TRANSITIVE CLOSURE AND RELATED SEMIRING PROPERTIES VIA ELIMINANTS

S. Kamal Abdali^{*}

Computer Science and Engineering Department University of Petroleum and Minerals Dhahran, Saudi Arabia B. David Saunders[†] Department of Mathematical Sciences Rensselaer Polytechnic Institute Troy, NY 12181, USA

February 26, 2006

Abstract

Closed semirings are algebraic structures that provide a unified approach to a number of seemingly unrelated problems of computer science and operations research. For example, semirings can be used to describe the algebra related to regular expressions, graph-theoretical path problems, and linear equations. We present a new axiomatic formulation of semirings. We introduce the concept of eliminant, which simplifies the treatment of closed semirings considerably and yields very simple proofs of otherwise difficult theorems. We use eliminants to define matrix closure, formulate closure algorithms, and prove their correctness.

Key words *-semirings, eliminants, asterates, transitive closure, iterative systems, linear systems.

1 Introduction

There are a number of important problems in computer science and operations research which had earlier been studied separately as seemingly unrelated problems, but have recently been recognized to be instances of the same general problem. Examples of these include various 'path problems' such as the determination of the shortest or the most reliable path or the path with the largest capacity, or the enumeration of all paths between each pair of points in a network (see the bibliographies on path problems [5, 12]). Other examples are cut-set enumeration, transitive closure of binary relations [14], finding the regular expression to describe the language accepted by a finite automaton [11], and compiled code optimization and data flow analysis [9].

The use of semirings as a unified approach to path problems was undertaken by a number of people (see [13, 16] for representative examples), and the problems were formulated in such a way that the optimal path computation became equivalent to the asteration (closure) of a matrix with elements from a suitable semiring. Later, Backhouse and Carré pointed out the similarities between the asteration or matrices over

^{*}Present Affiliation: Computer Research Lab, Tektronix, Inc., Beaverton, OR 97077, USA. This work was done while the author was visiting the University of Petroleum and Minerals, Dhahran, Saudi Arabia, on leave of absence from Rensselaer Polytechnic Institute, Troy, NY, USA.

[†]Present Affiliation: Computer Science Department, University of Delaware, Newark, DE 19711, USA. This author was partially supported by NSF Grant MCS-7909158.

semirings and the solution of linear systems of equations in ordinary algebra. It then became quite clear that, for example, the McNaughton-Yamada algorithm for regular expressions [11], Warshall's transitive closure algorithm [15], and Floyd's shortest path algorithm [6] were quite similar to the Gauss-Jordan elimination method in linear algebra, and that the Ford-Fulkerson shortest path algorithm [7] was similar to the Gauss-Seidel iteration method.

Under different names and with differing postulates, a number of formulations have been proposed for the semiring structure needed to express generalized path problems (see [3] fpr extensive bibliographic notes on this literature). For most path problems, the operation of asteration (closure), so important in the case of matrices over a semiring, was trivial for the elements of the semiring themselves. As a result, earlier definitions of semirings (e.g., [13, 16]) did not include or emphasize the asteration of elements. The later formulations (e.g., [?, 2]) generalized the structure so as to represent regular expressions also. But by assuming addition to be idempotent or by some other too strong conditions, these structures could not encompass real or complex linear algebra. Thus, in spite of a close similarity between then, path problems and the problem of solving linear equations still could not be unified completely as instances of the same general problem. The final step of incorporating path problems, regular expressions, and linear systems in real numbers into a single framework has been undertaken by Lehmann[10] and Tarjan[14].

A difficulty with most of the earlier formulations was the lack of precision in their treatment of the operation of matrix asteration (closure). This operation was defined in terms of (1) an implicit solution to an equation or (2) an explicit formula containing infinite summation or (3) the result of executing an algorithm. In each case, it was difficult to prove the properties of asterates (closures) rigorously, for example, to show that two different algorithms for asteration produced the same result. Lehmann [10] gave an explicit definition of asterates of matrices, and proved that the algorithms essentially equivalent to Gauss-Jordan and Gaussian elimination techniques compiled matrix asterates correctly.

The main contribution of our paper is to introduce the concept of eliminant, which bears some resemblance to the linear algebraic concept of determinant. Eliminants serve to represent the quantities produced during the execution of elimination algorithms in very natural, compact, and suggestive forms. Using eliminants, we have been able to define matrix asterates as well as to prove the correctness of asteration algorithms much more simply than in the literature. Several otherwise difficult proofs have been reduced to elementary consequences of the properties of eliminants.

Our formulation of semirings is very similar to, but slightly less general than that of Lehmann [10], because we include the axiom a.0 = 0.a = 0, which he does not. We feel that this axiom can be added without any sacrifice in the applicability of semirings to practical problems. On the other hand, any theoretical loss is more than adequately compensated by the resulting simplicity and beauty of the eliminant approach.

This paper is divided into seven sections. Section 2 defines *-semirings as an algebraic structure. Section 3 introduces matrix operations over semirings. Section 4 defines eliminants and presents a number of their interesting properties. Section 5 uses eliminants to give a very simple definition of matrix asterates. It also shows that the definition is suitable by proving that the relevant semiring axiom is satisfied by the defined asterates. Section 6 then describes two algorithms for computing the asterate of a matrix, and shows their correctness. The algorithms are just the *-semiring versions of the Gauss-Jordan and Gaussian elimination algorithms for matrix inversion. Finally, Section 7 presents an explicit solution for a linear system of equations.

