SIAM J. CONTROL AND OPTIMIZATION
Vol. 22, No. 5, September 1984

008

THE CANONICAL DIOPHANTINE EQUATIONS WITH APPLICATIONS*

W. A. WOLOVICH† AND P. J. ANTSAKLIS‡

Abstract. A fundamental relationship between appropriate pairs of polynomial matrices is presented. This relationship, termed canonical Diophantine equations, can be used to resolve a number of standard polynomial matrix problems. Here, the general Diophantine equation is constructively resolved in a unique minimal way; in addition, prime canonical factorizations of a system transfer matrix are derived from knowledge of any dual factorization.

Key words. multivariable control systems, linear systems, algebraic system theory, polynomial matrix algebra

1. Introduction. Polynomial matrices play an important role in many different aspects of linear system theory, especially when one describes the dynamical behavior of a given system in terms of either a right or left polynomial matrix factorization of the transfer matrix which defines the system; i.e. $T(s)=R(s)P_R^{-1}(s)=P_L^{-1}(s)Q(s)$. Questions such as obtaining state-space realizations of $T(s)$, or state observers associated with $T(s)$, or stabilizing compensators, which perform one or several simultaneous control functions, have been constructively resolved through the manipulation of polynomial matrices, and such results are cited in various texts and papers too numerous to delineate.

Generally speaking, there are certain "standard problems" (SP) involving polynomial matrix pairs, such as $\{R(s), P_R(s)\}$ or $\{P_L(s), Q(s)\}$, which underlie most of the polynomial matrix manipulations required to obtain solutions to questions such as those posed above. Some of these are the following:

(SP1) Solve the general Diophantine equation, $H(s)R(s)+K(s)P_R(s)=F(s)$, for an appropriate polynomial matrix pair, $\{H(s), K(s)\}$ given any arbitrary $F(s)$. The Bezout equation, when $F(s)=I$, would represent a special case of the general Diophantine equation.

(SP2) Obtain a dual, prime factorization, $P_L^{-1}(s)Q(s)$, of $T(s)$ from any given (not necessarily prime) factorization, $R(s)P_R^{-1}(s)$.

(SP3) Divide one polynomial matrix by another nonsingular one to obtain the unique strictly proper part and quotient.

(SP4) Determine a greatest common right or left divisor of a given pair of polynomial matrices.

Clearly, all of these "standard problems" are interrelated, and various solutions to all of them have been documented in numerous references, and this report will not even attempt to judge the merits of one solution relative to another.

It is important to note however that there is a fundamental, underlying relationship common to all of these standard polynomial matrix problems, which can be used to solve them all. In this paper, we will develop such a relationship which we will term "canonical Diophantine equations" because the solutions to such equations can be uniquely determined from canonical state-space representations.

* Received by the editors March 15, 1983, and in revised form August 22, 1983. This work was supported in part by the National Science Foundation under grant ECS79-16584 and by the Air Force Office of Scientific Research under grant AFOSR-82-0034.

† Division of Engineering and the Lefschetz Center for Dynamical Systems, Brown University, Providence, Rhode Island 02912.

‡ Department of Electrical Engineering, University of Notre Dame, Notre Dame, Indiana 46556.

In § 2, we formally establish both types of canonical Diophantine equations. The general Diophantine equation (SP1) is then constructively resolved in § 3 in a unique, minimal way. In § 4, we again employ the canonical Diophantine equation, along with the algorithm of § 3, to solve (SP2); i.e. to obtain canonical, dual prime factorizations of a given transfer matrix from knowledge of any matrix fraction description, and we conclude with some final remarks in § 5. It might be noted that solutions to (SP3) and (SP4), as well as other "standard polynomial matrix problems," will be addressed in subsequent reports using the canonical Diophantine formulation developed here.

