Algebraic Methods for the Study of Some Linear Matrix Equations

T. E. Djaferis* and S. K. Mitter†
Laboratory of Information and Decision Systems
Massachusetts Institute of Technology
Cambridge, Massachusetts

Submitted by R. S. Varga

ABSTRACT

An algebraic viewpoint permits the formulation of necessary and sufficient conditions for the existence of a unique solution to some linear matrix equations. The theory developed is then used to express the solution in a finite series form and to prove a stability theorem.

1. INTRODUCTION

Let B, A and Q be given matrices of dimension $m \times m$, $n \times n$, and $m \times n$ respectively with elements in some field F, and g_{ij} be elements of F. Our first purpose in this paper is to express necessary and sufficient conditions for the existence of a unique solution $P(m \times n)$ to linear matrix equations of the form

$$\sum_{i=0}^{s} \sum_{j=0}^{t} g_{ij} B^i P A^j = Q, \tag{1.1}$$

where s, t are positive integers. Assuming that a unique solution exists, we then use the theory developed to express it in a finite series form. The approach is algebraic in nature, and the construction procedures can easily be implemented on a digital computer. Particular attention is given to equations $PA + BP = Q$ and $P - BPA = Q$. Their special subcases when $B = A'$ are the

*The research of the first author was supported by ERDA under Grant ERDA-E(49-18)-2087, while at M.I.T. He is presently with the department of Electrical and Computer Engineering at the University of Massachusetts, Amherst.

†The research of the second author has been supported by ERDA under Grant ERDA-E(49-18)-2087 and by NASA-NG:-22-009-124.

52 Vanderbilt Ave., New York, NY 10017 0024-3795/82/030125+18$02.75

very well-known Lyapunov equations, which have wide applications in control theory (stability theory, optimal control, stochastic control, etc.).

Equation (1.1) was first studied almost a century ago by Sylvester [16], who, recognizing that this is merely a set of mn equations in mn unknowns, proceeded by rewriting it in the equivalent vector form:

$$G_g \mathbf{p} = \mathbf{q} \tag{1.2}$$

where $\mathbf{p}$ and $\mathbf{q}$ are the $mn \times 1$ column vectors

$$\mathbf{p} = [p_{11}, p_{12}, \dots, p_{1n}, \dots, p_{21}, \dots, p_{2n}, \dots, p_{mn}]',$$

$$\mathbf{q} = [q_{11}, q_{12}, \dots, q_{1n}, \dots, q_{21}, \dots, q_{2n}, \dots, q_{mn}]'$$

with

$$P = (p_{ij}), \qquad Q = (q_{ij}),$$

and where

$$G_g = \sum_{i=0}^{s} \sum_{j=0}^{t} g_{ij} B^i \otimes (A')^j.$$

The symbol $\otimes$ denotes the direct product [12], and G_g is $mn \times mn$. This approach was also used in [15], [12], [13]. It is well known that a solution of (1.2), [and (1.1)] exists if and only if $\operatorname{rank}[G_g, \mathbf{q}] = \operatorname{rank}[G_g]$ and that a unique solution exists if and only if G_g is nonsingular. Using these ideas, one can write the solution as $\mathbf{p} = G_g^{-1}\mathbf{q}$, which can be constructed by computing the inverse of G_g.

A different method of approach is used by Kucera [11] for the study of the equation $BP + PA = C$, by introducing the linear transformation $L: P \to BP + PA$ on the vector space of $m \times n$ matrices. By this means he is able to formulate necessary and sufficient conditions for the existence of a solution. In contrast with the approach of Lancaster [13], who uses methods of contour integration, Wimmer and Ziebur [18] attack (1.1) using Taylor's formula for matrix functions.

Of particular importance, especially from a computational point of view, in the case when a solution exists, is the form in which the solution can be expressed. This concern is evidenced in an extensive literature. The solution of equations of the form (1.1) can be expressed in an infinite series form [13].

According to Lancaster [13] and Brockett [3], the solution can be written in an integral form. For example if λ_i, μ_j are the eigenvalues of A and B respectively and $\operatorname{Re}\lambda_i < 0$, $\operatorname{Re}\mu_j < 0$ for all i, j, then the unique solution to $BP + PA = Q$ is given by

$$P = -\int_0^\infty e^{Bt} Q e^{At}\, dt.$$

Hartwig [4] uses the theory of resultants to obtain a finite series solution to $BP - PA = -Q$ when the solution is unique, and clarifies earlier techniques used by Jameson [6]. Another method of approach is to use decomposition methods to transform the given equation to an equivalent one for which the solution is easier to construct. Bartells and Stewart [1] use the Schur decomposition to obtain a computationally attractive algorithm for the solution of $BP + PA = Q$.

The way in which we will proceed is to introduce a module structure on the space of $m \times n$ matrices F_{mn}. This will allow us to write Equation (1.1) in the form

$$\alpha_g * P = Q, \tag{1.3}$$

where α_g is an element of the underlying ring, and $*$ indicates multiplication of ring elements and $m \times n$ matrices. We then show that (1.3) has a unique solution if and only if α_g has an inverse. This will very naturally lead to a finite series expression for the solution P of (1.1) as

$$P = \alpha_g^{-1} * Q.$$

The approach has been inspired by an important paper by Kalman [9], who was concerned with the characterization of polynomials whose zeros lie in certain algebraic domains.