2 Semirings

Definition 2.1. A *-*semiring* is a system $(S, +, \cdot, *, 0, 1)$ in which *S* is a set closed with respect to the binary operations + (addition) and \cdot (multiplication) and the unary operation * (asteration), 0 and 1 are elements of *S*, and the following laws are satisfied:

(1)	a + (b+c) = (a+b) + c,	addition is associative,
(2)	a+b=b+a,	addition is commutative,
(3)	a + 0 = 0,	0 is the identity for addition,
(4)	$(a \cdot b) \cdot c = a \cdot (b \cdot c),$	multiplication is associative,
(5)	$a \cdot 1 = 1 \cdot a = a,$	1 is the identity for multiplication,
(6)	$a \cdot 0 = 0 \cdot a = 0,$	0 is a zero for multiplication,
(7)	$a \cdot (b+c) = a \cdot b + a \cdot c,$	multiplication is left and,
(8)	$(a+b) \cdot c = a \cdot c + b \cdot c,$	right distributive over addition.
(9)	$a^* = a \cdot a^* + 1 = a^* \cdot a + 1.$	

The system $(S, +, \cdot, 0, 1)$ is called a *semiring* if S is possibly not closed with respect to * $(a^*$ is not defined for some or all a in S), but the laws (1) through (8) still hold.

For the most part, we will denote multiplication by juxtaposition as is customary.

Note: In the literature, asteration is usually called *closure*, and a *-semiring is usually called *closed* semiring. We prefer the term asteration to avoid such awkward statements as "... is closed with respect to closure". The term *asterate* of *a* for a^* was coined by Conway [4].

Some simple examples of *-semirings are shown in Table 1. Similar tabulations have often been given (cf. [2, 3, 10]).

S	a+b	$a \cdot b$	a^*	0	1	Description	Application
{0,1}	$a \lor b$	$a \wedge b$	1	0	1	Boolean values	Reachabilty in
							graphs; reflexive
							and transitive
							closure of binary
							relations
$\mathbf{R}^+ \cup \{\infty\}$	$\min\{a,b\}$	a+b	0	∞	0	Real numbers	Shortest paths
						augmented with the	
						element ∞	
$\mathbf{R}^+ \cup \{\infty\}$	$\max\{a,b\}$	$\min\{a,b\}$	∞	0	∞	Nonnegative real	Largest capacity
						numbers augmented	paths
						with the element ∞	
[0,1]	$\max\{a,b\}$	ab	1	0	1	Real numbers between	Most reliable
						0 and 1 inclusive	paths
$\mathbf{R} \cup \{\infty\}$	a+b	ab	1/(1-a)	0	1	Real numbers	Solution of linear
			if $a \neq 1$;			augmented with the	equations
			$1^* = \infty$,			element ∞	
			$\infty^* = \infty$				

Table 1: Some examples of semirings

3 Matrices over semirings

The set of all $n \times n$ matrices over a *-semiring $S = (S, +, \cdot, *, 0, 1)$ can itself be made into a semiring or *semiring by suitably defining $+, \cdot, *, 0$, and 1 for it. We define addition and multiplication of $n \times n$ matrices in the usual way, and 0 = O, the matrix with all entries zero, $1 = I = (\delta_{ij})$, the Kronecker δ . The size, n, of O and I is to be inferred from the context.

It is now an easy matter to verify that the set of all $n \times n$ matrices over a *-semiring, together with the above defined addition, multiplication, O and I, forms a semiring.

The asteration of matrices is best defined via eliminants which we introduce next.

4 Eliminants and selects

The theorems of this section provide some basic identities for the manipulation of eliminants which will be used in the subsequent sections.

Definition 4.1. Given an $n \times n$ matrix

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix},$$

we define the *eliminant* of A, written elim(A) or

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix},$$

as follows: For n = 1 and n = 2, the value is given explicitly:

$$|a| = a$$
, and $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = d + ca^*b$

For $n \ge 3$, the value is specified in terms of a smaller order eliminant,

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} b_{11} & \dots & b_{1,n-1} \\ \vdots & & \vdots \\ b_{n-1,1} & \dots & b_{n-1,n-1} \end{vmatrix}$$

where

$$b_{ij} = \begin{vmatrix} a_{11} & a_{1,j+1} \\ a_{i+1,1} & a_{i+1,j+1} \end{vmatrix}, \quad 1 \le i, j \le n-1.$$

Example

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = \begin{vmatrix} a & b \\ d & e \end{vmatrix} \begin{vmatrix} a & c \\ d & f \end{vmatrix} \\ \begin{vmatrix} a & b \\ g & h \end{vmatrix} \begin{vmatrix} a & c \\ g & i \end{vmatrix} = \begin{vmatrix} e + da^*b & f + da^*c \\ h + ga^*b & i + ga^*c \end{vmatrix}$$
$$= i + ga^*c + (h + ga^*b)(e + da^*b)^*(f + da^*c).$$

Definition 4.2. Given an $n \times n$ matrix

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix},$$

we define the k, i, j-select of A, written \tilde{A}_{ij}^k , for $1 \le i, j \le n$ and $0 \le k \le n$, to be the eliminant of the matrix obtained by selecting the first k rows followed by the *i*th and the first k column followed by the *j*th; in symbols,

$$\tilde{A}_{ij}^{k} = \begin{vmatrix} a_{11} & \dots & a_{1k} & a_{1j} \\ \vdots & & \vdots & \vdots \\ a_{k1} & \dots & a_{kk} & a_{kj} \\ a_{i1} & \dots & a_{ik} & a_{ij} \end{vmatrix}, \quad 1 \leq i, j \leq n, \quad 0 \leq k \leq n.$$

Note that, for k = 0, $\tilde{A}_{ij}^k = |a_{ij}| = a_{ij}$. For an $n \times n$ matrix A, \tilde{A}_{nn}^{n-1} is the same as $\operatorname{elim}(A)$, so that $\operatorname{elim}(A) = |\tilde{A}_{nn}^{n-1}|$. Furthermore, Definition 4.1 gives

$$\operatorname{elim}(A) = \begin{vmatrix} \tilde{A}_{22}^{1} & \tilde{A}_{23}^{1} & \dots & \tilde{A}_{2n}^{1} \\ \tilde{A}_{32}^{1} & \tilde{A}_{33}^{1} & \dots & \tilde{A}_{3n}^{1} \\ \vdots & \vdots & & \vdots \\ \tilde{A}_{n2}^{1} & \tilde{A}_{n3}^{1} & \dots & \tilde{A}_{nn}^{1} \end{vmatrix}.$$

A general relation embracing the above two as extreme cases is given by the next theorem.

