JOURNAL OF ALGEBRA 88, 350–360 (1984)

Inversion of Matrices over a Commutative Semiring

CHRISTOPHE REUTENAUER AND HOWARD STRAUBING

Université Paris 6, Paris, France
Reed College, Portland, Oregon 97202

Communicated by P. M. Cohn

Received October 4, 1982

It is a well-known consequence of the elementary theory of vector spaces that if A and B are n-by-n matrices over a field (or even a skew field) such that $AB = 1$, then $BA = 1$. This result remains true for matrices over a commutative ring, however, it is not, in general, true for matrices over non-commutatives rings.

In this paper we show that if A and B are n-by-n matrices over a *commutative semiring*, then the equation $AB = 1$ implies $BA = 1$. We give two proofs: one algebraic in nature, the other more combinatorial. Both proofs use a generalization of the familiar product law for determinants over a commutative semiring.

1. SEMIRING AND MATRICES

A *semiring* is a set R together with two binary operations, addition and multiplication, such that

(i) addition and multiplication are associative,

(ii) addition is commutative,

(iii) the distribution law holds, that is, if $r, s, t \in R$ then $r(s+t) = rs + rt$ and $(r+s)t = rt + st$,

(iv) there is an additive identity element (denoted 0) and a multiplicative identity element (denoted 1),

(v) $0 \cdot r = r \cdot 0 = 0$ for all $r \in R$.

The semiring R is said to be *commutative* if its multiplication is commutative.

Addition and multiplication of n-by-n matrices over a semiring R are defined in the usual fashion. The set $R^{n \times n}$ of all such matrices is itself a

0021-8693/84 $3.00

semiring under these operations. We denote the multiplicative identity by 1 (it will always be clear from the context when "1" means the identity of $R^{n\times n}$ and when it means the identity of R). The goal of this paper is the proof of the following theorem:

THEOREM. *Let R be a commutative semiring and let $A, B \in R^{n\times n}$. If $AB = 1$ then $BA = 1$.*

2. A GENERALIZATION OF THE DETERMINANT

In all that follows we assume that R is a commutative semiring and that $n \geqslant 2$ (our theorem is, of course, trivial in the case $n = 1$).

We denote by $\mathscr{E}_n$ the set of all maps from the set $\{1,..., n\}$ into itself, by $\mathscr{S}_n$ the set of all permutations of this set, by $\mathscr{A}_n$ the set of all even permutations and by $\mathscr{B}_n$ the set of all odd permutations. We denote the image of $i \in \{1,..., n\}$ under $\alpha \in \mathscr{E}_n$ by $i\alpha$. Let $A = (a_{ij}) \in R^{n\times n}$ and define

$$A\delta^+ = \sum_{\sigma\in\mathscr{A}_n} \prod_{1\leqslant i\leqslant n} a_{i,i\sigma}, \qquad A\delta^- = \sum_{\sigma\in\mathscr{B}_n} \prod_{1\leqslant i\leqslant n} a_{i,i\sigma}.$$

$A\delta^+$ and $A\delta^-$ are called the *positive determinant* and *negative determinant* of A. If R is a ring, then $A\delta^+ - A\delta^-$ is the determinant of A. The following lemma is a generalization of the product law for determinants.

LEMMA 1. *Let $A, B \in R^{n\times n}$.*

(a) *There exists $r \in R$ such that*

$$\begin{aligned}(AB)\delta^+ &= (A\delta^+)(B\delta^+) + (A\delta^-)(B\delta^-) + r\\ (AB)\delta^- &= (A\delta^+)(B\delta^-) + (A\delta^-)(B\delta^+) + r.\end{aligned} \tag{1}$$

(b)

$$\begin{aligned}&(AB)\delta^+ + (A\delta^+)(B\delta^-) + (A\delta^-)(B\delta^+)\\ &\quad= (AB)\delta^- + (A\delta^+)(B\delta^+) + (A\delta^-)(B\delta^-).\end{aligned} \tag{2}$$

Proof. (a) Let $A = (a_{ij})$, $B = (b_{ij})$. Let $S = \mathbb{N}[a'_{ij}, b'_{ij}]$ be the semiring of all polynomials over $\mathbb{N}$ in the $2n^2$ commuting indeterminates $\{a'_{ij}, b'_{ij} \mid 1 \leqslant i, j \leqslant n\}$. There is then a unique surjective semiring morphism $\psi: S \to R$ such that $a'_{ij}\psi = a_{ij}$, $b'_{ij}\psi = b_{ij}$ for all $i, j \in \{1,..., n\}$. Let $A' = (a'_{ij})$, $B' = (b'_{ij})$. Clearly $(A'\delta^+)\psi = A\delta^+$, $(B'\delta^+)\psi = B\delta^+$, and so on. It thus suffices to show that Eqs. (1) hold for the matrices A', B' in $S^{n\times n}$; we recover the result for A and B in $R^{n\times n}$ upon applying the morphism ψ.