The paper is divided into six sections. In Section 2 we define an action f_{BA}, using which we impose the module structure on F_{mn}. In Section 3 we express necessary and sufficient conditions for the existence of a unique solution to (1.1). In Sections 4 and 5 we give special attention to equations $PA + BP = Q$ and $P - BPA = Q$ respectively. In Section 6 we look at Equation (1.1) over an arbitrary integral domain. In Section 7 we use the explicit form of the solution to prove a stability theorem and give a new proof to a theorem of Krein [13, Theorem 4].

2. THE ACTION f_{BA}

Let A be an $n \times n$ matrix and B an $m \times m$ matrix over E, some integral domain. Let $E[x, y]$ be the ring of polynomials in two variables x and y over E. Let $\Psi = (\phi_2(x), \psi_2(y))$ be the ideal in $E[x, y]$ generated by $\phi_2(x), \psi_2(y)$, the characteristic polynomials of A and B respectively. Elements of the. quotient ring $E[x, y]/\Psi$ are cosets (equivalence classes) denoted by $\Psi + a(x, y)$. The Cayley-Hamilton theorem holds [14]; therefore $\phi_2(A) = 0$, $\psi_2(B) = 0$. Since $\phi_2(x), \psi_2(y)$ are monic polynomials, division by $\phi_2(x), \psi_2(y)$ is possible, and as a consequence we can state:

LEMMA 2.1. *Let $g(x, y)$ be an element of $E[x, y]$. Then $g(x, y)$ can be written uniquely as*

$$g(x, y) = t(x, y)\phi_2(x)\psi_2(y) + p(x, y)\phi_2(x) + q(x, y)\psi_2(y) + r(x, y),$$

where:

(a) *the degree of $p(x, y)$ in y is less than m (or $p(x, y) = 0$),*
(b) *the degree of $q(x, y)$ in x is less than n (or $q(x, y) = 0$),*
(c) *the degree of $r(x, y)$ in y is less than m, in x less than n (or $r(x, y) = 0$)*

Proof. Division in x is possible; therefore

$$g(x, y) = a(x, y)\phi_2(x) + b(x, y),$$

where the degree of $b(x, y)$ in x is less than n or $b(x, y)$ is zero. Division in y is possible; therefore

$$a(x, y) = t(x, y)\psi_2(y) + p(x, y),$$

where the degree of $p(x, y)$ in y is less than m or $p(x, y)$ is zero. Also

$$b(x, y) = q(x, y)\psi_2(y) + r(x, y),$$

where the degree of $r(x, y)$ in y is less than m and the degree of $r(x, y)$ in x is less than n, or $r(x, y)$ is zero. Now then

$$g(x, y) = t(x, y)\phi_2(x)\psi_2(y) + p(x, y)\phi_2(x) + q(x, y)\psi_2(y) + r(x, y).$$

This representation is unique, since if

$$g(x,y)=t_1(x,y)\phi_2(x)\psi_2(t)+p(x,y)\phi_2(x)+q(x,y)\psi_2(y)+r(x,y)$$

with both representations satisfying (2.1), then

$$r_1(x,y)-r(x,y)=\underbrace{(t_1-t)}_{=\alpha}\phi_2(x)\psi_2(y)+\underbrace{(p_1-p)}_{=\beta}\phi_2(x)+\underbrace{(q_1-q)}_{=\gamma}\psi_2(y). \tag{2.1}$$

Suppose that $\alpha\neq 0$. Then there exists a term on the r.h.s. of (2.1) of the form ax^iy^j, $i\geqslant n$, $j\geqslant m$. This term cannot be canceled by any other term on the r.h.s. of (2.1); therefore $\alpha=0$. Suppose that $\beta\neq 0$. Then there exists a term on the r.h.s. of (2.1) of the form bx^iy^j, $i\geqslant n$. This is impossible, and $\beta=0$. It then follows that $\gamma=0$ as well. ■

A direct consequence of this lemma is:

COROLLARY 2.2. *Let* $g_1=t_1\phi_2(x)\psi_2(y)+p_1\phi_2(x)+q_1\psi_2(y)+r_1$ *and* $g_2=t_2\phi_2(x)\psi_2(y)+p_2\phi_2(x)+q_2\psi_2(y)+r_2$, *written in the form of Lemma* 2.1 (a)–(c), *be the same coset* $\Psi+a(x,y)$. *Then* $r_1=r_2$.

The above results allow us to pick a unique representative from each coset $\Psi+g(x,y)$. If g is any element in $\Psi+g(x,y)$ and $g=t\phi_2(x)\psi_2(y)+p\phi_2(x)+q\psi_2(y)+r$ as in Lemma 2.1 (a)–(c), then $r=g(x,y)$ mod Ψ is this unique representative.

Let E_{mn} be the set of all $m\times n$ matrices over E. Define the action $f_{BA}: E[x,y]\times E_{mn}\to E_{mn}$ in the following manner:

$$f_{BA}(h(x,y),M)=\sum_{jk}h_{jk}B^jMA^k,$$

where $h(x,y)=\Sigma_{jk}h_{jk}y^jx^k$ is an element in $E[x,y]$ and M an element in E_{mn}. It can be shown that f_{BA} has the following properties:

(i) $f_{BA}(u,M)=uM$, where u is an element in E,
(ii) $f_{BA}(g(x,y)+h(x,y),M)=f_{BA}(g(x,y),M)+f_{BA}(h(x,y),M)$,
(iii) $f_{BA}(g(x,y)h(x,y),M)=f_{BA}(g(x,y),f_{BA}(h(x,y),M))$
$\qquad=f_{BA}(h(x,y)),f_{BA}(g(x,y),M)$,
(iv) $f_{BA}(g(x,y),M)=f_{BA}(g(x,y)\text{ mod }\Psi,M))$,
(v) $f_{BA}(g(x,y),M+N)=f_{BA}(g(x,y),M)+f_{BA}(g(x,y),N)$,

where $g(x, y)$, $h(x, y)$ are any elements in $E[x, y]$ and M, N any matrices in E_{mn}. All these properties follow directly from the definition. It is important to note that the Cayley-Hamilton theorem is crucial in proving (iv). The definition of f_{BA} allows for the interpretation of E_{mn} as an $E[x, y]/\Psi$-module.

