *Noetherian* ring, i.e., every ideal of R is finitely generated. For commutative rings this is a very weak restriction and it simplifies the exposition considerably.

We shall use the notation:

$R^n :=$ free R-module in n generators, i.e., the set of (column) n-vectors;

$R^{n\times m} :=$ set of $n \times m$ matrices with entries in R;

$\otimes :=$ tensor product of R-modules;

$\Omega :=$ the set of maximal ideals of R;

$\pi_M :=$ the canonical map $R \to R/M$, for any $M \in \Omega$.

If C is in $R^{n\times m}$, then $I_k(C) :=$ ideal generated by the set of all $k \times k$ minors of C. If α: $R \to S$ is a ring homomorphism, then $\alpha C := (\alpha c_{ij}) \in S^{n\times m}$.

We shall identify an R-linear map $R^n \to R^m$ with its matrix when the standard bases are used for R^n and R^m.

(1.1) Definition. Let M be an R-module. The *dual* M' of M is the R-module consisting of all R-linear maps from M into R (with the pointwise operations). For an R-module homomorphism f: $M \to N$ the *transpose* f': $N' \to M'$ is the R-linear map given by $f'(u) := u \circ f$ for all u: $N \to R$.

We shall work with the following definition of a projective module (see Bourbaki, Algèbre, II.2.2, Proposition 12; Algèbre Commutative, II.5.3, Theorem 2]):

(1.2) Definition. P is a (finitely generated) *projective* R-module iff there exist elements $v_1, \ldots, v_n$ in P and linear forms $v_1', \ldots, v_n'$ in P' such that for every v in P,

$$v = \sum_{i=1}^{n} v_i'(v) \cdot v_i .$$

P has *rank* s iff, for every M in Ω, the vector spaces $P \otimes (R/M)$ have equal dimension s. (Otherwise the rank is not defined.)

If R is an integral domain with quotient field Q, the rank of P is *always* defined; it is equal to the Q-dimension of $P \otimes Q$. See Bourbaki (Algèbre, II.2.3) for a discussion of these questions. When R is a polynomial ring, projective = free; see Quillen (1976).

(1.3) *Remark.* Let P be as in (1.2), and suppose that $f: P \to N$ is an R-homomorphism for which f' is surjective. Then f *splits*, i.e. there exists g: $N \to P$ such that $g \circ f =$ identity on P. Indeed, since f' is onto there exist $u_i : N \to R$, $i = 1,..., n$, such that $u_i \circ f = v_i'$. It is then enough to define

$$g(x) := \sum_{i=1}^{n} u_i(x) \cdot v_i$$

for all x in N.

(1.4) Definitions. An *(m, p)-response map* f over R is a sequence $(A_1, A_2, ...)$ of matrices in $R^{p\times m}$. An (m, p)-system $\Sigma = (X, F, G, H)$ over R is given by a finitely generated R-module X and R-module homomorphisms F: $X \to X$, G: $R^m \to X$, H: $X \to R^p$. (If clear from the context, X is not explicitly displayed.) Σ is projective [free,...] when X is *projective* [*free*,...]; Σ has rank n if X is projective of rank n. Given a response map f, a system Σ is a *realization* of f provided that $A_i = HF^{i-1}G$ for all i. The map f is *realizable* if there exists at least one realization of f. The *rank* of f is the smallest integer among the ranks of projective systems realizing f. Finally, the *dual* of Σ is the (p, m)-system $\Sigma' = (X', F', H', G')$. ∎

For background concerning these definitions, consult Kalman, Falb, and Arbib (1969), Eilenberg (1974, Chapter XVI) or Sontag (1976). The terminology "input/output map" is sometimes used instead of our "response map."

Given $f = (A_1, A_2, ...)$, let us define the block matrix

$$\mathbf{H}_n = \mathbf{H}_n(f) := \begin{bmatrix} A_1 & \cdots & A_n \\ \vdots & & \vdots \\ A_1 & \cdots & A_{2n-1} \end{bmatrix}. \tag{1.5}$$

For each n, the nth *order reachability* [resp. *observability*] *map* of Σ is defined as $\mathbf{R}_n : R^{nm} \to X$[resp. $\mathbf{O}_n : X \to R^{np}$], where $\mathbf{R}_n$ is given, in block form, as

$$\mathbf{R}_n := [G, FG,..., F^{n-1}G] \tag{1.6}$$

and $\mathbf{O}_n$ is given, in block form, as

$$\mathbf{O}_n := \begin{bmatrix} H \\ HF \\ \vdots \\ HF^{n-1} \end{bmatrix}. \tag{1.7}$$

Observe that Σ realizes f iff $\mathbf{H}_n := \mathbf{O}_n \circ \mathbf{R}_n$ for all n.