Now $(A'B')\delta^+ = \sum_{\sigma\in\mathscr{A}_n}\prod_{1\leqslant i\leqslant n}(a'_{i1}b'_{1,i\sigma}+\cdots+a'_{in}b'_{n,n\sigma})$. When we expand $\prod_{1\leqslant i\leqslant n}(a'_{i1}b'_{1,i\sigma}+\cdots+a'_{in}b'_{n,n\sigma})$ as a sum of monomials we obtain $n!$ terms of the form $\prod_{1\leqslant i\leqslant n}a'_{i,i\tau}b'_{i\tau,i\sigma}$, where τ runs over $\mathscr{S}_n$, plus some other terms. We obtain, upon rearranging factors,

$$\prod_{1\leqslant i\leqslant n} a'_{i,i\tau}b'_{i\tau,i\sigma} = \left(\prod_{1\leqslant i\leqslant n} a'_{i,i\tau}\right)\left(\prod_{1\leqslant i\leqslant n} b'_{i,i\tau^{-1}\sigma}\right).$$

Thus $(A'B')\delta^+ = \sum_{\sigma\in\mathscr{A}_n}\sum_{\tau\in\mathscr{S}_n}(\prod_{1\leqslant i\leqslant n}a'_{i,i\tau})(\prod_{1\leqslant i\leqslant n}b'_{i,i\tau^{-1}\sigma})+r^+$, where r^+ is the sume of the remaining terms.

For each $\sigma\in\mathscr{A}_n$, the map $\tau\mapsto\tau^{-1}\sigma$ is a bijection of $\mathscr{S}_n$ onto itself which takes $\mathscr{A}_n$ onto $\mathscr{A}_n$ and $\mathscr{B}_n$ onto $\mathscr{B}_n$. Thus

$$\begin{aligned}(A'B')\delta^+ &= \sum_{\eta\in\mathscr{A}_n}\sum_{\tau\in\mathscr{A}_n}\left(\prod a'_{i,i\tau}\right)\left(\prod b'_{i,i\eta}\right)\\ &\quad+\sum_{\eta\in\mathscr{B}_n}\sum_{\tau\in\mathscr{B}_n}\left(\prod a'_{i,i\tau}\right)\left(\prod b'_{i,i\eta}\right)+r^+\\ &=(A'\delta^+)(B'\delta^+)+(A'\delta^-)(B'\delta^-)+r^+.\end{aligned}$$

An analogous computation shows that $(A'B')\delta^- = (A'\delta^+)(B'\delta^-) + (A'\delta^-)(B'\delta^+) + r^-$ with r^- is S.

To complete the proof we need to show that $r^+ = r^-$: here we use the fact S is a subsemiring of the commutative ring T of polynomials over $\mathbb{Z}$ in the a'_{ij} and the b'_{ij}. In T we have

$$\begin{aligned}(A'\delta^+ - A'\delta^-)(B'\delta^+ - B'\delta^-) &= (\det A')(\det B') = \det(A'B')\\ &= (A'B')\delta^+ - (A'B')\delta^-\\ &= [(A'\delta^+)(B'\delta^+) + (A'\delta^-)(B'\delta^-) + r^+]\\ &\quad - [(A'\delta^+)(B'\delta^-) + (A'\delta^-)(B'\delta^+) + r^-]\\ &= (A'\delta^+ - A'\delta^-)(B'\delta^+ - B'\delta^-) + (r^+ - r^-).\end{aligned}$$

Thus $r^+ = r^-$.

(b) We obtain the identity (2) in the statement of the lemma immediately from Eqs. (1) upon adding $(A\delta^+)(B\delta^-) + (A\delta^-)(B\delta^+)$ to both sides of the first equation in (1) and $(A\delta^+)(B\delta^+) + (A\delta^-)(B\delta^-)$ to both sides of the second equation in (1). ∎

3. First Proof of the Theorem

Let $A = (a_{ij}) \in R^{n\times n}$. We denote by $\bar{A}$ the $n-1$-by-$n-1$ matrix obtained from A by erasing the ith rwo and the jth column. We now define

$$A^+_{ij} = \bar{A}\delta^+, \qquad A^-_{ij} = \bar{A}\delta^-.$$

A_{ij}^{+} and A_{ij}^{-} are called, respectively, the *positive* (ij)*-minor* and the negative (ij)-minor of A.