2. The canonical Diophantine equations. Consider a pair $\{R(s), P_R(s)\}$ of polynomial matrices in the Laplace operator s with $R(s)$ $p\times m$ and $P_R(s)$ $m\times m$ and column proper; i.e. the $m\times m$ constant matrix, $\Gamma_c[P_R(s)]$, consisting of the coefficients of the highest degree terms in each column of $P_R(s)$ is nonsingular. If[1] μ_i denotes the degree of each (ith) column of $P_R(s)$, a relation we denote as

(1) $$\partial_{ci}[P_R(s)]=\mu_i,$$

it follows [1] that $|P_R(s)|$, the determinant of $P_R(s)$, will be a polynomial of degree n, where

(2) $$n=\sum_1^m \mu_i.$$

If the pair $\{R(s), P_R(s)\}$ is used to denote a right transfer matrix factorization of some multivariable system, so that the transfer matrix of the system

(3) $$T(s)=R(s)P_R^{-1}(s),$$

then a state-space realization $\{A, B, C, E(s)\}$ of $T(s)$ can readily be determined by the well-known "structure theorem" for linear multivariable systems [1], [2]. In particular, if we apply the polynomial matrix division algorithm to (3) to separate $T(s)$ into its strictly proper part, $\bar{R}(s)P_R^{-1}(s)$, and quotient, $E(s)$, i.e.

(4) $$T(s)=\bar{R}(s)P_R^{-1}(s)+E(s),$$

then a real triple $\{A, B, C\}$ of dimensions $n\times n$, $n\times m$, and $p\times n$, respectively, can be found such that

(5) $$C(sI-A)^{-1}B=\bar{R}(s)P_R^{-1}(s).$$

More specifically, following the development in [1], if the $(n\times m)$ polynomial matrix $S_R^{\mu}(s)$ is defined by the relation

(6) $$S_R^{\mu}(s)=\text{block diagonal}\begin{bmatrix}1\\ s\\ \vdots\\ s^{\mu_i-1}\end{bmatrix},$$

then there exists a real pair of matrices $\{A, B\}$ in multi-input controllable companion form [1] such that

(7) $$(sI-A)S_R^{\mu}(s)=BP_R(s).$$

[1] We will assume throughout for convenience, and without much loss of generality, that each $\mu_i\geqq 1$ and, later, that each $\nu_j\geqq 1$.

Furthermore, the μ_i defined by (1) will represent the controllability indices of $\{A, B\}$ in the sense that the following $n \times n$ "column ordered controllability matrix" associated with the pair, namely

$$\bar{L} = [b_1, Ab_1, \cdots A^{\mu_1 - 1} b_1, b_2, Ab_2, \cdots A^{\mu_2 - 1} b_2, \cdots A^{\mu_m - 1} b_m], \tag{8}$$

will be nonsingular. In (8), b_i denotes the ith column of B.

Since $\bar{R}(s) P_R^{-1}(s)$ is strictly proper, it can be shown [1] that

$$\bar{R}(s) = C S_R^{\mu}(s) \tag{9}$$

for some constant $(p \times n)$ matrix C, so that (7) and (9) together imply that

$$C S_R^{\mu}(s) P_R^{-1}(s) = \bar{R}(s) P_R^{-1}(s) = C(sI - A)^{-1} B, \tag{10}$$

thus verifying (5).

Now consider the "total observability matrix", $\mathcal{O}$, associated with the pair $\{C, A\}$, i.e., the $np \times n$ real matrix

$$\mathcal{O} = \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{bmatrix}. \tag{11}$$

Let $\bar{n}$ denote the rank of $\mathcal{O}$, a relation we represent as

$$\rho[\mathcal{O}] = \bar{n} \leqq n, \tag{12}$$

and select from top to bottom the first $\bar{n}$ linearly independent rows of $\mathcal{O}$. If these $\bar{n}$ rows are then reordered so that all rows containing the kth row of C, c_k, precede those containing $c_{k+\bar{1}}$, in increasing powers of A, we will obtain a set of observability indices, ν_j, associated with the pair $\{C, A\}$ as well as an $\bar{n} \times n$ real matrix $\bar{M}$, analogous to the $\bar{L}$ of (8), which we will call a "row ordered observability matrix" of $\{C, A\}$. In particular,

$$\bar{M} = \begin{bmatrix} c_1 \\ c_1 A \\ \vdots \\ c_1 A^{\nu_1 - 1} \\ c_2 \\ c_2 A \\ \vdots \\ c_2 A^{\nu_2 - 1} \\ \vdots \\ c_p A^{\nu_{p-1}} \end{bmatrix}, \tag{13}$$

a real matrix of full rank $\bar{n}$, where

$$\bar{n} = \sum_1^p \nu_j. \tag{14}$$

In view of this observation, a $(\bar{n}\times p)$ polynomial matrix, $S_R^\nu(s)$, can be defined by the relation

$$S_R^\nu(s)=\text{block diagonal}\begin{bmatrix}1\\ s\\ \vdots\\ s^{\nu_j-1}\end{bmatrix}. \tag{15}$$

In view of these preliminaries, we can now state the main result of this section.