Assume X can be generated by n elements. We define Σ to be *reachable* [resp. *observable*, resp. *canonical*] iff $\mathbf{R}_n$ is surjective [resp. $\mathbf{O}_n$ is injective, resp. Σ is reachable and observable].

The following is a new

(1.8) DEFINITION. A system Σ is *split* iff the following three conditions hold:

(i) X is projective,

(ii) Σ is reachable, and

(iii) Σ' is reachable.

The response map f *splits* iff it can be realized by a split system.

The terminology is motivated by the fact that $\mathbf{O}_n$ splits (c.f. (1.3)) for a split Σ with n generators.

It is not difficult to prove that a split system is necessarily canonical. When R is a field, it is clear that canonical = split.

(1.9) *Remark.* When Q is an overring of R, any input/output map f over R can be naturally seen as an input/output map over Q. This applies in particular to an integral domain R and its quotient field Q. More generally, let S be an R-algebra; if Σ is a system over R then $\Sigma \otimes S$ is defined as the system ($X \otimes S$, $F \otimes 1_S$, $G \otimes 1_S$, $H \otimes 1_S$) over S. If f is a response map over R, then $f \otimes S$ is defined as the response over S given by $\{A_i \otimes 1_S\}$, in other words, by the sequence $\iota A_1, \iota A_2, \ldots$, where $\iota: R \to S$ is the map defining the algebra structure.

We write $f(M)$, $X(M)$, etc. instead of $f \otimes (R/M)$, $X \otimes (R/M)$, etc., for M in Ω.

One of the main reasons for the restriction on R to be Noetherian is the following important result due to Rouchaleau, Wyman, and Kalman (1972):

(1.10) THEOREM. *Let R be a Noetherian integral domain, Q its quotient field. Let f be a response map over R. Suppose that $f \otimes Q$ is realizable over Q. Then f is realizable over R.*

Proof. See the above reference or the alternative proofs in Eilenberg (1974, Chapter XVI, Theorem 12.1) and Sontag (1976, Appendix). ∎

2. THE MAIN RESULT

The main result of this paper is Theorem (2 1).

(2.1) THEOREM. *Let R be a Noetherian integral domain, Q its quotient field, and f a response map over R. Suppose*

$$\operatorname{rank}_Q f = n.$$

Then f splits if and only if $I_n(\mathbf{H}_n) = R$.

For R = principal-ideal domain, the condition $I_n(\mathbf{H}_n) = R$ means that the greatest common divisor of all $n \times n$ minors of $\mathbf{H}_n$ must be a unit. Further, over this R projective modules are free. So (2.1) gives a useful condition for existence of free split realizations over principal-ideal domains.

The proof of (2.1) will be delayed until certain general facts are established. The next result is useful in studying questions of reachability.

(2.2) PROPOSITION. *A system Σ over R is reachable if and only if for any M in Ω the system $\Sigma(M)$ over R/M is reachable.*

Proof. If Σ has n generators then each $\Sigma(M)$ has dimension not greater than n. Therefore the problem is to show that

$$\mathbf{R}_n \textit{ is surjective iff every } \mathbf{R}_n(M) \textit{ is surjective.}$$

This is immediate from Bourbaki (Algèbre Commutative II.3.3, Proposition 11). ∎

(2.3) OBSERVATION. *Let C be in $R^{s \times t}$* and let $n \leqslant \min\{s, t\}$. Then $I_n(C) = R$ *if and only if* $\operatorname{rank}_{R/M} \pi_M C \geqslant n$ *for all M in Ω*. Indeed, this condition is equivalent to the existence, for each M, of a minor of order n of C which is nonzero in R/M. In other words, for each M there is some minor of order n of C not in M. This can only happen when the ideal $I_n(C)$ is not contained in any maximal ideal, i.e., if it is not proper. ∎

(2.4) PROPOSITION. *Let R be a commutative ring. Suppose that $\Sigma = (X, F, G, H)$ is a canonical projective realization of f of rank n. The following statements are then equivalent:*