Theorem 4.3. *Given an* $n \times n$ *matrix* A *and an integer* r, $1 \le r \le n-1$, *let* B *be the* $(n-r) \times (n-r)$ *matrix* specified by

$$b_{ij} = \hat{A}_{r+i,r+j}^r, \quad 1 \leq i, j \leq n-r.$$

Then

$$\operatorname{elim}(A) = \operatorname{elim}(B).$$

Note: The construction of b_{ij} from A can be pictorially represented in terms of a partitioning of A as follows:

$$A = \begin{bmatrix} x & Y \\ \hline Z & W \end{bmatrix} \stackrel{r \text{ rows}}{\stackrel{n-r \text{ rows}}{n-r \text{ rows}}} , \qquad b_{ij} = \begin{vmatrix} X & Y_{*j} \\ Z_{i*} & w_{ij} \end{vmatrix}$$

where Z_{i*} and Y_{*j} are the *i*th row and *j*th column of Z and Y, respectively.

Before proving the theorem, let us look at an example. For a 4×4 matrix partitioned by taking r = 2, the theorem asserts that 7 | | 7 7 | . .

$$\begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{bmatrix} = \begin{bmatrix} a & b & c \\ e & f & g \\ i & j & k \\ e & f & g \\ e & f & g \\ m & n & o \\ \end{bmatrix} \begin{bmatrix} a & b & c \\ e & f & g \\ m & n & o \\ m & n & p \\ \end{bmatrix}$$

On the other hand, by definition, the left-hand side equals

$\left \begin{array}{cc}a&b\\e&f\end{array}\right $	$\left \begin{array}{cc}a&c\\e&g\end{array}\right $	a d e h
$\left \begin{array}{cc}a&b\\i&j\end{array}\right $	$\left \begin{array}{cc}a&c\\i&k\end{array}\right $	$\left \begin{array}{cc}a&d\\i&l\end{array}\right .$
a b m n	a c m o	$\begin{vmatrix} a & d \\ m & p \end{vmatrix}$

Of course, the latter equality is also obtained from the theorem by taking r = 1.

Proof of Theorem 4.3. We prove the theorem by induction on *r*. The case r = 1 immediately follows from Definition 4.1. For r = s + 1, let *B* be the $(n - r) \times (n - r)$ matrix given by

$$b_{ij} = \tilde{A}_{r+i,r+j}^r, 1 \leq i, j \leq n-r.$$

We need to show that $\operatorname{elim}(A) = \operatorname{elim}(B)$. By the induction hypothesis, $\tilde{A}_{r+i,r+j}^r$ or $\tilde{A}_{s+1+i,s+1+j}^{r+1}$ can be expanded, giving

$$b_{ij} = \left| \begin{array}{cc} \tilde{A}_{s+1,s+1}^{s} & \tilde{A}_{s+1,s+1+j}^{s} \\ \tilde{A}_{s+1+i,s+1}^{s} & \tilde{A}_{s+1+i,s+1+j}^{s} \end{array} \right|$$

Each element of the $(n - s - 1) \times (n - s - 1)$ matrix *B* is now a 2 × 2 eliminant, and Definition 4.1 is applicable (in reverse) to *B*. Specifically, we get

$$\operatorname{elim}(B) = \operatorname{elim}(C),$$

where *C* is an $(n-s) \times (n-s)$ matrix with elements $c_{ij} = \tilde{A}^s_{s+i,s+j}$. Using the induction hypothesis again, we obtain

 $\operatorname{elim}(C) = \operatorname{elim}(A).$

Some easily proven properties of eliminants are given by the next three theorems.

Theorem 4.4. A common premultiplier of the last row, or postmultiplier of the last column, can be factored out of an eliminant.

Theorem 4.5. Eliminants which are equal element-by-element in all positions except in the last row (respectively column) can be added by adding their last rows (respectively columns) element-by-element.

Theorem 4.6. A constant can be added to an eliminant by adding that constant to the last diagonal element of the eliminant.

The following equalities illustrate the use of the above theorems:

$$\begin{vmatrix} a & b & c \\ d & e & f \\ mg & mh & mi \end{vmatrix} = m \cdot \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix},$$

$$\begin{vmatrix} a & b & cm \\ d & e & fm \\ g & h & im \end{vmatrix} = \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} \cdot m,$$

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} + \begin{vmatrix} a & b \\ e & f \end{vmatrix} = \begin{vmatrix} a & b \\ c + e & d + f \end{vmatrix},$$

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} + \begin{vmatrix} a & e \\ e & f \end{vmatrix} = \begin{vmatrix} a & b + e \\ c & d + f \end{vmatrix},$$

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} + k = \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i + k \end{vmatrix}.$$

Theorem 4.7. If the last row (respectively column) of an eliminant consists of zeros except, possibly, in the diagonal position, then the eliminant equals this last diagonal element. In symbols:

$$\begin{vmatrix} a_{11} & \cdots & a_{1,n-1} & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,n-1} & a_{n-1,n} \\ 0 & \cdots & 0 & a_{nn} \end{vmatrix} = a_{nn} = \begin{vmatrix} a_{11} & \cdots & a_{1,n-1} & 0 \\ \vdots & \vdots & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,n-1} & 0 \\ a_{n1} & \cdots & a_{n,n-1} & a_{nn} \end{vmatrix}$$

Proof. We will prove the theorem for the row case by induction on n. The proof for the column case is similar.