If R is a ring then the usual (ij)-minor of A is given by $A_{ij}=A_{ij}^{+}-A_{ij}^{-}$.

LEMMA 2. *If j is odd, then*

$$A\delta^{+}=a_{1j}A_{1j}^{+}+a_{2j}A_{2j}^{-}+a_{3j}A_{3j}^{+}+\cdots$$
$$A\delta^{-}=a_{1j}A_{1j}^{-}+a_{2j}A_{2j}^{+}+a_{3j}A_{3j}^{-}+\cdots.$$

If j is even, we obtain identities upon interchanging $A\delta^{+}$ and $A\delta^{-}$ in the above equations.

Proof. We use the same sort of reasoning that we used in the proof of Lemma 1(a): it is sufficient to prove the identities in the free semiring $S=\mathbb{N}[a_{ij}]$ of polynomials over $\mathbb{N}$ in the n^2 indeterminates a_{ij}. Since S embeds in the ring $T=\mathbb{Z}[a_{ij}]$ we can use the expansion of $\det A$ in terms of minors of the jth column. Thus

$$A\delta^{+}-A\delta^{-}=\det A=\sum_{1\leqslant i\leqslant n}a_{ij}A_{ij}(-1)^{i+j}$$
$$=\sum_{1\leqslant i\leqslant n}(-1)^{i+j}a_{ij}(A_{ij}^{+}-A_{ij}^{-}).$$

If we suppose j odd—the argument is entirely analogous in the case j is even—we obtain the equation

$$A\delta^{+}-A\delta^{-}=(a_{1j}A_{1j}^{+}+a_{2j}A_{2j}^{-}+\cdots)-(a_{1j}A_{1j}^{-}+a_{2j}A_{2j}^{+}+\cdots).$$

It remains to show that we can identify the positive and negative parts of the right-hand side.

The left-hand side is a sum of $n!$ monomials: there is no canceellation of terms of $A\delta^{+}$ by terms of $A\delta^{-}$, since these are all distinct. Since each of the two sums of the right-hand side is a sum of $\frac{1}{2}n!$ monomials, there can be no cancellation there either. Thus we can identify positive and negative parts of the two sides of the equation, and the lemma follows. ∎

We now define the positive comatrix A^{+} and the negative comatrix A^{-} of A by

$$A^{+}=\begin{pmatrix}A_{11}^{+} & A_{21}^{-} & A_{31}^{+} & \cdots\\ A_{12}^{-} & A_{22}^{+} & \cdots & \\ A_{13}^{+} & \cdots & & \\ \vdots & & & \end{pmatrix},\qquad A^{-}=\begin{pmatrix}A_{11}^{-} & A_{21}^{+} & A_{31}^{-} & \cdots\\ A_{12}^{+} & A_{22}^{-} & \cdots & \\ A_{13}^{-} & \cdots & & \\ \vdots & & & \end{pmatrix}.$$

Let C_{ij} be the matrix obtained by replacing the ith column of A by the jth column of A. Easily, $C_{ij}\delta^+ = C_{ij}\delta^-$. We denote the common value by $C_{ij}\delta^{\pm}$. Let

$$C = \begin{pmatrix} 0 & C_{12}\delta^{\pm} & C_{13}\delta^{\pm} & \cdots \\ C_{21}\delta^{\pm} & 0 & C_{23}\delta^{\pm} & \cdots \\ C_{31}\delta^{\pm} & C_{32}\delta^{\pm} & 0 & \cdots \\ \vdots & & & \end{pmatrix}.$$

LEMMA 3. *$A^+A = A\delta^+ + C$, $A^-A = A\delta^- + C$ (by $A\delta^+$ and $A\delta^-$ we mean the scalar matrices whose diagonal entries are $A\delta^-$ and $A\delta^-$, respectively).*

Proof. If i is odd, then the (i, j)-entry of A^+A is

$$A^+_{1i}a_{1j} + A^-_{2i}a_{2j} + A^+_{3i}a_{3j} + \cdots.$$

If $i = j$ then this is $A\delta^+$ (by Lemma 2). If $i \neq j$ then (Lemma 2 again) it is equal to the positive determinant of the matrix obtained by replacing the ith column of A by the jth column; that is, $C_{ij}\delta^{\pm}$. The reasoning is entirely analogous if i is even: thus $A^+A = A\delta^+ + C$. The same line of argument shows $A^-A = A\delta^- + C$. ∎

We say that an element r of a semiring T is *opposable* in T if there exists $s \in T$ such that $r + s = 0$. If r is opposable then the equation $r + s = r + t$ implies $s = t$. Further, the sum of two opposable elements is opposable and the product of an opposable element by any element of T is opposable.