(a) *f splits.*

(b) *Σ is a split system.*

(c) *Σ' is reachable.*

(d) *$\Sigma'(M)$ is reachable for every M in Ω.*

(e) *$\Sigma(M)'$ is reachable for every M in Ω.*

(f) *$\Sigma(M)$ is observable for every M in Ω.*

(g) *$\Sigma(M)$ is canonical for every M in Ω.*

(h) $\operatorname{rank}_{R/M} f(M) = n$ *for every M in Ω.*

(i) $\mathbf{H}_n(M) = \pi_M \mathbf{H}_n$ *has rank n for every M in Ω.*

(j) $I_n(\mathbf{H}_n) = R$.

(k) $\mathbf{O}_n(M)$ *has rank n for every M in Ω.*

If Σ is free, the above statements are also equivalent to:

(l) $I_n(\mathbf{O}_n) = R$.

Proof. First observe that since each R/M is a field, the equivalence between (e), (f) and (k), and the equivalence among (g), (h) and (i) are all well-known facts (see for instance Kalman, Arbib, and Falb 1969, Chapter 10). Observation (2.3) proves that (i) is equivalent to (j) and that (k) is equivalent to (l). Therefore it will be enough to prove that equivalence of (a), (b), (c), (d), (e) and the equivalence of (f), (g).

(a) Equivalent to (b). Any split realization Σ_1 of f is in particular canonical. By the uniqueness of canonical realizations (see Eilenberg, 1974, p. 419), $\Sigma \simeq \Sigma_1$. Therefore Σ is also a split system.

(b) Equivalent to (c). Trivial, because Σ is by hypothesis already reachable and projective.

(c) Equivalent to (d). Clear from (2.2).

(d) Equivalent to (e). Consider M in Ω. It follows from the discussion in Bourbaki (Algèbre, II.5.4) that the state-space $P(M)'$ can be canonically identified with $P'(M)$ (here P = projective is essential!). Under this identification, $F'(M)$ [resp. $G'(M)$, $H'(M)$] corresponds to $F(M)'$ [resp. $G(M)'$, $H(M)'$]. Therefore $\Sigma'(M)$ is canonically isomorphic to $\Sigma(M)'$. The equivalence is now clear.

(f) Equivalent to (g). By hypothesis Σ is reachable. So by (2.2) all the R/M-systems $\Sigma(M)$ are reachable. ∎

We may now give the

Proof of (2.1). Assume that f splits. Then the equivalence of (a) and (j) in (2.4) shows that $I_n(\mathbf{H}_n) = R$.

Conversely, suppose that $I_n(\mathbf{H}_n) = R$, i.e. $\pi_M \mathbf{H}_n$ has rank n for all M. To prove that f splits, it is enough to show that (2.4) can be applied. In other words, it must be proved that the canonical state space $X = X_f$ is a (finitely generated) projective R-module of rank n.

Since R is Noetherian, f is realizable; see (1.10). Assume then that X can be generated by s elements. Then X is isomorphic to the R-module generated by the columns of $\mathbf{H}_s$ (Rouchaleau, 1972, Section 2.A); see also Sontag (1976, Lemma (3.11)).

Fix a maximal ideal M. Denote by R_M the *localization* of R at M, the local ring consisting of all fractions a/b with a, b in R and b not in M (see Bourbaki, Algèbre Commutative II.3.2, Proposition 3). Since R_M is a *flat* R-module (see Bourbaki, Algèbre Commutative II.2.4, Theorem 1) it follows that the canonical state-space of $f \otimes R_M$ is $X_M := X \otimes R_M$. Therefore X_M is isomorphic to the R-module generated by the columns of $\mathbf{H}_s$ (viewed as a matrix over R_M).

Since obviously $s \geqslant n$, from the hypothesis on the ranks of f over Q and of $\pi_M \mathbf{H}_n$ over R/M it follows that $\mathbf{H}_s$ has rank n over Q and $\pi_M \mathbf{H}_s$ has rank n over $R/M = R_M/MR_M$. The lemma in the Appendix can be applied over R_M (with $\Lambda = \{1\}$ and $K_1 = Q$). Therefore X_M is free.