THEOREM 1. *Consider a polynomial matrix pair,* $\{R(s), P_R(s)\}$, *with* $R(s)$ $p\times m$ *and* $P_R(s)$ $m\times m$ *and column proper. Let* $S_R^\mu(s)$ *be given by* (6), $\bar{M}$ *by* (13), *and* $S_R^\nu(s)$ *by* (15). *There exists another unique* $(\bar{n}\times m)$ *polynomial matrix,* $\hat{M}(s)$, *such that*

$$S_R^\nu(s)R(s)-\hat{M}(s)P_R(s)=\bar{M}S_R^\mu(s). \tag{*}$$

Proof. Using the results in [1], we first note that the given polynomial matrix pair $\{R(s), P_R(s)\}$ directly defines a Laplace transformed differential operator representation of a system which is equivalent to the state-space realization of the $T(s)$ given by (3), namely

$$P_R(s)z(s)=u(s), \tag{16a}$$

$$y(s)=R(s)z(s), \tag{16b}$$

where the relationship between the partial state, $z(s)$, of (16) and the state, $x(s)$, of the state-space realization is given by

$$S_R^\mu(s)z(s)=x(s). \tag{17}$$

By repeated "differentiation" of the (Laplace transformed) state-space output equation

$$y(s)=Cx(s)+E(s)u(s), \tag{18a}$$

while substituting the state equation,

$$sx(s)=Ax(s)+Bu(s), \tag{18b}$$

we obtain the relation

(19)

$$\begin{bmatrix}y(s)\\ sy(s)\\ \vdots\\ s^{n-1}y(s)\end{bmatrix}=\begin{bmatrix}C\\ CA\\ \vdots\\ CA^{n-1}\end{bmatrix}x(s)+\begin{bmatrix}E(s) & 0 & 0 & \cdots & 0\\ CB & E(s) & 0 & \cdots & 0\\ \vdots & & \vdots & & \vdots\\ CA^{n-2}B & CA^{n-3}B & \cdots & & E(s)\end{bmatrix}\begin{bmatrix}I\\ sI\\ \vdots\\ s^{n-1}I\end{bmatrix}u(s).$$

We next observe that the $\bar{M}$ of (13) can be directly obtained from the $\mathcal{O}$ of (11) by premultiplying $\mathcal{O}$ by a real $(\bar{n}\times np)$ "row selector matrix" which contains only 0's and $(\bar{n})$1's. If we now premultiply (19) by exactly the same row selector matrix, we obtain the relation

$$S_R^\nu(s)y(s)=\bar{M}x(s)+\hat{M}(s)u(s), \tag{20}$$

where

$$\hat{M}(s)=\begin{bmatrix}\hat{M}_1(s)\\ \vdots\\ \hat{M}_p(s)\end{bmatrix} \tag{21}$$

with each

$$\hat{M}_j(s)=\begin{bmatrix}E_j(s) & 0 & 0 & \cdots & 0\\ C_jB & E_j(s) & 0 & \cdots & 0\\ \vdots & & & & \vdots\\ C_jA^{\nu_j-2}B & \cdots & & & E_j(s)\end{bmatrix}\begin{bmatrix}I\\ sI\\ \vdots\\ s^{\nu_j-1}I\end{bmatrix}. \tag{22}$$

In (22), $E_j(s)$ and C_j denote the jth rows of $E(s)$ and C, respectively.

If we now use (16) and (17) to substitute into (20), we obtain

$$S_R^{\nu}(s)R(s)z(s)=\bar{M}S_R^{\mu}(s)z(s)+\hat{M}(s)P_R(s)z(s), \tag{23}$$

or since (23) must hold for arbitrary $z(s)$, that (*) must hold.