PROPOSITION 2.3. *The set E_{mn} of $m \times n$ matrices with elements in E is a module over the quotient ring $E[x, y]/\Psi$.*

Proof. The set of $m \times n$ matrices under addition is an abelian group. Define multiplication $(*)$ of cosets $\Psi + h(x, y)$ and $m \times n$ matrices M, in the following manner:

$$(\Psi + h(x, y)) * M = f_{BA}(h(x, y) \bmod \Psi, M).$$

The multiplication is well defined, and the properties of f_{BA} ensure that:

(1) $[\Psi + h(x, y)] * (M + N) = [\Psi + h(x, y)] * M + [\Psi + h(x, y)] * N$,
(2) $[\Psi + h(x, y)] * \{[\Psi + g(x, y)] * M\}$
$= \{[\Psi + h(x, y)][\Psi + g(x, y)]\} * M$,
(3) $\{[\Psi + h(x, y)] + [\Psi + g(x, y)]\} * M$
$= [\Psi + h(x, y)] * M + [\Psi + g(x, y)] * M$,
(4) $(\Psi + 1) * M = M$

for all M, N in E_{mn} and all $\Psi + h(x, y)$, $\Psi + g(x, y)$ in $E[x, y]/\Psi$, with $\Psi + 1$ being the multiplicative identity in $E[x, y]/\Psi$.

3. THE GENERAL EQUATION

We have already mentioned that Equation (1.1) can be written in the equivalent vector form (1.2) and that a unique solution exists if and only if G_g is invertible. We now show that Proposition 2.3 can be used to formulate an equivalent algebraic condition. For this and the next two sections we restrict our analysis to the case where E is actually some field F, and postpone the analysis over an arbitrary integral domain to Section 6.

Let F be some field, and let K be an algebraically closed extension of F. If $f(x, y)$ is an element of $F[x, y]$, we denote by $V(f(x, y))$ the variety of $f(x, y)$ in A_2^K (the affine space of dimension 2 over K). Let $\lambda_1, \lambda_2, \ldots, \lambda_n$ be the eigenvalues of A, and $\mu_1, \mu_2, \ldots, \mu_m$ be the eigenvalues of B, and $g(x, y)$ a polynomial in $F[x, y]$. We have already expressed Equation (1.1) in the equivalent form (1.2):

$$G_g\mathbf{p}=\mathbf{q}.$$

We can now state:

THEOREM 3.1. *The following statements are equivalent*:

(1) *Equation* (1.1) *has a unique solution for all Q.*
(2) *G_g is invertible.*
(3) *$g(\lambda_i,\mu_j)\neq 0$ for all μ_j,λ_i.*
(4) *$V(g(x,y))\cap V(\phi_2(x))\cap V(\phi_2(y))=\varnothing$.*
(5) *The coset $\Psi+g(x,y)$ is a unit in $F[x,y]/\Psi$.*

In particular if $e(x,y)$ is a polynomial for which $[\Psi+e(x,y)][\Psi+g(x,y)]=\Psi+1$ holds, then $p=f_{BA}(e(x,y) \bmod \Psi, Q)$ is the unique solution of (1.1).

Proof. We will show the equivalences in the order

$$(1)\to(2)\to(3)\to(4)\to(5)\to(1).$$

(1) → (2): Clear.

(2) → (3): Suppose that $g(\lambda,\mu)=0$ for an eigenvalue λ of A and an eigenvalue μ of B. Let a' and b be eigenvectors of A, B, $(a'A=\lambda a',\ Bb=\mu b)$. Then $b\otimes a'\neq 0$, $G_g\cdot(b\otimes a')=\Sigma g_{ij}\mu^i\lambda^j(b\otimes a')=0$, *and G_g is singular.*

(3) → (4): Since $g(\lambda_i,\mu_j)\neq 0$ for all λ_i,μ_j, it follows that $g(x,y), \phi_2(x), \Psi_2(y)$ have no common zero in A_2^K.

(4) → (5): The coset $\Psi+g(x,y)$ is a unit if there exists a $\Psi+e(x,y)$ such that

$$[\Psi+e(x,y)][\Psi+g(x,y)]=\Psi+1.$$

Equivalently, $\Psi+g(x,y)$ is a unit if there exist $e(x,y)$, $a_1(x,y)$, $a_2(x,y)$ such that

$$e(x,y)g(x,y)+a_1(x,y)\phi_2(x)+a_2(x,y)\psi_2(y)=1.$$

Assuming that (4) holds [which also says that the polynomial $h(x,y)=1$ vanishes at every common zero of $g(x,y),\phi_2(x),\psi_2(y)$], by the Hilbert-*Nullstellensatz* [19] there exist polynomials $e(x,y), a_1(x,y), a_2(x,y)$ such that (3.1) holds, which implies that $\Psi+e(x,y)$ is a unit.