It follows from Bourbaki (Algèbre Commutative, II.5.3, Theorem 2) that X is projective of rank n. ∎

(2.5) *Remark.* In many cases of interest the realizations whose existence is claimed (under the stated hypothesis) can in fact be constructed explicitly. For principal-ideal domains, for example, it is only necessary to apply the usual realization procedure generalizing "Silverman's formulas" (see Rouchaleau and Sontag, 1978); the resulting canonical system will be necessarily split. For local rings, it is only necessary to find a submatrix C of the Hankel matrix such that πC is invertible; "Silverman's formulas" can be applied over the field Q and the realization obtained will necessarily be over R.

When $f = (a_1, a_2, ...)$ is a scalar response map and the formal power series $\Sigma\, a_i z^{-i}$ is expressed over R as p/q, where $p, q \in R[z]$, we may state a condition directly in terms of the "transfer function" p/q. Given two polynomials p, q over R we denote by $\rho(p, q)$ the *resultant* of p and q (see Lang [1965, p. 135]). This is an element of R. Recall Bourbaki [Algèbre Commutative, V.1.2]) that an integral domain R is *integrally closed* iff for any equation

$$z^n + a_1 z^{n-1} + \cdots + a_n = 0 \qquad (*)$$

(where all a_i are in R) every solution in Q is necessarily in R. (For instance, unique factorization domains are integrally closed.)

A scalar realizable response map f over an integrally closed domain R admits a transfer function p/q, where q is in fact the minimal polynomial of f over Q (see Eilenberg, 1974, Chapter XVI Section 12; Rouchaleau and Sontag, 1978, Lemma (1.2)). We call such a transfer function *irreducible*. We can then state

(2.6) Proposition. *Let R be an integrally closed integral domain. Let f be a $(1, 1)$-response map over R, with irreducible transfer function p/q. Then f splits iff $\rho(p, q)$ is a unit.*

Proof. The condition $\rho(p, q) =$ unit is equivalent to the following requirement: $\rho(p(M), q(M)) \neq 0$ for all M in Ω, where $p(M)$, $q(M)$ are obtained by reducing modulo M the coefficients of p, q. But $\rho(p(M), q(M)) = 0$ precisely when $p(M)$, $q(M)$ have a common factor, i.e. when $\operatorname{rank} f(M) < n$. The result follows then immediately from (2.1). ∎

3. The Case of Reduced Rings

Recall that a commutative ring R is *reduced* when R has no nilpotent elements. (Example: $\mathbb{Z}_{10}$, the integers modulo 10.) If R is a Noetherian reduced ring, let $\mathbf{P}(R)$ denote the (finite) set of *minimal prime ideals* of R. Let $\mathbf{Q}(R)$ denote the set of quotient fields of the R/p, p in $\mathbf{P}(R)$.

The following result generalizes (2.1) to the case of reduced rings:

(3.1) THEOREM. *Let R be a Noetherian reduced ring. Then the response map f splits if and only if:*

(i) *the numbers* $\operatorname{rank}_Q(f \otimes Q)$ *are equal for all Q in* $\mathbf{Q}(R)$, *and*

(ii) *for every M in Ω,* $\operatorname{rank}_{R/M} \mathbf{H}_n(M) = n$, *where n is the common value of* $\operatorname{rank}_Q(f \otimes Q)$.

Sketch of Proof. ["if"] Let $S := (R/p_1) \times \cdots \times (R/p_n)$, where $p_1, ..., p_n$ are the elements of $\mathbf{P}(R)$. Since each R/P_i is a Noetherian integral domain, each $f \otimes (R/p_i)$ is realizable and hence f is realizable as a map over S. But S is a finite extension of R, so f is realizable over R. Therefore the canonical state-space $X = X_f$ is a finitely generated R-module. As in (2.1), it must be proved that X is projective of rank n.

Let M be in Ω. Then R_M is also reduced (Bourbaki [Algèbre Commutative, II.2.7, Proposition 17]). The minimal ideals of R_M correspond to those minimal ideals of R which are contained in M and $\mathbf{Q}(R_M)$ is a subset of $\mathbf{Q}(R)$ (see Bourbaki, Algèbre Commutative, II.3.1, Proposition 3). Therefore the result in the Appendix can be again applied, where the K_λ are the elements of $\mathbf{Q}(R_M)$.