Finally, by right dividing (*) by $P_R(s)$, we note that

$$S_R^{\nu}(s)R(s)P_R^{-1}(s)=\bar{M}S_R^{\mu}(s)P_R^{-1}(s)+\hat{M}(s). \tag{24}$$

Since $\bar{M}S_R^{\mu}(s)P_R^{-1}(s)$ is strictly proper, it thus follows that the polynomial matrix $\hat{M}(s)$ *represents the unique quotient of* $S_R^{\nu}(s)R(s)P_R^{-1}(s)$; i.e. given the pair $\{R(s), P_R(s)\}$, $\hat{M}(s)$ is uniquely specified via (24) by the choice for $S_R^{\nu}(s)$. Theorem 1 is therefore established. We call (*) *a right canonical Diophantine equation of the pair* $\{R(s), P_R(s)\}$.

As we have now shown, (*) can be solved by first determining $S_R^{\mu}(s)$ by inspection of the column degrees of the column proper $P_R(s)$. The structure theorem of [1] can then be used to determine a state-space realization $\{A, B, C, E(s)\}$ of $T(s)=R(s)P_R^{-1}(s)$. The pair $\{C, A\}$ then defines the total observability matrix via (11), from which $\bar{M}$ and $S_R^{\nu}(s)$ are derived. Finally, $\hat{M}(s)$ can be obtained directly via (21) and (22).

We next note that nothing has been said, thus far, regarding the "primeness" of lack thereof of $R(s)$ and $P_R(s)$. In particular, (*) holds whether or not $R(s)$ and $P_R(s)$ are relatively right prime (*rrp*). We observe, moreover, that in light of the results given in [1], the zeros of the determinant of any greatest common right divisor, $\tilde{G}_R(s)$, of $R(s)$ and $P_R(s)$ will represent all of the unobservable modes of the system defined by (10). In view of this observation, it follows that

$$\bar{n}=\rho[\mathcal{O}]=n-\partial|\tilde{G}_R(s)|, \tag{25}$$

and, as a result, that $\bar{n}=n$ *if and only if* $R(s)$ *and* $P_R(s)$ *are rrp.* In such cases, the $\bar{M}$ given by (13) will be $n\times n$ and nonsingular.

It is of interest to note that once the full rank matrix $\bar{M}$ has been determined, premultiplication of $R(s)P_R^{-1}(s)$ by any polynomial matrix $H(s)$, followed by a separation of the resulting rational matrix into its *spp* and quotient, will always yield a constant premultiplier of $S_R^{\mu}(s)P_R^{-1}(s)$ in the span of $\bar{M}$, i.e. for any $q\times m$ polynomial matrix, $H(s)$,

$$H(s)R(s)P_R^{-1}(s)=\bar{H}\bar{M}S_R^{\mu}(s)P_R^{-1}(s)+\tilde{R}(s) \tag{26}$$

for some constant matrix $\bar{H}$. If this were not true, $\bar{M}$ would not represent the full rank row ordered observability matrix it is. The relationship represented by (26) is a useful one, as we will later show.

A dual result, analogous to (*), can now be readily established by considering any left matrix factorization $P_L^{-1}(s)Q(s)$ of a $\tilde{T}(s)$; i.e. consider a pair of polynomial matrices $\{P_L(s), Q(s)\}$, with $P_L(s)$ $p\times p$ and row proper, and $Q(s)$ $p\times m$, which define the $(p\times m)$ rational transfer matrix,

$$\tilde{T}(s)=P_L^{-1}(s)Q(s). \tag{27}$$

Define

$$\tilde{\nu}_j=\partial_{rj}[P_L(s)] \tag{28}$$

for $j=1,2,\cdots p$,

$$d=\sum_1^p \tilde{\nu}_j, \tag{29}$$

and the $(p\times d)$ polynomial matrix

$$S_L^\nu(s)=\text{block diagonal}\,[1 \quad s \quad \cdots \quad s^{\tilde{\nu}_j-1}]. \tag{30}$$