Basis step (n = 1): $|a_{11}| = a_{11}$. *Inductive step* (n > 1):

$$\begin{vmatrix} a_{i1} & \cdots & a_{1,n-1} & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,n-1} & a_{n-1,n} \\ 0 & \cdots & 0 & a_{nn} \end{vmatrix} = \begin{vmatrix} b_{11} & \cdots & b_{1,n-1} \\ \vdots & \vdots \\ b_{n-1,1} & \cdots & b_{n-1,n-1} \end{vmatrix},$$
(1)

where

$$b_{ij} = \begin{vmatrix} a_{11} & a_{1,j+1} \\ a_{i+1,1} & a_{i+1,j+1} \end{vmatrix}$$

Hence, for all $j, 1 \leq j \leq n-2$,

$$b_{n-1,j} = \left| \begin{array}{cc} a_{11} & a_{1,j+1} \\ a_{n1} & a_{n,j+1} \end{array} \right| = \left| \begin{array}{cc} a_{11} & a_{1,j+1} \\ 0 & 0 \end{array} \right| = 0.$$

Thus, all off-diagonal elements of the last row in the right-hand side eliminant in (1) are zero. Therefore, by the induction hypothesis, the eliminant equals $b_{n-1,n-1}$, which is

$$\begin{vmatrix} a_{11} & a_{1n} \\ a_{n1} & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{1n} \\ 0 & a_{nn} \end{vmatrix} = a_{nn} + 0.a_{11}^* a_{1n} = a_{nn}.$$

Theorem 4.8. If, in an $n \times n$ eliminant, the last row consists of zeros except for a one in column i, i < n, then the last row can be replaced by the *i*-th row. In symbols:

a_{11}	•••	a_{1i}	•••	a_{1n}		a_{11}	•••	a_{1i}	•••	a_{1n}
:		:		÷		:		÷		÷
a_{i1}	•••	a_{ii}	•••	a_{in}	_	a_{i1}	•••	a_{ii}	•••	a_{in}
÷		:		÷		:		:		÷
$a_{n-1,1}$	•••	$a_{n-1,i}$		$a_{n-1,n}$		$a_{n-1,1}$	•••	$a_{n-1,i}$	•••	$a_{n-1,n}$
0	• • •	1	•••	0		a_{i1}	•••	a_{ii}	• • •	a_{in}

Note: The right-hand side can also be written as \tilde{A}_{in}^{n-1} . With the subscript (i^*) denoting the *i*th row, the theorem may be rephrased as follows: If, for an $n \times n$ matrix A, the last row is the *i*th row of the identity matrix, $A_{n^*} = I_{i^*}$ for some i < n, then $\operatorname{elim}(A) = \tilde{A}_{in}^{n-1}$.

Proof of Theorem 4.8. The proof follows by induction on *n*. For n = 1, the result is vacuously true. For n = 2, the only value for *i* is 1. In this case,

$$\begin{vmatrix} a_{11} & a_{12} \\ 1 & 0 \end{vmatrix} = 0 + 1(a_{11})^* a_{12} = a_{11}^* a_{12} = (1 + a_{11}a_{11}^*)a_{12}$$
$$= a_{12} + a_{11}a_{11}^* a_{12} = \begin{vmatrix} a_{11} & a_{12} \\ a_{11} & a_{12} \end{vmatrix}.$$

For the induction step, let n > 2. Using the definition of eliminants, the left-hand side can be rewritten as

This is an order n-1 eliminant in which the last row is $I_{i-1,*}$ (0's, but 1 in the (i-1)st position). By the induction hypothesis, we can replace the last row by row i-1. The resulting eliminant is seen to be equivalent to the right-hand side of the theorem by virtue of Definition 4.1.

The analogous theorem for the column case is the following.

Theorem 4.9. If, in an $n \times n$ eliminant, the last column consists of zeros except for a one in row j, j < n, then the last column may be replaced by the *j*th column.

Note: With the subscript *j denoting the *j*th column, the theorem may be rephrased as follows: If, for an $n \times n$ matrix A, $A_{*n} = I_{*j}$ for some j < n, then $\operatorname{elim}(A) = \tilde{A}_{nj}^{n-1}$.

Theorem 4.10. For any $n \times n$ matrix A,

$$\begin{array}{ll} (1) & \tilde{A}_{ij}^{k} = \tilde{A}_{ij}^{k-1} + \tilde{A}_{ik}^{k-1} (\tilde{A}_{kk}^{k-1})^{*} \tilde{A}_{kj}^{k-1}, & 1 \leq i, j, k \leq n. \\ (2) & \tilde{A}_{ik}^{k} = \tilde{A}_{ik}^{k-1} (\tilde{A}_{kk}^{k-1})^{*}, & 1 \leq i, k \leq n. \\ (3) & \tilde{A}_{kj}^{k} = (\tilde{A}_{kk}^{k-1})^{*} \tilde{A}_{kj}^{k-1}, & 1 \leq j, k \leq n. \\ (4) & \tilde{A}_{ij}^{k} = \tilde{A}_{ij}^{k-1} + \tilde{A}_{ik}^{k-1} \tilde{A}_{kj}^{k} = \tilde{A}_{ij}^{k-1} + \tilde{A}_{ik}^{k} \tilde{A}_{kj}^{k-1}, & 1 \leq i, j, k \leq n. \\ (5) & \tilde{A}_{ij}^{k} = \tilde{A}_{ij}^{m} + \sum_{p=m+1}^{k} \tilde{A}_{ip}^{m} \tilde{A}_{pj}^{k}, & 1 \leq i \leq m \leq k \leq n, \ 1 \leq j \leq n. \end{array}$$