LEMMA 4. *Let $A, B \in R^{n\times n}$. If $AB = 1$ then $(B\delta^+)C$ and $(B\delta^-)C$ are opposable in $R^{n\times n}$.*

Proof. Let $A = (a_{ij})$, $B = (b_{ij})$. Since $AB = 1$, $\sum_{k=1}^n a_{ik}b_{kj} = 0$ when $i \neq j$. Thus $a_{ik}b_{kj}$ is opposable in R for all $i, j, k \in \{1,..., n\}$ such that $i \neq j$.

If $i = j$, the (i, j)-entry of $(B\delta^+)C$ is 0, which is opposable.

If $i \neq j$, the (i, j)-entry of $(B\delta^+)C$ is

$$\begin{aligned}(B\delta^+)(C_{ij}\delta^{\pm}) &= \left(\sum_{\sigma\in\mathscr{A}_n} b_{1,1\sigma}\cdots b_{n,n\sigma}\right)\left(\sum_{\tau\in\mathscr{A}_n} x_{1\tau,\tau}\cdots x_{n\tau,n}\right) \\ &= \sum_{\sigma,\tau}\prod_{k=1}^{n} b_{k,k\sigma}x_{k\tau,k}\end{aligned}$$

where $x_{kl} = a_{kl}$ if $l \neq i$ and $x_{ki} = a_{kj}$. For each pair of permutations σ and τ in $\mathscr{A}_n$ either $j\sigma \neq j\tau$ or $j\sigma \neq i\tau$. In either case, each term of $(B\delta^+)(C_{ij}\delta^{\pm})$ contains a factor of the form $a_{rs}b_{st}$ with $r \neq t$. Consequently, each term of

$(B\delta^+)(C_{ij}\delta^+)$ is opposable in R, so $(B\delta^+)(C_{ij}\delta^\pm)$ is opposable in R. As each entry of $(B\delta^+)C$ is opposable in R, it follows that $(B\delta^+)C$ is opposable in $R^{n\times n}$. A parallel argument shows that $(B\delta^-)C$ is opposable in $R^{n\times n}$.

Proof of the Theorem. If $AB=1$ we have, by Lemma 3,

$$A^+A = A^+(AB)A = (A\delta^+)BA + CBA$$
$$A^-A = A^-(AB)A = (A\delta^-)BA + CBA.$$

We multiply the first equation through by $B\delta^+$, the second by $B\delta^-$, and add, obtaining

$$\begin{aligned}&A^+A(B\delta^+) + A^-A(B\delta^-)\\&\quad= [(A\delta^+)(B\delta^+) + (A\delta^-)(B\delta^-)]\,BA + (B\delta^+)\,CBA + (B\delta^-)\,CBA.\end{aligned}$$

We apply Lemma 3 again, obtaining

$$\begin{aligned}&(A\delta^+)(B\delta^+) + (A\delta^-)(B\delta^-) + (B\delta^+)\,C + (B\delta^-)C\\&\quad= [(A\delta^+)(B\delta^+) + (A\delta^-)(B\delta^-)]\,BA + (B\delta^+)\,CBA + (B\delta^-)\,CBA.\end{aligned}$$

Since $AB=1$, Lemma 1(b) gives $1 + (A\delta^+)(B\delta^-) + (A\delta^-)(B\delta^+) = (A\delta^+)(B\delta^+) + (A\delta^-)(B\delta^-)$. We apply this and Lemma 3 to the above equation, obtaining

$$\begin{aligned}&1 + (A\delta^+)(B\delta^-) + (A\delta^-)(B\delta^+) + (B\delta^+)C + (B\delta^-)C\\&\quad= BA + [(A\delta^+)(B\delta^-) + (A\delta^-)(B\delta^+)]\,BA + (B\delta^+)\,CBA + (B\delta^-)\,CBA\\&\quad= BA + (B\delta^+)(A\delta^- + C)\,BA + (B\delta^-)(A\delta^+ + C)\,BA\\&\quad= BA + (B\delta^+)\,A^-ABA + (B\delta^-)\,A^+ABA\\&\quad= BA + (B\delta^+)\,A^-A + (B\delta^-)\,A^+A\\&\quad= BA + (B\delta^+)(A\delta^- + C) + (B\delta^-)(A\delta^+ + C)\\&\quad= BA + (A\delta^+)(B\delta^-) + (A\delta^-)(B\delta^+) + (B\delta^+)C + (B\delta^-)C.\end{aligned}$$