Let $\tilde{\mu}_i$ denote an ordered set of controllability indices of any minimal state-space realization of the system defined by (27). Define

$$\bar{d}=\sum_1^m \tilde{\mu}_i \tag{31}$$

and the $(m\times \bar{d})$ polynomial matrix

$$S_L^\mu(s)=\text{block diagonal}\,[1 \quad s \quad \cdots \quad s^{\tilde{\mu}_i-1}]. \tag{32}$$

In view of (30) and (32), a *left canonical Diophantine equation of the polynomial matrix pair* $\{P_L(s), Q(s)\}$ could then be written as

$$Q(s)S_L^\mu(s)-P_L(s)\hat{L}(s)=S_L^\nu(s)\bar{L} \tag{$*^T$}$$

where $\hat{L}(s)$ is the quotient of $P_L^{-1}(s)Q(s)S_L^\mu(s)$ and $(d\times\bar{d})$ $\bar{L}$ is a real, full rank $(\bar{d})$, column ordered controllability matrix of the system defined by (27).

It is of interest to note that if $\tilde{T}(s)$ given by (27) is equal to the $T(s)$ given by (3), then $R(s)P_R^{-1}(s)$ and $P_L^{-1}(s)Q(s)$ will represent "dual factorizations" of the same transfer matrix which thus satisfy the relation:

$$Q(s)P_R(s)=P_L(s)R(s). \tag{33}$$

Furthermore, if the $\tilde{\nu}_j$ given by (28) correspond to the ν_j defined by (13), so that

$$d=\sum_1^p \tilde{\nu}_j=\sum_1^p \nu_j=\bar{n}, \tag{34}$$

then $P_L(s)$ and $Q(s)$ will be relatively left prime, and $P_L^{-1}(s)Q(s)$ will represent a minimal order, left prime factorization of $T(s)=R(s)P_R^{-1}(s)$. It is well known [3] that such a factorization of $T(s)$ can always be found such that $P_L(s)$ is both row proper and column proper with

$$\partial_{rj}[P_L(s)]=\partial_{cj}[P_L(s)]=\nu_j, \tag{35}$$

and

$$\Gamma_c[P_L(s)]=I_p. \tag{36}$$

A new constructive procedure for obtaining such canonical, dual, prime factorizations of $T(s)$ via (*) will be presented in § 4.

3. General Diophantine equations. Polynomial matrix Diophantine equations of the form

$$H(s)R(s)+K(s)P_R(s)=F(s) \tag{37}$$

play an important role in many aspects of linear system theory, and numerous references can be cited to substantiate this observation; e.g. see [4]–[12], a nonexhaustive list. It is well known that if, in general, $R(s)$, $P_R(s)$, and $F(s)$ are of dimensions $p\times m$, $k\times m$, and $q\times m$, respectively, and if the rank (over the field of rational functions in s) of the composite $(p+k)\times m$ matrix

$$\begin{bmatrix} R(s) \\ \hline P_R(s) \end{bmatrix}$$

is m, i.e. if

$$\rho\begin{bmatrix} R(s) \\ \hline P_R(s) \end{bmatrix}=m, \tag{38}$$

then (37) has a solution $\{H(s), K(s)\}$ if and only if any gcrd, $\tilde{G}_R(s)$, of $R(s)$ and $P_R(s)$ is a right divisor of $F(s)$. A variety of different techniques have been devised to solve (37) when solutions do exist. In this section, a new constructive proof of sufficiency will be given, based on (*), which directly yields a unique, solution $\{H(s), K(s)\}$ to (37) with $H(s)$ of minimum column degree modulo the choice for $S_R^\nu(s)$.

To obtain this general result, first consider (37) when $P_R(s)$ is $m\times m$ and column proper, so that (*) holds, and right divide $F(s)$ by $P_R(s)$, i.e.,

$$F(s)P_R^{-1}(s)=\bar{F}S_R^\mu(s)P_R^{-1}(s)+\hat{F}(s) \tag{39}$$

to obtain the $(q\times n)$ real matrix $\bar{F}$ and the polynomial matrix quotient, $\hat{F}(s)$.