Proof. (1) For the case k = 1, the result is thus verified:

$$\tilde{A}_{ij}^{1} = \begin{vmatrix} a_{11} & a_{1j} \\ a_{i1} & a_{ij} \end{vmatrix} = a_{ij} + a_{i1}a_{11}^{*} + a_{ij} = \tilde{A}_{ij}^{0} + \tilde{A}_{i1}^{0}(\tilde{A}_{11}^{0})^{*}\tilde{A}_{1j}^{0}.$$

Now, let $1 < k \le n$, and consider the eliminant

$$\tilde{A}_{ij}^{k} = \begin{vmatrix} a_{11} & \cdots & a_{1,k-1} & a_{1k} & a_{1j} \\ \vdots & \vdots & \vdots & \vdots \\ a_{k-1,1} & \cdots & a_{k-1,k-1} & a_{k-1,k} & a_{k-1,j} \\ \hline a_{k1} & \cdots & a_{k,k-1} & a_{kk} & a_{kj} \\ a_{i1} & \cdots & a_{i,k-1} & a_{ik} & a_{ij} \end{vmatrix}.$$

By Theorem 4.3, this can be rewritten as

$$\begin{vmatrix} a_{11} & \cdots & a_{1,k-1} & a_{1k} \\ \vdots & \vdots & \vdots \\ a_{k-1,1} & \cdots & a_{k-1,k-1} & a_{k-1,k} \\ a_{k1} & \cdots & a_{k,k-1} & a_{kk} \end{vmatrix} \begin{vmatrix} a_{11} & \cdots & a_{1,k-1} & a_{1j} \\ \vdots & \vdots & \vdots \\ a_{k-1,1} & \cdots & a_{k,k-1} & a_{kk} \end{vmatrix} \begin{vmatrix} a_{11} & \cdots & a_{k-1,k-1} & a_{k-1,j} \\ a_{k1} & \cdots & a_{k,k-1} & a_{kj} \end{vmatrix}$$
$$\begin{vmatrix} a_{11} & \cdots & a_{1,k-1} & a_{1k} \\ \vdots & \vdots & \vdots \\ a_{k-1,1} & \cdots & a_{k-1,k-1} & a_{k-1,k} \\ a_{i1} & \cdots & a_{i,k-1} & a_{ik} \end{vmatrix} \begin{vmatrix} a_{11} & \cdots & a_{1,k-1} & a_{1j} \\ \vdots & \vdots & \vdots \\ a_{k-1,1} & \cdots & a_{i,k-1} & a_{k-1,k} \\ a_{i1} & \cdots & a_{i,k-1} & a_{ij} \end{vmatrix}$$
$$= \tilde{A}_{ij}^{k-1} + \tilde{A}_{ik}^{k-1} (\tilde{A}_{kk}^{k-1})^* \tilde{A}_{kj}^{k-1}.$$

(2) $\tilde{A}_{ik}^{k} = \tilde{A}_{ik}^{k-1} + \tilde{A}_{ik}^{k-1} (\tilde{A}_{kk}^{k-1})^{*} \tilde{A}_{kk}^{k-1} = \tilde{A}_{ik}^{k-1} (1 + (\tilde{A}_{kk}^{k-1})^{*} \tilde{A}_{kk}^{k-1}) = \tilde{A}_{ik}^{k-1} (\tilde{A}_{kk}^{k-1})^{*}.$

The proof of part (3) is similar. Part (4) is obvious from (1), (2), and (3).

(5) This part follows by backward induction on *m*. For m = k, the result is immediate. For the inductive step, let $1 \le m \le k$. We derive the result for m - 1:

$$\begin{split} \tilde{A}_{ij}^{m-1} + &\sum_{p=m}^{k} \tilde{A}_{ip}^{m-1} \tilde{A}_{pj}^{k} \\ &= \tilde{A}_{ij}^{m-1} + \tilde{A}_{im}^{m-1} \tilde{A}_{mj}^{k} + \sum_{p=m+1}^{k} \tilde{A}_{ip}^{m-1} \tilde{A}_{pj}^{k} \\ &= \tilde{A}_{ij}^{m-1} + \tilde{A}_{im}^{m-1} \left(\tilde{A}_{mj}^{m} + \sum_{p=m+1}^{k} \tilde{A}_{mp}^{m} \tilde{A}_{pj}^{k} \right) + \sum_{p=m+1}^{k} \tilde{A}_{ip}^{m-1} \tilde{A}_{pj}^{k}, \end{split}$$

using the induction hypothesis,

$$= \left(\tilde{A}_{ij}^{m-1} + \tilde{A}_{im}^{m-1}\tilde{A}_{mj}^{m}\right) + \sum_{p=m+1}^{k} \left(\tilde{A}_{im}^{m-1}\tilde{A}_{mp}^{m} + \tilde{A}_{ip}^{m-1}\right)\tilde{A}_{pj}^{k}$$
$$= \tilde{A}_{ij}^{m} + \sum_{p=m+1}^{k} \tilde{A}_{ip}^{m}\tilde{A}_{pj}^{k} \quad \text{using part (4)}$$
$$= \tilde{A}_{ij}^{k} \quad \text{by the induction hypothesis.} \quad \Box$$

5 Matrix asterates

We are now in a position to define asterates for matrices over a *-semiring. We present a formal definition of A^* , and then justify it by showing that $A^* = AA^* + I = A^*A + I$.