["only if"] This is similar to the proof of (2.1). ▮

APPENDIX. A CRITERION FOR FREENESS

LEMMA. *Let R be a (commutative) local ring and write $\pi: R \to k$ for the canonical map into the residue field k of R. Suppose there is given a family of fields $\{K_\lambda, \lambda \in \Lambda\}$ and a family of ring homomorphisms $\alpha_\lambda : R \to K_\Lambda$ such that* $\bigcap \ker \alpha_\lambda = 0$. *Let V be in $R^{s \times t}$ and let X be the R-module generated by the columns of V. Then a sufficient condition for X to be a free module is*

$$\operatorname{rank}_{K_\lambda}(\alpha_\lambda V) = \operatorname{rank}_k(\pi V)$$

for all λ in Λ.

Proof. By definition of rank over the field k, πV has an $n \times n$ nonsingular submatrix πW, where W is an $n \times n$ submatrix of V. Let $\delta := \det W$. Thus $\pi\delta \neq 0$, i.e. δ is not in the unique maximal ideal of R. By Bourbaki (Algèbre Commutative II.3.1, Proposition 1), δ is a unit in R. Let $w_1, ..., w_n$ denote those columns of V which belong to W. Clearly the vectors $\{w_1, ..., w_n\}$ are R-linearly independent, because $\delta =$ unit.

The proof now reduces to showing that the vectors $w_1, ..., w_n$ generate X. In fact, let v be any other column of V. Let $\rho_1, ..., \rho_n$ denote the row indices of the submatrix W. Let $\delta_l := \det(a_{ij}^l)$ where

$$\begin{aligned} a_{ij}^l &= w_{\rho_i, j} && \text{if } j \neq l, \\ &= v_{\rho_i} && \text{if } j = l. \end{aligned}$$

(w_{ij} is the ith entry of w_j and v_i is the ith entry of v).

Consider

$$x := \delta v - \sum_{i=1}^{n} \delta_i w_i \in X.$$

Then, $\alpha_\lambda x = (\alpha_\lambda \delta)(\alpha_\lambda v) - \sum (\alpha_\lambda \delta_i)(\alpha_\lambda w_i)$ for each λ in Λ. Since δ is a unit in R, it follows that $\alpha_\lambda \delta$, which is equal to $\det(\alpha_\lambda W)$, is nonzero in K_λ. By definition of rank over a field, $\alpha_\lambda v$ is a unique K_λ-linear combination of the $\alpha_\lambda w_i$, and by Cramer's rule this combination has the coëfficients $\alpha_\lambda \delta_i / \alpha_\lambda \delta$. Therefore $\alpha_\lambda x = 0$.

Hence x is in $\ker \alpha_\lambda$ for each λ. Since $\bigcap \ker \alpha_\lambda = 0$, it follows that $x = 0$. Therefore $v = \sum (\delta_i/\delta)\, w_i$. ∎

Acknowledgment

The author wishes to thank Dr. E. Kamen for bringing the problem of existence of observers to the author's attention, thus motivating the research reported here and Professor R. E. Kalman for numerous suggestions concerning the preparation of this paper.

RECEIVED: July 1976

References

EILENBERG, S. (1974), "Automata, Languages, and Machines," Vol. A, Academic Press, New York.

KALMAN, R. E. (1968), "Lectures on Controllability and Observability," CIME Summer Course, 1968, Cremonese, Roma.

KALMAN, R. E., FALB, P. L., AND ARBIB, M. A. (1969), "Topics in Mathematical System Theory," McGraw–Hill, New York.

LANG, S. (1965), "Algebra," Addison–Wesley, Mass.

QUILLEN, D. (1976), Projective modules over polynomial rings, *Inv. Math.* **36**, 167–171.

ROUCHALEAU, Y., WYMAN, B. F., AND KALMAN, R. E. (1978), Algebraic structure of linear dynamical systems. III. Realization theory over a commutative ring, *Proc. Nat. Acad. Sci. USA* **69**, 3404–3406.

ROUCHALEAU, Y. (1972), Linear, discrete-time, finite-dimensional dynamical systems over some classes of commutative rings, Ph.D. Dissertation, Stanford University, Stanford, Calif.

ROUCHALEAU, Y., AND SONTAG, E. D. (1978), Minimal realizations of systems over rings, to appear in *J. Comp. System Sciences.*

SONTAG, E. D. (1976), Linear systems over commutative rings: a survey, *Richerche di Automatica* **7**, 1–34.