(5) → (1): Assume that $\Psi + g(x, y)$ is a unit in $F[x, y]/\Psi$. Let $\Psi + e(x, y)$ be such that $[\Psi + e(x, y)][\Psi + g(x, y)] = \Psi + 1$. We show that $P = f_{BA}(e(x, y) \bmod \Psi, Q)$ is the unique solution of (1.1), by substitution:

$$\begin{aligned}\sum_{i=0}^{s} \sum_{j=0}^{t} g_{ij} B^i P A^j &= f_{BA}(g(x, y), P)\\ &= f_{BA}(g(x, y), f_{BA}(e(x, y), Q))\\ &= f_{BA}(g(x, y) e(x, y), Q)\\ &= f_{BA}(1, Q) = Q.\end{aligned}$$

The solution is unique, since $f_{BA}(g(x, y), P) = Q$ implies

$$P = f_{BA}(e(x, y), f_{BA}(g(x, y), P)) = f_{BA}(e(x, y), Q). \qquad ■$$

Remark. In the above proof we give an explicit expression for the solution in finite series form. A general method for constructing such an $e(x, y)$ is through a constructive proof of the Hilbert *Nullstellensatz* or by using resultant theory [17]. In the next two sections we will show that for the equations $BP + PA = Q$ and $P - BPA = Q$ this generality is unnecessary and easier methods do exist.

Remark. It is interesting to note that Hartwig [5], while studying the equation $BP - PA = -Q$ using λ-matrices, obtains a similar finite series expression for the solution, in which the resultant of $\phi_2(x)$ and $\psi_2(y)$ appears. The approach we suggest applies equally well to the more general equation (1.1).

Remark. In our approach we have been using the ideal $\Psi = (\phi_2(x), \psi_2(y))$. Other ideals can be used, such as $\bar{\Psi} = (\bar{\phi}_2(x), \bar{\psi}_2(y))$, where $\bar{\phi}_2(x)$, $\bar{\psi}_2(y)$ are the minimal polynomials of A and B respectively. This could be used advantageously in order to reduce the amount of computation needed to construct the solution.

4. THE EQUATION $BP + PA = Q$

We have already shown that the solution to $BP + PA = Q$ (assuming a unique solution exists) can be expressed as

$$P = f_{BA}(e(x,y) \bmod \Psi, Q),$$

where $e(x,y)$ is such that $[\Psi + e(x,y)][\Psi + (x+y)] = \Psi + 1$. We now present two methods for the construction of such an $e(x,y)$.

Let $\phi_1(x) = \phi_2(-x)$, $\psi_1(x) = \psi_2(-x)$. It can be shown that $x + y$ divides $\phi_2(x)\psi_2(y) - \phi_1(y)\psi_1(x)$, and so let

$$p(x,y) = \frac{\phi_2(x)\psi_2(y) - \phi_1(y)\psi_1(x)}{x+y}.$$

This is a Bezoutian form [8]. Since $\lambda_i + \mu_j \neq 0$, this means that $\phi_2(x), \psi_1(x)$ are coprime and therefore there exist polynomials $a(x)$, $b(x)$, $a'(x), b'(x)$ such that

$$a(x)\psi_1(x) + b(x)\phi_2(x) = 1,$$

$$a'(x)\psi_2(x) + b'(x)\phi_1(x) = 1.$$

Let $e(x,y) = -a(x)b'(y)p(x,y)$. We then have

$$\begin{aligned} e(x,y)(x+y) &= -a(x)b'(y)[\phi_2(x)\psi_2(y) - \phi_1(y)\psi_1(x)] \\ &= -a(x)b'(y)\phi_2(x)\psi_2(y) - a(x)\psi_1(x)b'(y)\phi_1(y) \\ &= -a(x)b'(y)\phi_2(x)\psi_2(y) + [1 - b(x)\phi_2(x)][1 - a'(y)\psi_2(y)] \\ &= -[b(x)a'(y) - a(x)b'(y)]\phi_2(x)\psi_2(y) \\ &\quad - a'(y)\psi_2(y) - b(x)\psi_2(x) + 1. \end{aligned}$$

Therefore $[\Psi + e(x,y)]\,[\Psi + (x+y)] = \Psi + 1$.

A different method for obtaining an $\bar{e}(x,y)$ such that $\bar{e}(x,y)(x+y) + k_1(x,y)\phi_2(x) + k_2(x,y)\psi_2(y) = 1$ is the following. Divide $\phi_2(x)$ by $x + y$ in x:

$$\phi_2(x) = h(x,y)(x+y) + q(y).$$

Clearly $\phi_2(-y)=\phi_1(y)=q(y)$. Since $\phi_1(x)$, $\psi_2(x)$ are coprime, there exist $\lambda(y)$, $\mu(y)$ such that

$$\lambda(y)\phi_1(y)+\mu(y)\psi_1(y)=1$$

$$\rightarrow \quad \lambda(y)[\phi_2(x)-h(x,y)(x+y)]+\mu(y)\psi_2(y)=1$$

$$\rightarrow \quad -\lambda(y)h(x,y)(x+y)+\lambda(y)\phi_2(x)+\mu(y)\psi_2(y)=1.$$

Therefore let $\bar{e}(x,y)=-\lambda(y)h(x,y)$.