Definition 5.1. Give an $n \times n$ matrix A, the asterate of A, denoted A^* , is the $n \times n$ matrix (b_{ij}) given by

$$b_{ij} = \begin{vmatrix} a_{11} & \cdots & a_{1i} & \cdots & a_{1j} & \cdots & a_{1n} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{i1} & \cdots & a_{ii} & \cdots & a_{ij} & \cdots & a_{in} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{j1} & \cdots & a_{ji} & \cdots & a_{jj} & \cdots & a_{jn} & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{ni} & \cdots & a_{nj} & \cdots & a_{nn} & 0 \\ 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 & 0 \end{vmatrix}, \quad 1 \leq i, j \leq n.$$

Note: The above eliminant is obtained by bordering A at right and bottom; the bordering elements are all zero, except for 1's in row j and column i. Thus, we can also write

$$b_{ij} = \left| \begin{array}{c} A & I_{*j} \\ \hline I_{i*} & 0 \end{array} \right|.$$

Theorem 5.2. With A^* defined as above, $A^* = AA^* + I = A^*A + I$.

Proof. We will prove $A^* = AA^* + I$; the other part can be proven in a similar way. Let $C = AA^* + I$. Then, for 1 < i, j < n, we have

$$c_{ij} = \delta_{ij} + \sum_{k=1}^{n} a_{ik} b_{kj}$$
, where $\delta_{ij} = 1$ if $i = j$, and 0 otherwise.

We can transform the right-hand expression as follows. First, we apply Theorem 4.4 to move the premultiplier a_{ik} into the *k*th position in the bottom row of b_{kj} . Next, we use Theorem 4.5 to carry out the summation of the *k* eliminants into a single eliminant. Finally, we use Theorem 4.6 to add the constant term δ_{ij} to the diagonal element in the bottom row. The result is

$$c_{ij} = \begin{vmatrix} a_{11} & \cdots & a_{1k} & \cdots & a_{1n} & 0 \\ \vdots & & \vdots & & \vdots & \vdots \\ a_{j1} & \cdots & a_{jk} & \cdots & a_{jn} & 1 \\ \vdots & & \vdots & & \vdots & \vdots \\ a_{n1} & \cdots & a_{nk} & \cdots & a_{nn} & 0 \\ a_{i1} & \cdots & a_{ik} & \cdots & a_{in} & \delta_{ij} \end{vmatrix}.$$

Consider row *i* in the above eliminant. The last element of this row is 1 if i = j and 0 otherwise, that is, its last element is δ_{ij} . It follows that the last row and row *i* are equal in the above eliminant. By Theorem 4.8, we can replace that last row by I_{*i} . But, then, the eliminant is b_{ij} . Thus, $b_{ij} = c_{ij}$ and $A^* = C = AA^* + I$.

Theorem 5.3. For an $n \times n$ matrix $A, A^* = (b_{ij})$ where

$$b_{ij} = \tilde{A}^n_{ij} + \delta_{ij}, \quad 1 \leq i, j \leq n.$$

Proof. We use the definition of A^* and Theorems 4.6, 4.8, and 4.9:

$$b_{ij} = \left| \frac{A |I_{*j}|}{I_{i*} |0|} \right| = \left| \frac{A |I_{*j}|}{A_{i*} |\delta_{ij}|} \right| = \left| \frac{A |I_{*j}|}{A_{i*} |0|} \right| + \delta_{ij}$$
$$= \left| \frac{A |A_{*j}|}{A_{i*} |a_{ij}|} \right| + \delta_{ij} = \tilde{A}_{ij}^n + \delta_{ij}. \quad \Box$$

Of course, the equality proved in this theorem could have been used alternatively to define matrix asterate.

6 Matrix asteration algorithms

In many applications of *-semirings, one is required to compute the asterate A^* of A. One way to accomplish this is to use the following algorithm which was given in its present form by McNaughton and Yamada [11]. This algorithm is equivalent to the Gauss-Jordan elimination method for inverting matrices in linear algebra.

Algorithm 6.1

Input : An $n \times n$ matrix A. Output: An $n \times n$ matrix S. Claim : $S = A^*$.

begin

1. $B^{(0)} := A;$ 2. **for** k := 1 **to** n **do**

3. **for**
$$i := 1$$
 to n **do**
4. **for** $j := 1$ **to** n **do**
5. $b_{ij}^{(k)} := b_{ij}^{(k-1)} + b_{ik}^{(k-1)} (b_{kk}^{(k-1)})^* b_{kj}^{(k-1)};$
6. $S := B^{(n)} + I$
end

Theorem 6.2 (Correctness of Algorithm 6.1). When Algorithm 6.1 terminates, $S = A^*$.

Proof. We will first prove by induction on k that the matrices $B^{(k)}$ computed in steps 1 to 5 satisfy the relation

$$\begin{split} b_{ij}^{(k)} &= \tilde{A}_{ij}^{k}, \quad 0 \leqslant k \leqslant n, \quad 1 \leqslant i, j \leqslant n. \\ \text{For } k &= 0, \; b_{ij}^{(0)} = a_{ij} = \tilde{A}_{ij}^{0}. \\ \text{For } 0 < k \leqslant n, \\ b_{ij}^{(k)} &= b_{ij}^{(k-1)} + b_{ik}^{(k-1)} \left(b_{kk}^{(k-1)} \right)^{*} b_{kj}^{(k-1)} \quad \text{from step 5} \\ &= \tilde{A}_{ij}^{k-1} + \tilde{A}_{ik}^{k-1} \left(\tilde{A}_{kk}^{k-1} \right)^{*} \tilde{A}_{kj}^{k-1} \quad \text{by the induction hypothesis} \\ &= \tilde{A}_{ij}^{k} \quad \text{by Theorem 4.10 (1).} \end{split}$$

Now, from step 6,

$$s_{ij} = b_{ij}^{(n)} + \delta_{ij}$$
, where $\delta_{ij} = 1$ if $i = j$, and 0 otherwise,
 $= \tilde{A}_{ij}^n + \delta_{ij}$.

Thus, $S = A^*$ by Theorem 5.3.