By Lemma 4, $(B\delta^+)C$ and $(B\delta^-)C$ are opposable in $R^{n\times n}$. From Lemma 1(a) and the fact that $(AB)\delta^- = 1\delta^- = 0$ we conclude that $(A\delta^+)(B\delta^-) + (A\delta^-)(B\delta^+)$ is opposable, both as an element of R and as a scalar matrix in $R^{n\times n}$. Thus we can cancel $(A\delta^+)(B\delta^-) + (A\delta^-)(B\delta^+) + (B\delta^+)C + (B\delta^-)C$ from both ends of the above equation, obtaining

$$1 = BA. \quad \blacksquare$$

4. Second Proof of the Theorem

We denote by a_{ij}, $(AB)_{ij}$ and $(BA)_{ij}$ the (i, j)-entries of A, B, AB and BA, respectively. We must show, assuming $AB = 1$, that $(BA)_{ij} = 1$ when $i = j$ and $(BA)_{ij} = 0$ when $i \neq j$. To simplify the notation a bit, we will prove only that $(BA)_{11} = 1$ and $(BA)_{12} = 0$—there is no loss of generality in this.

We denote by $\mathscr{C}_n$ the set $\mathscr{E}_n \backslash \mathscr{S}_n$—that is, $\mathscr{C}_n$ consists of all maps from $\{1,..., n\}$ into itself which are *not* permutations. We define a map $\Phi: \mathscr{C}_n \times \mathscr{S}_n \to \mathscr{C}_n \times \mathscr{S}_n$ as follows: If $\alpha \in \mathscr{C}_n$ there exists a pair of indices $i < j$ such that $i\alpha = j\alpha$. Let i and j be the two *smallest* integers with this property. For each $(\alpha, \sigma) \in \mathscr{C}_n \times \mathscr{S}_n$ we define $(\alpha, \sigma)\Phi = (\alpha, \eta\sigma)$, where η is the transposition (i, j). It is easy to see that the composition $\Phi\Phi$ is the identity on $\mathscr{C}_n \times \mathscr{S}_n$. Thus the restriction of Φ to $\mathscr{C}_n \times \mathscr{A}_n$ is a bijection from $\mathscr{C}_n \times \mathscr{A}_n$ onto $\mathscr{C}_n \times \mathscr{B}_n$.

We say that an ordered pair $(\alpha, \beta) \in \mathscr{E}_n \times \mathscr{E}_n$ is $(1, 2)$-*linked* if there exists $i \in \{1,..., n\}$ such that $i\alpha = 2$, $i\beta = 1$ and $j\alpha = j\beta$ whenever $j \neq i$. The set of all $(1, 2)$-linked pairs is denoted $\mathscr{D}_n$. We define a map $\Psi: \mathscr{D}_n \times \mathscr{S}_n \to \mathscr{D}_n \times \mathscr{S}_n$ as follows: Let $((\alpha, \beta), \sigma) \in \mathscr{D}_n \times \mathscr{S}_n$. If β is *not* a permutation, then we proceed as in the definition of Φ, finding the smallest two indices $i < j$ such that $i\beta = j\beta$, and we define

$$((\alpha, \beta), \sigma)\Psi = ((\alpha, \beta), \eta\sigma)$$

where η is the transposition (i, j). If β *is* a permutation, then there exists a unique pair of indices i and j such that $i\alpha = j\alpha = 2$. In this case we define

$$((\alpha, \beta), \sigma)\Psi = ((\alpha, \eta\beta), \eta\sigma)$$

where η is the transposition (i, j). Once again it is easy to check that the composition $\Psi\Psi$ is the identity on $\mathscr{D}_n \times \mathscr{S}_n$, and, consequently, that the restriction of Ψ to $\mathscr{D}_n \times \mathscr{A}_n$ is a bijection from $\mathscr{D}_n \times \mathscr{A}_n$ onto $\mathscr{D}_n \times \mathscr{B}_n$.