REMARK. The Lyapunov equation $A'P+PA=Q$ is dealt with in the same manner bearing in mind that $\psi_2(x)=\phi_2(x)$. Numerical examples can be found in [4].

5. THE EQUATION $P-BPA=Q$

The objective is to again construct an $e(x,y)$ such that

$$[\Psi+e(x,y)][\Psi+(1-xy)]=\Psi+1.$$

Let

$$\phi_2(x)=\det(xI-A)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0,$$

$$\psi_2(x)=\det(xI-B)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_0,$$

$$\phi_3(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n,$$

$$\psi_3(x)=b_0x^m+b_1x^{m-1}+\cdots+b_m.$$

If λ_i is a root of $\phi_2(x)$ which is nonzero, then $1/\lambda_i$ is a root of $\phi_3(x)$. Since we assume that a unique solution to $P-BPA=Q$ $(1-\lambda_i\mu_j\neq 0)$, we must have that $\phi_2(x)$, $\psi_3(x)$ are coprime. We also have that:

(a) if $n\geqslant m$, then $1-xy$ divides $y^{n-m}\phi_2(x)\psi_2(y)-\phi_3(y)\psi_3(x)$,
(b) if $n<m$, then $1-xy$ divides $x^{m-n}\phi_2(x)\psi_2(y)-\phi_3(y)\psi_3(x)$.

We comment on the validity of (a). Let

$$\begin{aligned} p_1 &= y^{n-m}\phi_2(x)\psi_2(y) \\ &= y^{n-m}(a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0)(b_my^m + \cdots b_0). \\ p_2 &= \phi_3(y)\psi_3(x) = (a_0y^n + a_1y^{n-1} + \cdots + a_n)(b_0x^m + \cdots b_m). \end{aligned}$$

In forming $p_1 - p_2$, combine terms from p_1 and p_2 which have the same coefficients (i.e., a_nb_m with $a_nb_mx^ny^my^{n-m}$, $a_{n-1}b_my$ with $a_{n-1}b_mx^{n-1}y^my^{n-m}$, and in general $a_kb_ly^{n-k}x^{m-l}$ with $a_kb_lx^ky^ly^{n-m}$, where $0 \leqslant k \leqslant n$, $0 \leqslant l \leqslant m$). Clearly

$$a_kb_l(x^ky^ly^{n-m} - y^{n-k}x^{m-l}) = k(x,y)(1-x^iy^i)$$

for some i, and consequently $1-xy$ divides $a_kb_l(x^ky^ly^{n-m} - y^{n-k}x^{m-l})$.

We are now in a position to construct $e(x,y)$. Since $\phi_3(x)$, $\psi_2(x)$ are coprime, there exist $a(x)$, $b(x)$, $a'(x)$, $b'(x)$ such that

$$\begin{aligned} a(x)\psi_3(x) + b(x)\phi_2(x) &= 1, \\ a'(x)\psi_2(x) + b'(x)\phi_3(x) &= 1. \end{aligned}$$

Now then if $n \geqslant m$, let

$$p(x,y) = \frac{y^{n-m}\phi_2(x)\psi_2(y) - \phi_3(y)\psi_3(x)}{1-xy};$$

if $n < m$, let

$$p(x,y) = \frac{x^{n-m}\phi_2(x)\psi_2(y) + \phi_3(y)\psi_3(x)}{1-xy}.$$

Let $e(x,y) = -a(x)b'(y)p(x,y)$. It immediately follows (assume $n \geqslant m$) that

$$\begin{aligned} e(x,y)(1-xy) &= -a(x)b'(y)[y^{n-m}\phi_2(x)\psi_2(y) - \phi_3(y)\psi_3(x)] \\ &= -a(x)b'(y)y^{n-m}\phi_2(x)\psi_2(y) + a(x)b'(y)\phi_3(y)\psi_3(x) \\ &= [b(x)a'(y) - a(x)b'(y)y^{n-m}]\,\phi_2(x)\psi_2(y) \\ &\quad - a'(y)\psi_2(y) - b(x)\phi_2(x) + 1. \end{aligned}$$

It follows that the solution can be written as $P = f_{BA}(e(x,y) \bmod \Psi, Q)$.

Remark. The discrete Lyapunov equation is the special case when $B = A'$, which introduces the simplification $\psi_2(x) = \phi_2(x)$, $n = m$.

6. OVER INTEGRAL DOMAINS

We now turn our attention to the case when Equation (1.1) [or its equivalent vector form (1.2)] is a linear equation over E, some integral domain. It is known that a unique solution exists if and only if $\det G_g$ is a unit in E (i.e. an element which has an inverse). Clearly $\det G_g$ is a unit iff G_g is invertible. We will now show that as in the case of a field the algebraic condition we have formulated remains valid. Let $\pi(u) = \det(I_{mn}U - G_g)$ and $\Pi = (\pi(u))$ the ideal generated by $\pi(u)$. We will need the following result.

Lemma 6.1. *Let* $h: E[u]/\Pi \to E[x, y]/\Psi$ *be the function defined by*

$$h: \Pi + a(u) \to \Psi + a(g(x, y)).$$

Then h is a ring homomorphism.

Proof. We first show that h is well defined. Let $\Pi + a(u) = \Pi + b(u)$ [i.e., $a(u) = b(u) = k(u)\pi(u)$]. Show that $\Psi + a(g(x, y)) = \Psi + b(g(x, y))$. We claim that $\pi(g(x, y)) = k(x, y)\phi_2(x)\psi_2(x) + k_1(x, y)\phi_2(x) + k_2(x, y)\psi_2(y)$ in the unique form of Lemma 2.1(a)–(c).