THEOREM 2. *Consider the Diophantine equation* (37) *with* $P_R(s)$ $m\times m$ *and column proper. If* (37) *is solvable, there exists a real* $(q\times\bar{n})$ *matrix* $\bar{H}$ *such that*

$$\bar{H}\bar{M}=\bar{F} \tag{40}$$

where $\bar{F}$ *is given by* (39). *Furthermore, the polynomial matrix pair*

$$H(s)=\bar{H}S_R^\nu(s) \tag{41}$$

and

$$K(s)=\hat{F}(s)-\bar{H}\hat{M}(s) \tag{42}$$

solves (37) *with* $H(s)$, *as given by* (41), *a unique* $(q\times p)$ *polynomial matrix of minimum column degree in the sense that*

$$\partial_{cj}[H(s)]<\nu_j \tag{43}$$

for $j=1,2,\cdots p$.

Proof. First, recall that (26) holds for any polynomial matrix, $H(s)$; i.e.

$$H(s)R(s)=\bar{H}\bar{M}S_R^\mu(s)+\tilde{R}(s)P_R(s) \tag{44}$$

for some real matrix, $\bar{H}$. Since

$$F(s)=\bar{F}S_R^\mu(s)+\hat{F}(s)P_R(s) \tag{45}$$

in light of (39), the solvability of (37) now implies that

$$[\bar{H}\bar{M}-\bar{F}]S_R^\mu(s)=[\hat{F}(s)-K(s)-\tilde{R}(s)]P_R(s). \tag{46}$$

or that

$$[\bar{H}\bar{M}-\bar{F}]S_R^\mu(s)P_R^{-1}(s)=\hat{F}(s)-K(s)-\tilde{R}(s). \tag{47}$$

Since the left side of (47) is either a strictly proper rational matrix or zero, while the right side is either a polynomial matrix or zero, both sides must be zero, thus establishing (40).

If the right canonical Diophantine equation (*) is now premultiplied by $\bar{H}$ and $F(s)-\hat{F}(s)P_R(s)$ is substituted for $\bar{H}\bar{M}S_R^\mu(s)=\bar{F}S_R^\mu(s)$ in light of (45), the general Diophantine equation, (37), is satisfied with $H(s)$ given by (41) and $K(s)$ given by (42).

To establish Theorem 2, we must finally show that the particular $H(s)$ given by (41) uniquely satisfies (43). To do this, consider any dual, relatively left prime factorization, $P_L^{-1}(s)Q(s)$, of $T(s)=R(s)P_R^{-1}(s)$, such that (33) through (35) hold. The composite $p\times(p+m)$ matrix

$$[P_L(s) \mid -Q(s)]$$

represents a prime basis for the null space of the composite $(p+m)\times m$ matrix [4]

$$\begin{bmatrix} R(s) \\ \hdashline P_R(s) \end{bmatrix}.$$

Therefore, if $\{H(s), K(s)\}$ represents any particular solution to (37), any other solution to (37), $\{\tilde{H}(s), \tilde{K}(s)\}$, can be written as

$$\tilde{H}(s)=H(s)+J(s)P_L(s) \tag{48}$$

and

$$\tilde{K}(s)=K(s)-J(s)Q(s), \tag{49}$$

for some polynomial matrix $J(s)$. In particular,

$$\begin{aligned}&[H(s)+J(s)P_L(s)]R(s)+[K(s)-J(s)Q(s)]P_R(s)\\ &\quad=H(s)R(s)+K(s)P_R(s)+J(s)[P_L(s)R(s)-Q(s)P_R(s)]=F(s)\end{aligned} \tag{50}$$

in light of (33). In light of (41), (35), and (36), however,

$$\partial_{cj}[H(s)]<\nu_j=\partial_{cj}[P_L(s)], \tag{51}$$

with $\Gamma_c[P_L(s)]=I_p$. It therefore follows from (48) that the unique

$$\operatorname{spp}\{\tilde{H}(s)P_L^{-1}(s)\}=H(s)P_L^{-1}(s), \tag{52}$$

or that the $H(s)$ given by (41) represents a unique solution to (37) of minimum column degree ν_j, for $j=1,2,\cdots p$. Theorem 2 is thus established.