Let $\sigma \in \mathscr{S}_n$ and $\alpha, \beta \in \mathscr{E}_n$. We define

$$\Gamma(\sigma) = \prod_{i=1}^{n} a_{i,i\sigma}$$

$$\Delta(\sigma) = \prod_{i=1}^{n} b_{i,i\sigma}$$

$$T((\alpha, \beta), \sigma) = \prod_{i=1}^{n} a_{i,i\alpha} b_{i\beta,i\sigma}$$

$$E(\alpha, \sigma) = T((\alpha, \alpha), \sigma) = \prod_{i=1}^{n} a_{i,i\alpha} b_{i\alpha,i\sigma}.$$

It is easy to verify that

$$E(\alpha,\sigma)=\Gamma(\alpha)\,\Delta(\alpha^{-1}\sigma) \qquad \text{if} \quad \alpha\in\mathscr{S}_n \tag{3}$$

$$E((\alpha,\sigma)\Phi)=E(\alpha,\sigma) \qquad \text{if} \quad \alpha\in\mathscr{C}_n \tag{4}$$

$$T(((\alpha,\beta),\sigma)\Psi)=T((\alpha,\beta),\sigma) \qquad \text{if} \quad (\alpha,\beta)\in\mathscr{D}_n. \tag{5}$$

We denote by $H(\alpha,\sigma)$ the element

$$\underbrace{1+\cdots+1}_{k\text{ times}}$$

of R, where k is the number of indices $j\in\{1,\dots,n\}$ such that $j\alpha=1$. Since $H(\alpha,\sigma)$ depends only on α, we have

$$H((\alpha,\sigma)\Phi)=H(\alpha,\sigma). \tag{6}$$

We define

$$\begin{aligned} Q_\sigma^{(i,j)} &= a_{1j}b_{i,1\sigma}(AB)_{2,2\sigma}\cdots(AB)_{n,n\sigma}\\ &\quad + (AB)_{1,1\sigma}a_{1j}b_{i,2\sigma}(AB)_{3,3\sigma}\cdots(AB)_{n,n\sigma}\\ &\quad \vdots\\ &\quad + (AB)_{1,1\sigma}\cdots(AB)_{n-1,(n-1)\sigma}a_{nj}b_{i,n\sigma}. \end{aligned}$$

If σ is the identity permutation then $(AB)_{i,i\sigma}=1$, and thus $Q_\sigma^{(i,j)}=(BA)_{ij}$. If σ is not the identity permutation, then each of the n terms in the definition of $Q_\sigma^{(i,j)}$ contains a factor of the form $(AB)_{p,q}$ with $p\neq q$; thus $Q_\sigma^{(i,j)}=0$. Combining these two observations shows

$$\begin{aligned} \sum_{\sigma\in\mathscr{A}_n} Q_\sigma^{(i,j)} &= (BA)_{ij}\\ \sum_{\sigma\in\mathscr{B}_n} Q_\sigma^{(i,j)} &= 0. \end{aligned} \tag{7}$$

Now if we attentively expand $Q_\sigma^{(1,1)}$ as a sum of monomials we obtain

$$Q_\sigma^{(1,1)}=\sum_{\alpha\in\mathscr{C}_n} H(\alpha,\sigma)\,E(\alpha,\sigma). \tag{8}$$

Indeed, each monomial that appears is of the form $\prod_{i=1}^{n} a_{i,i\alpha}b_{i\alpha,i\sigma}=E(\alpha,\sigma)$ for some $\alpha\in\mathscr{C}_n$, and this monomial appears once in $Q_\sigma^{(1,1)}$ for each index j such that $j\alpha=1$.

When we expand $Q_\sigma^{(1,2)}$, each monomial is of the form $T((\alpha,\beta),\sigma)$, where (α,β) is $(1,2)$-linked, and each $(1,2)$-linked pair appears exactly once. Thus

$$Q_\sigma^{(1,2)}=\sum_{(\alpha,\beta)\in\mathscr{D}_n} T((\alpha,\beta),\sigma). \tag{9}$$

We now complete the proof.