Clearly

$$\pi(u) = \prod_{ij} \left[u - g(\lambda_i, \mu_j)\right]$$

$$\to \quad \pi(g(x, y)) = \prod_{ij} \left[g(x, y) - g(\lambda_i, \mu_j)\right].$$

Now if $g(x, y) = g_t x^t + \cdots + g_0$ with g_t in $E[y]$, divide $g(x, y)$ by $x - \lambda_i$ in x. Then we have

$$\begin{aligned} g(x, y) = \big[& g_t x^{t-1} + (g_{t-1} + g_t\lambda_i)x^{t-2} \\ & + (g_{t-2} + g_{t-1}\lambda_i + g_t\lambda_i^2)x^{t-3} + \cdots \\ & + (g_1 + g_2\lambda_i + \cdots + g_t\lambda_i^{t-1})\big](x - \lambda_i) + h(y), \end{aligned}$$

but since $h(y)=g(\lambda_i, y)$, we have that

$$g(x,y)-g(\lambda_i,\mu_j)=k_{ij}(x,y)(x-\lambda_i)+g(\lambda_i,y)-g(\lambda_i,\mu_j).$$

It is also clear that $y-\mu_j$ divides $g(\lambda_i, y)-g(\lambda_i,\mu_j)$. Therefore

$$\pi(g(x,y))=\prod_{ij}\left[k_{ij}(x,y)(x-\lambda_i)+l_{ij}(x,y)(y-\mu_j)\right].$$

In expanding this product we see that every term in the sum will be of one of the two forms $a(x,y)\phi_2(x)$ or $b(x,y)\psi_2(y)$. This means that over $K[x,y]$ (where K is an algebraically closed extension of E) $\pi(g(x,y))$ can be written in the form of Lemma 2.1(a)–(c) as

$$\pi(g(x,y))=t_1(x,y)\phi_2(x)\psi_2(y)+p_1(x,y)\phi_2(x)+q_1(x,y)\psi_2(y).$$

Since by Lemma 2.1 this is a unique expression, we must have that t_1, p_1, q_1 are elements of $E[x,y]$. This means that

$$a(g(x,y))-b(g(x,y))=c_1(x,y)\phi_2(x)+c_2(x,y)\psi_2(y)$$

and that h is well defined.

It is immediate from the definition that

$$h([\Pi+a(u)]+[\Pi+b(u)])=h(\Pi+a(u))+h(\Pi+b(u))$$

and

$$h([\Pi+a(u)][\Pi+b(u)])=h(\Pi+a(u))h(\Pi+b(u)). \qquad \blacksquare$$

We are now in a position to state:

THEOREM 6.2. *Equation* (1.1) *has a unique solution over E if and only if* $\Psi+g(x,y)$ *is a unit in* $E[x,y]/\Psi$.

Proof. If $\Psi+g(x,y)$ is a unit, then $P=f_{BA}(e(x,y) \bmod \Psi, Q)$ is the unique solution, where $e(x,y)$ is such that $[\Psi+e(x,y)][\Psi+g(x,y)]=\Psi+1$. If (1.1) does have a unique solution for each Q, it means that $\det G_g$ is a unit in E. This means that if $\pi(u)=\pi_t u^t+\cdots+\pi_0$, $\pi_0=\det G_g$ is a unit. Let

$$k(u)=-\frac{\pi_t}{\pi_0}u^{t-1}-\frac{\pi_{t-1}}{\pi_0}u^{t-2}-\cdots-\frac{\pi_1}{\pi_0}.$$

Then $k(u)u+(1/\pi_0)\pi(u)=1$. Since $[\Pi+k(u)](\Pi+u)=\Pi+1$, from Lemma 6.1 we have

$$h(\Pi+k(u))h(\Pi+u)=h(\Pi+1),$$

$$\rightarrow \quad [\Psi+k(g(x,y))][\Psi+g(x,y)]=\Psi+1.$$

Remark. In particular E can be a polynomial ring, which means that matrices A and B can contain parameters. Using the techniques suggested previously, the solution can be expressed in terms of these parameters, the expression being valid for all parameter values for which a unique solution exists. For an example see [4]. This has a potential application in optimal control.

7. APPLICATIONS

A very important issue in stability theory is to be able to characterize a polynomial (i.e., determine in what region of the complex plane its roots lie) without having to compute the roots. This is done by devising methods which depend only on polynomial coefficients. It has been demonstrated [7, 9, 10, 2] that Lyapunov type equations play an important role in this investigation. What we propose to do is show that the explicit solution given in this paper can be used to prove stability theorems.