It might be noted that if $P_R(s)$ of (37) is nonsingular but not column proper, (37) can be postmultiplied by any unimodular matrix, $U_R(s)$, which reduces $P_R(s)U_R(s)$ to column proper form. The results of this section can then be directly employed to obtain the unique solution $\{H(s), K(s)\}$ to (37) with $H(s)$ of minimum column degree in the sense of (43).

We finally note that $P_R(s)$ need not be square or nonsingular in order to utilize (*) to solve (37). In particular, note that (37) can be written in composite form as

$$[H(s) \mid K(s)]\begin{bmatrix} R(s) \\ \hdashline P_R(s) \end{bmatrix}=F(s). \tag{53}$$

Therefore, if (38) holds, (37) has a solution if and only if any *gcrd*, $\tilde{G}_R(s)$, of (the rows of)

$$\begin{bmatrix} R(s) \\ \hdashline P_R(s) \end{bmatrix}$$

is a right divisor of $F(s)$. If this condition holds, a new "$P_R(s)$" can be defined as any m linearly independent rows of

$$\begin{bmatrix} R(s) \\ \hdashline P_R(s) \end{bmatrix},$$

with the new "$R(s)$" given by the remaining rows. With these new definitions, (53) can then be solved for "$H(s)$" and "$K(s)$" using the results presented in this section. Finally, the actual $H(s)$ and $K(s)$, consistent with their original definitions, can be obtained by repositioning the columns of "$H(s)$" and "$K(s)$".

4. Canonical dual prime factorizations. At the conclusion of § 2, we noted that given a right matrix factorization, $R(s)P_R^{-1}(s)$, of $T(s)$, a dual, left matrix factorization, $P_L^{-1}(s)Q(s)$, can always be found which satisfies properties (35) and (36). In this section, we will present a new algorithm for obtaining such dual, canonical factorizations via the right canonical Diophantine equation (*), of § 2. In particular we will now constructively establish the following known result [3] in a new, direct way using (*).

THEOREM 3. *Consider any polynomial matrix pair $\{R(s), P_R(s)\}$ with $R(s)$ $p\times m$ and $P_R(s)$ $m\times m$ and column proper. There exists a "dual" relatively left prime pair $\{P_L(s), Q(s)\}$ of polynomial matrices with*

$$\partial_{cj}[P_L(s)] = \partial_{rj}[P_L(s)] = \nu_j, \tag{54}$$

for $j = 1, 2, \cdots, p$,

$$\Gamma_c[P_L(s)] = I_p, \tag{55}$$

and $\Gamma_r[P_L(s)]$ nonsingular with 1's along the diagonal such that $T(s) = R(s)P_R^{-1}(s) = P_L^{-1}(s)Q(s)$, or

$$P_L(s)R(s) = Q(s)P_R(s). \tag{56}$$

Proof. In light of (*) define the $p\times p$ diagonal polynomial matrix

$$D^\nu(s) = \text{diagonal}\,[s^{\nu_j}], \tag{57}$$

and set

$$F_L(s) = D^\nu(s)R(s) \tag{58}$$

in the general Diophantine equation (37), so that (39) implies that

$$F_L(s) = D^\nu(s)R(s) = \bar{F}_L S_R^\mu(s) + \hat{F}_L(s)P_R(s). \tag{59}$$

Equation (37) is clearly solvable in that any gcrd of $R(s)$ and $P_R(s)$ will be a right divisor of the particular $F_L(s) = D^\nu(s)R(s)$ given by (59). In light of Theorem 2, therefore, a constant $\bar{H}_L$ exists such that

$$\bar{H}_L\bar{M} = \bar{F}_L. \tag{60}$$

It thus follows that the polynomial matrix pair

$$H_L(s) = \bar{H}_L S_R^\nu(s), \tag{61}$$

and

(62) $$K_L(s)=\hat{F}_L(s)-\bar{H}_L\hat{M}(s)$$

solves (37) i.e., that

(63) $$\bar{H}_L S_R^\nu(s)R(s)+[\hat{F}_L(s)-\bar{H}_L\hat{M}(s)]P_R(s)=D^\nu(s)R(s),$$

or that

(64) $$[D^\nu(s)-\bar{H}_L S_R^\nu(s)]R(s)=[\hat{F}_L(s)-\bar{H}_L\hat{M}(s)]P_R(s),$$

so that (56) holds with

(65) $$Q(s)=\hat{F}_L(s)-\bar{H}_L\hat{M}(s)$$

and

(66) $$P_L(s)=D^\nu(s)-\bar{H}_L S_R^\nu(s).$$

Note that the $P_L(s)$ thus defined will be both column proper and row proper. In particular, in light of (66), it is clear that