Algorithm 6.1 requires *n* intermediate $n \times n$ matrices in addition to input and output matrices. It is possible to do the asteration in place without requiring any other matrix storage by rescheduling the computations so that no entry is modified before its use. Specifically, we can use the following algorithm.

Algorithm 6.3 (In place matrix asteration)

Input : An $n \times n$ matrix A. *Output*: A is overwritten to contain its own asterate on termination.

```
begin

for k := 1 to n do

begin

for i := 1 to k - 1, k + 1 to n do a_{ik} := a_{ik}a_{kk}^*;

for i := 1 to k - 1, k + 1 to n do

for j := 1 to k - 1, k + 1 to n do

a_{ij} := a_{ij} + a_{ik}a_{kj};

for j := 1 to k - 1, k + 1 to n do a_{kj} := a_{kk}^* a_{kj};

a_{kk} := a_{kk}^*

end

end
```

The proof that this algorithm correctly performs asteration is quite easy, The identities in Theorem 4.10 can be used in establishing the fact that, after any iteration of the main loop (on k), the matrix entries will be

 $a_{ij} = \tilde{A}_{ij}^k + \delta_{ij}.$

Another asteration algorithm is given below, which corresponds to the Gaussian elimination method for inverting matrices in linear algebra.

Algorithm 6.4

Input : An $n \times n$ matrix A. Output: An $n \times n$ matrix S. Claim : $S = A^*$.

begin

1.	$C^{(0)} := A;$
2.	for <i>k</i> := 1 to <i>n</i> do
3.	for $i := k$ to n do
4.	for $j := 1$ to n do
5.	$c_{ij}^{(k)}:=c_{ij}^{(k-1)}+c_{ik}^{(k-1)}\left(c_{kk}^{(k-1)} ight)^{*}c_{kj}^{(k-1)};$
6.	for $i := n$ downto 1 do
7.	for $j := 1$ to n do
8.	$d_{ij} := c_{ij}^{(i)} + \sum_{k=i+1}^n c_{ik}^{(i)} d_{kj};$
9.	S := D + I
	end

Theorem 6.5 (Correctness of Algorithm 6.4). Upon termination of Algorithm 6.4, $S = A^*$.

The proof of this theorem becomes obvious once the following lemma is shown.

Lemma 6.6. Upon termination of Algorithm 6.4, the following hold:

(1)
$$c_{ij}^{(i)} = A_{ij}^i, \quad 1 \le i, j \le n$$

(2) $d_{ij} = \tilde{A}_{ij}^n, \quad 1 \le i, j \le n$

Proof. (1) Comparing Algorithms 6.1 and 6.4, we find that, for $k = i, b_{ij}^{(k)}$ and $c_{ij}^{(k)}$ have the same values. (2) This part follows by backward induction on *i*. For i = n,

$$d_{nj} = c_{nj}^{(n)}$$
 from steps 6, 7, and 8,
= \tilde{A}_{nj}^n by equation (1).

For the induction step, $1 \leq i < n$,

$$d_{i-1,j} = c_{i-1,j}^{(i-1)} + \sum_{k=1}^{n} c_{i-1,k}^{(i-1)} d_{kj}$$

= $\tilde{A}_{i-1,j}^{i-1} + \sum_{k=1}^{n} \tilde{A}_{i-1,k}^{i-1} \tilde{A}_{kj}^{n}$ by (1) and the induction hypothesis,
= $\tilde{A}_{i-1,j}^{n}$ from Theorem 4.10(5).

7 Solution of linear systems of equations

Theorem 7.1. A solution to the system of linear equations

$$x_1 = a_{11}x_1 + \dots + a_{1n}x_n + b_1,$$

$$\vdots$$

$$x_n = a_{n1}x_1 + \dots + a_{nn}x_n + b_n,$$

is given by

$$x_{i} = \begin{vmatrix} a_{11} & \cdots & a_{1i} & \cdots & a_{1n} & b_{1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{i1} & \cdots & a_{ii} & \cdots & a_{in} & b_{i} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{ni} & \cdots & a_{nn} & b_{n} \\ 0 & \cdots & 1 & \cdots & 0 & 0 \end{vmatrix}, \quad 1 \leq i \leq n.$$

Note: The last row in the above eliminant consists of zeros except for a one in column *i*. Hence the solution may also be expressed as

$$x_i = \left| \begin{array}{c|c} A & B \\ \hline I_{i*} & 0 \end{array} \right|,$$

where A, B are the matrix of coefficients and the vector of constants, respectively, in the system of equations, and I_{i*} is the *i*th row of the identity matrix of the same size as A. Furthermore, by Theorem 4.8, the last row of the eliminant can also be replaced with row *i*; pictorially,

$$x_i = \left| \begin{array}{c} A & B \\ A_{i*} & 0 \end{array} \right|.$$

Proof of Theorem 7.1. For $1 \le i \le n$, let x_i be defined as above. Then we have

$$b_{i} + \sum_{j=1}^{n} a_{ij} x_{i}$$

$$= b_{i} + \sum_{j=1}^{n} \begin{vmatrix} a_{11} & \cdots & a_{1i} & \cdots & a_{1n} & b_{1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{i1} & \cdots & a_{ii} & \cdots & a_{in} & b_{i} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{ni} & \cdots & a_{nn} & b_{n} \\ 0 & \cdots & a_{ij} & \cdots & 0 & 0 \end{vmatrix}$$
by Theorem 4.4
$$= \begin{vmatrix} a_{11} & \cdots & a_{1i} & \cdots & a_{1n} & b_{1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{i1} & \cdots & a_{ii} & \cdots & a_{in} & b_{i} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{i1} & \cdots & a_{ii} & \cdots & a_{in} & b_{n} \\ a_{i1} & \cdots & a_{ii} & \cdots & a_{in} & b_{n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{i1} & \cdots & a_{ii} & \cdots & a_{in} & b_{n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{i1} & \cdots & a_{ni} & \cdots & a_{nn} & b_{n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{ni} & \cdots & a_{nn} & b_{n} \\ 0 & \cdots & 1 & \cdots & 0 & 0 \end{vmatrix}$$
by Theorem 4.8
$$= x_{i}. \square$$

If several systems of linear equations have to be solved simultaneously, the problem is formulated in terms of a matrix equation: For give $n \times n$ matrices A, B, find an $n \times n$ matrix X satisfying

$$X = AX + B. \tag{2}$$

Since $A^*B = (AA^* + I)B = A(A^*B) + B$, we know that $X = A^*B$ is a solution of (2).