Following [9], we associate with any polynomial $p(x,y)$ in $\mathbb{C}[x,y]$ ($\mathbb{C}$ denoting the complex numbers) a unique square matrix C_p in the following manner: if $p(x,y)=\Sigma_{jk}c_{jk}y^j x^k$, c_{jk} in $\mathbb{C}$, then $C_p=(c_{jk})$, which is a matrix of dimension one plus the largest exponent in $p(x,y)$ of either x or y. Then $p(x,y)$ is called *positive* iff C_p is hermitian symmetric positive definite matrix. If $p(x,y)$ is a polynomial of degree $n-1$, it can be shown that $p(x,y)$ is positive iff $p(x,y)=\Sigma_{j=1}^{n}\pi_j(x)\bar{\pi}_j(y)$, where $\{\pi_j(x)\}$ is a basis for the vector space of polynomials of degree less than n over $\mathbb{C}$. This is a direct consequence of the fact that a matrix T is positive definite iff $T=V^*V$ for some V, $\det V\neq 0$. It is also true [9] that if $p(x,y)$ is of degree $n-1$ and positive, with $\lambda(x)$ mod ϕ a unit, then $\lambda(x)\bar{\lambda}(y)p(x,y)$ mod Φ is also positive. Φ is the ideal $\Phi=(\phi(x),\phi(y))$, where $\phi(x)$ is a polynomial of degree n.

Suppose now that $k(x)$ is a polynomial with real coefficients, and let Σ be the region in the complex plane defined by

$$\Sigma=\{\lambda\in\mathbb{C}\,|\,k(\lambda)+k(\bar{\lambda})<0\}.$$

If $k(x)=x$, then Σ is the left half plane. If $k(x)=x^2$, then Σ is a region in the complex plane contained within two straight lines which pass through the origin. If $k(x)=x^2-2$, then Σ is a region defined by a hyperbola. We can now state:

THEOREM 7.1. *Let A,C be real $n\times n$ matrices and (A,C) an observable pair (i.e., $L'=(C',(CA)',\cdots(CA^{n-1})')$ is full rank). A has all its eigenvalues in Σ if and only if there exits a unique symmetric positive definition solution to the equation*

$$k(A')P+Pk(A)=-C'C. \tag{7.1}$$

Proof. Let P be the unique symmetric positive definite solution to (7.1). Let $z\neq 0$ be an eigenvector corresponding to an eigenvalue λ of A. This means that

$$k(A')P+Pk(A)=-C'C,$$

$$A'k(A')PA+A'Pk(A)A=-A'CCA,$$

$$(A')^{n-1}k(A')PA^{n-1}+(A')^{n-1}Pk(A)A^{n-1}=-(A')^{n-1}C'CA.$$

Multiplying by $\bar{z}'$ on the left, z on the right, and adding, we have

$$\underbrace{(1+\lambda\bar{\lambda}+\cdots+\lambda^{n-1}\bar{\lambda}^{n-1})}_{=q}\bar{z}'[k(A')P+Pk(A)]z=-\bar{z}'L'Lz<0,$$

where $q>0$. Now $k(A)z=k(\lambda)z$ and therefore

$$q[k(\bar{\lambda})\bar{z}'Pz+z'Pzk(\lambda)]<0$$
$$\rightarrow\quad q[k(\bar{\lambda})+k(\lambda)]\bar{z}'Pz<0.$$

Since $q>0$ and P is positive definite, $k(\bar{\lambda})+k(\lambda)<0$, which means that λ is in Σ.

Assume that A does have its eigenvalues in Σ. Show that (7.1) has a unique symmetric positive definite solution. If we let $B=k(A)$, then for any eigenvalue λ of A we have that $k(\lambda)+k(\bar{\lambda})<0$, which means that B is a stable matrix. If $\phi_2(x)=\det(xI-B)$, $\phi_1(x)=\phi_2(-x)$, $\Phi=(\phi_2(x), \phi_2(y))$, then

$$p(x,y)=\frac{\phi_2(x)\phi_2(y)-\phi_1(x)\phi_1(y)}{x+y} \tag{7.2}$$

is positive [since B is positive and (7.2) is a Bezoutian form]. Let $\tau(x), \pi(x)$ be such that $\tau(x)\phi_1(x)+\pi(x)\phi_2(x)=1$ and

$$e(x,y)=-\tau(x)\tau(y)p(x,y) \bmod \Phi.$$

Since $\tau(x)$ mod ϕ_2 is a unit, it follows that $e(x,y)$ is negative, and $C_e=(e_{ij})$ negative definite.

A unique symmetric solution clearly exists and is given by

$$\begin{aligned} P &= f_{BA}(e(x,y),-C'C) \\ &= -\underbrace{\left[C',(CA)',\ldots,(CA^{n-1})'\right]}_{=L'}(C_e\otimes I)\underbrace{\begin{bmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{bmatrix}}_{=L}. \end{aligned}$$

Since C_e is negative definite, so is $C_e\otimes I$, and since L is full rank, P is positive definite. ■

Remark. For further results on how controllability and inertia theory are used to prove stability theorems, see [2].

One can also use the explicit form of the solution to give a new proof of an earlier result due to Krein [13, Theorem 4].

Theorem 7.2 (M. G. Krein). *Let B $(m\times m)$, A $(n\times n)$, and Q $(m\times n)$ be matrices over $\mathbb{C}$, and let $g(\lambda_i,\mu_j)\neq 0$ for all λ_i, μ_j, $1\leqslant i\leqslant n$, $1\leqslant j\leqslant m$. Then the unique solution P of* (1.1) *is*

$$P=-\frac{1}{4\pi^2}\int_{\Gamma_1}\int_{\Gamma_2}\frac{(yI-B)^{-1}Q(xI-A)^{-1}}{g(x,y)}dx\,dy,$$

where Γ_1, Γ_2 *are contours containing and sufficiently close to* $\{\mu_1, \dots \mu_m\}$, $\{\lambda_1, \dots \lambda_n\}$ *respectively.*