(67) $$\partial_{cj}[P_L(s)]=\nu_j$$

for $j=1,2,\cdots,p$, and that

(68) $$\Gamma_c[P_L(s)]=I_p.$$

Since the ν_j represent an appropriately ordered set of observability indices of the system, $P_L(s)$ will be row proper as well [3] with 1's along the diagonal of $\Gamma_r[P_L(s)]$. We finally observe that since $\bar{n}=\sum_1^p \nu_j$ represents the order of a minimal realization of $T(s)=R(s)P_R^{-1}(s)=P_L^{-1}(s)Q(s)$, and $\partial|P_L(s)|=\bar{n}$, $P_L(s)$ and $Q(s)$ will be relatively left prime. Theorem 3 is thus established.

5. Concluding remarks. A new, fundamental relationship between appropriate pairs of polynomial matrices has now been presented and employed to resolve some "standard (polynomial matrix) problems" in a new and direct manner. In particular, the utility of the dual, canonical Diophantine equations (*) and ($*^T$), has now been thoroughly demonstrated with respect to (SP1) obtaining unique minimal degree solutions to general Diophantine equations, and (SP2) determining canonical, prime, transfer matrix factorizations of a given system from knowledge of any dual factorization.

It is of interest to note that the dimension of the largest matrix, M, which need be inverted in order to solve a general matrix Diophantine equation of the form (37) is n, the system order, unlike earlier algorithms which require the inversion of a matrix of generic dimension $2n$. This could significantly reduce the computations necessary to implement a variety of adaptive control algorithms.

Finally, it should be noted that additional implications of (*) and ($*^T$) do exist with respect to other polynomial matrix problems, and that some of these will be addressed in subsequent reports.

REFERENCES

[1] W. A. WOLOVICH, *Linear Multivariable Systems*, Springer-Verlag, New York, 1974.
[2] W. A. WOLOVICH AND P. L. FALB, *On the structure of multivariable systems*, this Journal, 7 (1969), pp. 437–451.

[3] R. GUIDORZI, *Canonical structures in the identification of multivariable systems*, Automatica, 11 (1975), pp. 361–374.
[4] G. D. FORNEY, JR. *Minimal bases of rational vector spaces with applications to multivariable linear systems*, this Journal, 13 (1975), pp. 493–520.
[5] W. A. WOLOVICH, P. ANTSAKLIS AND H. ELLIOTT, *On the stability of solutions to minimal and nonminimal design problems*, IEEE Trans. Automat. Control, 22 (1977), pp. 88–94.
[6] R. R. BITMEAD, S.-Y. KUNG, B. D. O. ANDERSON AND T. KAILATH, *Greatest common divisors via generalized Sylvester and Bezout matrices*, IEEE Trans. Automat. Control, AC-23 (1978), pp. 1043–1047.
[7] L. CHENG AND J. B. PEARSON, JR., *Frequency domain synthesis of multivariable linear regulators*, IEEE Trans. Automat. Control, AC-23 (1978), pp. 3–15.
[8] P. J. ANTSAKLIS, *Some relations satisfied by prime polynomial matrices and their role in linear multivariable system theory*, IEEE Trans. Automat. Control, AC-24 (1979), pp. 611–616.
[9] T. KAILATH, *Linear Systems*, Prentice-Hall, Englewood Cliffs, NJ, 1980.
[10] L. CHENG AND J. B. PEARSON, JR., *Synthesis of linear multivariable regulators*, IEEE Trans. Automat. Control, AC-26 (1981), pp. 194–202.
[11] V. KUCERA, *Discrete Linear Control*, John Wiley, New York, 1979.
[12] E. EMRE, *The polynomial equation* $AA_c + RP_c = \Phi$ *with application to dynamic feedback*, this Journal, 18 (1980), pp. 611–620.