$$
\begin{aligned}
(BA)_{11} &= \sum_{\sigma \in \mathscr{A}_n} Q_\sigma^{(1,1)} && \text{(by (7))} \\
&= \sum_{\alpha \in \mathscr{T}_n, \sigma \in \mathscr{A}_n} H(\alpha, \sigma)\, E(\alpha, \sigma) && \text{(by (8))} \\
&= \sum_{\substack{\alpha \in \mathscr{C}_n \\ \sigma \in \mathscr{A}_n}} H(\alpha, \sigma)\, E(\alpha, \sigma) + \sum_{\substack{\alpha \in \mathscr{S}_n \\ \sigma \in \mathscr{A}_n}} E(\alpha, \sigma) && \text{(since } H(\alpha, \sigma) = 1 \text{ when } \alpha \in \mathscr{S}_n) \\
&= \sum_{\substack{\alpha \in \mathscr{C}_n \\ \sigma \in \mathscr{A}_n}} H((\alpha, \sigma)\Phi)\, E((\alpha, \sigma)\Phi) + \sum_{\substack{\alpha \in \mathscr{B}_n \\ \sigma \in \mathscr{A}_n}} \Gamma(\alpha)\, \Delta(\alpha^{-1}\sigma) \\
&\quad + \sum_{\substack{\alpha \in \mathscr{A}_n \\ \sigma \in \mathscr{A}_n}} \Gamma(\alpha)\, \Delta(\alpha^{-1}\sigma) && \text{(by (3), (4), (6))} \\
&= \sum_{\substack{\alpha \in \mathscr{B}_n \\ \tau \in \mathscr{B}_n}} \Gamma(\alpha)\, \Delta(\tau) + \sum_{\substack{\alpha \in \mathscr{A}_n \\ \tau \in \mathscr{A}_n}} \Gamma(\alpha)\, \Delta(\tau) + \sum_{\substack{\alpha \in \mathscr{C}_n \\ \sigma \in \mathscr{B}_n}} H(\alpha, \sigma)\, E(\alpha, \sigma) \\
& && \text{(since } \Phi \text{ is a bijection from } \mathscr{C}_n \times \mathscr{A}_n \text{ onto } \mathscr{C}_n \times \mathscr{B}_n) \\
&= (A\delta^-)(B\delta^-) + (A\delta^+)(B\delta^+) + \sum_{\substack{\sigma \in \mathscr{C}_n \\ \sigma \in \mathscr{B}_n}} H(\alpha, \sigma)\, E(\alpha, \sigma) \\
&= 1 + (A\delta^+)(B\delta^-) + (A\delta^-)(B\delta^+) + \sum_{\substack{\alpha \in \mathscr{C}_n \\ \sigma \in \mathscr{B}_n}} H(\alpha, \sigma)\, E(\alpha, \sigma) \\
& && \text{(by Lemma 1(b) and the fact that } (AB)\delta^+ = 1\delta^+ = 1 \text{ and } (AB)\delta^- = 1\delta^- = 0) \\
&= 1 + \sum_{\substack{\alpha \in \mathscr{A}_n \\ \tau \in \mathscr{B}_n}} \Gamma(\alpha)\, \Delta(\tau) + \sum_{\substack{\alpha \in \mathscr{B}_n \\ \tau \in \mathscr{A}_n}} \Gamma(\alpha)\, \Delta(\tau) + \sum_{\substack{\alpha \in \mathscr{C}_n \\ \sigma \in \mathscr{B}_n}} H(\alpha, \sigma)\, E(\alpha, \sigma) \\
&= 1 + \sum_{\substack{\alpha \in \mathscr{A}_n \\ \sigma \in \mathscr{B}_n}} \Gamma(\alpha)\, \Delta(\alpha^{-1}\sigma) + \sum_{\substack{\alpha \in \mathscr{B}_n \\ \sigma \in \mathscr{B}_n}} \Gamma(\alpha)\, \Delta(\alpha^{-1}\sigma) \\
&\quad + \sum_{\substack{\alpha \in \mathscr{C}_n \\ \sigma \in \mathscr{B}_n}} H(\alpha, \sigma)\, E(\alpha, \sigma) \\
&= 1 + \sum_{\substack{\alpha \in \mathscr{T}_n \\ \sigma \in \mathscr{B}_n}} H(\alpha, \sigma)\, E(\alpha, \sigma) = 1 + \sum_{\sigma \in \mathscr{B}_n} Q_\sigma^{(1,1)} && \text{(by (8))} \\
&= 1 + 0 && \text{(by (9))} \\
&= 1.
\end{aligned}
$$