To describe the solution in the form of eliminants, we will make use of the following theorem.

Theorem 7.2. For $n \times n$ matrices A, B, C.D,

$$\begin{vmatrix} A & B \\ C & D \end{vmatrix} [i,j] = \left[\overbrace{C & D}^{n} \right]_{n+i,n=j}^{n}, \quad 1 \leq i,j \leq n.$$

Proof. Let *E* be the 2×2 eliminant (with $n \times n$ matrix entries) and *F* the $(2n) \times (2n)$ matrix, such that

$$E = \left| \begin{array}{cc} A & B \\ C & D \end{array} \right|, \qquad F = \left[\begin{array}{cc} A & B \\ \hline C & D \end{array} \right].$$

Since $E = D + CA^*B$, we have, for $1 \le i, j \le n$,

$$e_{ij} = d_{ij} + \sum_{k=1}^{n} c_{ik} \cdot \sum_{l=1}^{n} \begin{vmatrix} a_{11} & \cdots & a_{1k} & \cdots & a_{1n} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{l1} & \cdots & a_{lk} & \cdots & a_{ln} & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nk} & \cdots & a_{nn} & 0 \\ 0 & \cdots & 1 & \cdots & 0 & 0 \end{vmatrix} \cdot b_{ij}.$$

By repeatedly applying Theorems 4.4 and 4.5 and finally, Theorem 4.6, we can transform this into

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} & b_{1j} \\ \vdots & & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} & b_{nj} \\ c_{i1} & \cdots & c_{in} & d_{ij} \end{vmatrix},$$

which is $\tilde{F}^n_{n+i,n+j}$. \Box

Theorem 7.3. A solution of the system

$$X = AX + B,$$

where A, B are given $n \times n$ matrices and X is an $n \times n$ matrix of unknowns, is

$$x_{ij} = \left| \begin{array}{c} A & B_{*j} \\ \hline I_{i*} & 0 \end{array} \right|, \quad 1 \leqslant i, j \leqslant n.$$

Proof. For $1 \leq i, j \leq n$,

$$\begin{aligned} x_{ij} &= (A^*B)[i,j] = \left| \begin{array}{c} A & B \\ I & 0 \end{array} \right| [i,j] = \left[\begin{array}{c} \widetilde{A} & B \\ I & 0 \end{array} \right]_{n+i,n+j}^n \\ &= \left| \begin{array}{c} A & B_{*j} \\ I_{i*} & 0 \end{array} \right|. \qquad \Box \end{aligned}$$

Since $X = BA^*$ is clearly a solution of X = XA + B, we can similarly prove the following theorem.

Theorem 7.4. A solution of the system

$$X = XA + B,$$

where A, B are given $n \times n$ matrices, is

$$x_{ij} = \left| \begin{array}{c} A & I_{*j} \\ B_{i*} & 0 \end{array} \right|, \quad 1 \leq i, j \leq n.$$

References

- [1] A.V. Aho, J.E. Hopcroft and J.D. Ullman, *Design and Analysis of Computer Algorithms* (Addison-Wesley, Reading, MA, 1974).
- [2] R.C. Backhouse and B.A. Carré, Regular algebra applied to path-finding problems, *J. Inst, Math. Appl.* 15 (1975) 161–186.
- [3] B.A. Carré, Graphs and Networks, (Clarendon Press, Oxford, 1979).
- [4] J.H. Conway, Regular Algebra and Finite Machines, (Chapman & Hall, London, 1971).
- [5] N. Deo and C. Pang, Shortest path algorithms: Taxonomy and annotation, Tech. Rept. CS-80-057, Washington State University, 1980.
- [6] R.W. Floyd, Algorithm 97: Shortest path, Comm. ACM 5 (6) (1962) 345.
- [7] L.R. Ford and D.R. Fulkerson, Flows in Networks (Princeton University Press, 1962).
- [8] M. Gondran, Path algebras and algorithms, in: B. Roy, ed., *Combinatorial Programming* (Reidel, Boston, MA/Dordrecht, 1975).
- [9] J.B. Kam and J.D. Ullman, Global data flow analysis and iterative algorithms, *J. ACM* **23** (1) (1976) 158–171.
- [10] D.J. Lehmann, Algebraic structures for transitive closure, Theoret. Comput. Sci. 4 (1) (1977) 59-76.
- [11] R. McNaughton and H. Yamada, Regular expressions and state graphs for automata, *IRE Trans.* EC9 (1960) 39–47.
- [12] A.R. Pierce, Bibliography on algorithms for shortest paths, shortest spanning tree and related circuit routing problems, 1956–1974, *Networks* **5** (1975) 129–149.
- [13] P. Robert and J. Ferland, Généralisation de l'algorithme de Warshall, *RAIRO Inform. Théor.* 2 (1968) 71–85.
- [14] R.E. Tarjan, A unified approach to solving path problems, Tech. Rept. CS-79-729, Stanford Univ., 1979.
- [15] S. Warshall, A theorem on Boolean matrices, J. ACM 9 (1) (1962) 11–12.
- [16] M. Yoeli, A note on a generalization of Boolean matrix theory, Amer. Math. Monthly, 68 (1961) 552– 557.