Proof. Since a unique solution to (1.1) exists, let $e(x,y) = \Sigma_{jk} e_{jk} y^j x^k$ such that

$$g(x,y)e(x,y) = 1 + \alpha_1(x,y)\phi_2(x) + \alpha_2(x,y)\Psi_2(y). \tag{7.3}$$

The unique solution is then given by

$$P = f_{BA}(e(x,y), Q) = \sum_{jk} e_{jk} B^j Q A^k. \tag{7.4}$$

From Equation (19) of [12, p. 551] we have

$$B^j = \frac{1}{2\pi i} \int_{\Gamma_1} y^j (yI - B)^{-1} dy,$$

$$A^k = \frac{1}{2\pi i} \int_{\Gamma_2} x^k (xI - A)^{-1} dx.$$

Substituting in (7.4), we have

$$P = -\frac{1}{4\pi^2} \sum_{jk} e_{jk} \left(\int_{\Gamma_1} y^j (yI - B)^{-1} dy \right) Q \left(\int_{\Gamma_2} x^k (xI - A)^{-1} dx \right)$$

$$= -\frac{1}{4\pi^2} \sum_{jk} \int_{\Gamma_1} \int_{\Gamma_2} e_{jk} y^j x^k (yI - B)^{-1} Q (xI - A)^{-1} dx\, dy$$

$$= -\frac{1}{4\pi^2} \int_{\Gamma_1} \int_{\Gamma_2} e(x,y)(yI - B)^{-1} Q (xI - A)^{-1} dx\, dy.$$

Using (7.3), we can write

$$P = -\frac{1}{4\pi^2} \int_{\Gamma_1} \int_{\Gamma_2} \frac{(yI - B)^{-1} Q (xI - A)^{-1}}{g(x,y)} dx\, dy$$

$$-\frac{1}{4\pi^2} \int_{\Gamma_2} \left(\int_{\Gamma_1} \frac{\alpha_1(x,y)}{g(x,y)} (yI - B)^{-1} dy \right) Q (xI - A)^{-1} \phi_2(x)\, dx$$

$$-\frac{1}{4\pi^2} \int_{\Gamma_1} \psi_2(y) (yI - B)^{-1} Q \left[\int_{\Gamma_2} \frac{\alpha_2(x,y)}{g(x,y)} (xI - A)^{-1} dx \right] dy.$$

Since $g(\lambda_i, \mu_j) \neq 0$, we can choose Γ_1, Γ_2 so close to $\{\mu_1, \dots \mu_m\}, \{\lambda_1, \dots \lambda_n\}$ that the functions in round and square brackets exist and are regular functions of x on Γ_2 and y on Γ_1 respectively. The result follows from [13, Lemma, p. 551].

The authors wish to thank Bernard Levy and the reviewer for their comments.

REFERENCES

1 R. H. Bartels and G. W. Stewart, Solution of the equations $AX + XB = C$, *Comm. ACM* 15:816–820 (1972).

2 D. Carlson and R. D. Hill, Controllability and inertia theory for functions of a matrix, *J. Math. Anal. Appl.* 59:260–266 (1977).

3 R. Brockett, *Finite Dimensional Linear Systems*, Wiley, New York, 1970, p. 61.

4 T. E. Djaferis and S. K. Mitter, Exact solution to Lyapunov's equation using algebraic methods, *Proc. IEEE CDC*, 1976, pp. 1194–1200.

5 R. Hartwig, Resultants and the solution of $AX - XB = C$, *SIAM J. Appl. Math.* 23:104–117 (1972).

6 A. Jameson, Solution of equation $AX + XB = C$ by inversion of an $m \times m$ or $n \times n$ matrix, *SIAM J. Appl. Math.* 16:1020–1023 (1968).

7 E. I. Jury, *Inners and Stability of Dynamic Systems*, Wiley, New York, 1974.

8 T. Kailath, *Linear Systems*, Prentice-Hall, Englewood Cliffs, N.J., 1980, p. 144.

9 R. E. Kalman, Algebraic characterization of polynomials whose zeroes lie in certain algebraic domains, *Proc. Nat. Acad. Sci. Math.* 64:818–823 (1969).

10 R. E. Kalman, On the Hermite-Fujiwara theorem in stability theory, *Quart. Appl. Math.* 23:279–282 (1965).

11 V. Kucera, The matrix equation $AX + XB = C$, *SIAM J. Appl. Math.* 26:15–24 (1974).

12 P. Lancaster, *Theory of Matrices*, Academic, New York, 1969.

13 P. Lancaster, Explicit solutions of linear matrix equations, *SIAM Rev.* 12:544–566 (1970).

14 S. Lang, *Algebra*, Addison-Wesley, Reading, Mass. 1965, p. 400.

15 C. C. MacDuffee, *The Theory of Matrices*, Chelsea, New York, 1946.

16 J. J. Sylvester, Sur la solution du cas le plus général des équations linéaires en quantités binaires c'est-a-dire en quaternions ou en matrices du second ordre," *C. R. Acad. Sci. Paris* 22 (1884).

17 A. L. Van Der Waerden, *Modern Algebra*, Vol. II, Ungar, 1966.

18 H. Wimmer and A. D. Ziebur, Solving the matrix equation $\Sigma f_\rho(A) \times g_\rho(B) = C$, *SIAM Rev.* 14:318–323 (1972).

19 O. Zariski and P. Samuel, *Commutative Algebra*, Vol. II, Van Nostrand, Princeton, 1958, p. 164.

Received 27 February 1981; revised 1 October 1981