Further

$$
\begin{aligned}
(BA)_{12} &= \sum_{\sigma \in \mathscr{A}_n} Q_\sigma^{(1,2)} && \text{(by (7))}\\
&= \sum_{\substack{(\alpha,\beta)\in \mathscr{D}_n\\ \sigma \in \mathscr{A}_n}} T((\alpha,\beta),\sigma) && \text{(by (9))}\\
&= \sum_{\substack{(\alpha,\beta)\in \mathscr{D}_n\\ \sigma \in \mathscr{A}_n}} T(((\alpha,\beta),\sigma)\Psi) && \text{(by (5))}\\
&= \sum_{\substack{(\alpha,\beta)\in \mathscr{D}_n\\ \sigma \in \mathscr{B}_n}} T((\alpha,\beta),\sigma) && \text{(since } \Psi \text{ is a bijection from } \mathscr{D}_n \times \mathscr{A}_n \text{ onto } \mathscr{D}_n \times \mathscr{B}_n)\\
&= \sum_{\sigma \in \mathscr{B}_n} Q_\sigma^{(1,2)} && \text{(by (9))}\\
&= 0. && \text{(by (7))}
\end{aligned}
$$

This completes the proof. ∎

5. Stability in Matrix Semigroups

We have shown that the monoid of $n \times n$ matrices over a commutative semiring has the property that every right-invertible (or left-invertible) element is invertible. M. P. Schützenberger suggested that we study a related property, called *stability*. A monoid M is said to be stable if for all a, b in M

$$Ma \subset Mb \text{ and } bM \subset aM \text{ implies } aM = bM \text{ and } Ma = Mb.$$

(See Lallement [1, p. 36], where stability is defined in a slightly different way.) Every finite monoid has this property. If a monoid is stable, then the equation $ab = 1$ implies $ba = 1$. Indeed, if $ab = 1$, then $1 \in aM$ and consequently $M = 1M \subset aM$. Since $Ma \subset M = M1$, stability implies that $M = Ma$. Thus $1 = xa$ for some x in M. Finally, $x = x(ab) = (xa)b = b$, so $ba = 1$.

If R is a commutative ring, then $R^{n\times n}$ is stable. Indeed, suppose that A and B are elements of $R^{n\times n}$ such that $A \cdot R^{n\times n} \subset B \cdot R^{n\times n}$ and $R^{n\times n} \cdot B \subset R^{n\times n} \cdot A$. Then there exist matrices X, Y in $R^{n\times n}$ such that $A = BY$ and $B = XA$, and consequently $A = X^kAY^k$, $B = X^kBY^k$ for all $k \geqslant 0$. By the Cayley–Hamilton Theorem, there exist $\alpha_0, \ldots, \alpha_{n-1}$ in R such that

$$Y^n = \alpha_{n-1}Y^{n-1} + \cdots + \alpha_0$$

and thus

$$Y^{2n} = \alpha_{n-1}Y^{2n-1} + \cdots + \alpha_0 Y^n.$$

It follows that

$$A = X^{2n} A Y^{2n} = \sum_{0 \leqslant i \leqslant n-1} \alpha_i X^{2n} A Y^{n+i} = \sum_{0 \leqslant i \leqslant n-1} \alpha_i X^{n-i-1} X^{n+i} (XA) Y^{n+i}$$

$$= \sum_{0 \leqslant i \leqslant n-1} \alpha_i X^{n-i-1} (X^{n+i} B Y^{n+i}) = \left(\sum_{0 \leqslant i \leqslant n-1} \alpha_i X^{n-i-1} \right) B.$$

Thus A is in the left ideal $R^{n \times n} B$ generated by B and consequently $R^{n \times n} A = R^{n \times n} B$. A parallel argument shows that the right ideals $AR^{n \times n}$ and $BR^{n \times n}$ are equal. Thus $R^{n \times n}$ is stable.

The following example, due to J. E. Pin, shows that if R is a commutative semiring then $R^{n \times n}$ is not necessarily stable: let $R = \mathbb{Q}_+$, the semiring of non-negative rational numbers, and let

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}.$$

Then $A = BC$ and $B = DA$. If $R^{2 \times 2}$ were stable, there would exist a matrix E in $R^{2 \times 2}$ such that $B = AE$. However, if the equation $B = AE$ holds in $Q^{2 \times 2}$ then $E = A^{-1} B = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 2 \end{smallmatrix} \right)$, which is not in $R^{2 \times 2}$, thus $R^{2 \times 2}$ is not stable.

REFERENCE

1. G. LALLEMENT, "Semigroups and Combinatorial Applications," Wiley, New York, 1979.