

Regular Algebra Applied to Path-finding Problems

R. C. BACKHOUSE†

Department of Computing and Control, Imperial College, London

AND

B. A. CARRÉ‡

Laboratoire d'Automatique et d'Analyse des Systèmes, C.N.R.S., Toulouse, France

[Received 20 March 1973 and in revised form 31 October 1973]

In an earlier paper, one of the authors presented an algebra for formulating and solving extremal path problems. There are striking similarities between that algebra and the algebra of regular languages, which lead one to consider whether the previous results can be generalized—for instance to path enumeration problems—and whether the algebra of regular languages can itself be profitably used for the general study of path-finding problems. This paper gives affirmative answers to both these questions.

1. Introduction

IN AN EARLIER paper (Carré, 1971), an algebra was presented for the formulation of certain extremal path problems, i.e. problems involving the determination of a path through a graph such that some specified function of the numerical labels of its arcs is either maximized or minimized. It was shown that in terms of this algebra, an extremal path problem can be posed as that of solving a matrix equation of the form $Y = AY + B$ where A and B are specified, and it was demonstrated that such equations can be solved by variants of classical methods of linear algebra, differing from these only in the significance of the additive and multiplicative operations.

There is a striking similarity between some of the results in this earlier paper and some results in regular algebra, i.e. the algebra of regular languages. It is therefore natural to consider whether the results of the earlier paper (henceforth referred to as BAC 71) can be generalized—for instance to path enumeration problems—and whether it is profitable to use regular algebra itself to obtain general methods of solving path problems.

In Section 2 we first give an axiomatic definition of regular algebra. This differs slightly from that given by other authors, in two respects. Firstly, it employs a concept of “*definiteness*”, which is a generalization of the notion of definiteness of BAC 71. This concept has various concrete interpretations, which will be discussed subsequently: for instance it will be proved that for regular languages, non-definiteness corresponds to the empty word property. The only other novelty of our axiomatic formulation of regular algebra is that it is equally applicable to matrices on regular algebras; our reasons for making this innovation will become evident in the following sections.

† Now at Department of Computer Science, Heriot-Watt University, Edinburgh, Scotland.

‡ On leave from the University of Southampton, England.

In Section 3 we note some well-known identities of regular algebra. It is then shown (in Section 4) that two of these identities yield product forms for the closure A^* of a square matrix A , similar to the Jordan product form and triangular factor representations of inverse matrices in linear algebra. The product forms immediately give algorithms for computing closure matrices and for solving equations of the form $Y = AY + B$. These algorithms are similar to some of those derived in BAC 71, but the algorithms given here are more general, and more evidently related to methods of linear algebra.

We then consider various homomorphic images of regular algebras (in Section 5), and find that these include several algebras which have already been applied to path problems by other authors. In Section 6 we compare regular algebra with the network algebra of BAC 71, and find that they are inconsistent in only one respect: that whereas in regular algebra the closure A^* of any matrix A is well-defined, if we add to its axiom system the cancellative property of BAC 71 then A^* ceases to be well-defined unless A is meaningful in a physical sense.

We conclude with an illustrative example, in which we apply regular algebra and one of its homomorphic images to path enumeration problems. The resulting algorithm is the most efficient method of enumerating elementary paths known to us.

2. Regular Algebra

2.1. Definitions

2.1.1. *Axioms.* We shall consider an algebra $R = (S, +, \cdot, *)$ consisting of a set S on which are defined two binary operations $+$ and \cdot and one unary operation $*$. The following are assumed as axiomatic.

$$\begin{array}{ll} \text{A1} & (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \\ \text{A2} & \alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma \\ \text{A3} & \alpha + \beta = \beta + \alpha \\ \text{A4} & \alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma) \\ \text{A5} & (\alpha + \beta) \cdot \gamma = (\alpha \cdot \gamma) + (\beta \cdot \gamma) \\ \text{A6} & \alpha + \alpha = \alpha \end{array}$$

where $\alpha, \beta, \gamma \in S$.

The set S contains a zero element ϕ such that

$$\text{A7} \quad \alpha + \phi = \alpha \qquad \text{A8} \quad \phi \cdot \alpha = \phi = \alpha \cdot \phi,$$

and a unit element e such that

$$\text{A9} \quad e \cdot \alpha = \alpha = \alpha \cdot e$$

Finally the star (or *closure*) operator $*$ obeys:

$$\left. \begin{array}{l} \text{A10} \quad \alpha^* = e + \alpha \cdot \alpha^* \\ \text{A11} \quad \alpha^* = (e + \alpha)^* \end{array} \right\} \text{ for all } \alpha \in S.$$

2.1.2. *Partial ordering.* In view of A1, A3 and the idempotency law A6 we can define a partial ordering \preceq on the set S by

$$\alpha \preceq \beta \Leftrightarrow \alpha + \beta = \beta$$

and a strict ordering \prec by

$$\alpha \prec \beta \Leftrightarrow \alpha \preceq \beta \text{ and } \alpha \neq \beta.$$

It is easily verified that

$$\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma,$$

$$\alpha \cdot \gamma \leq \beta \cdot \gamma,$$

and

$$\gamma \cdot \alpha \leq \gamma \cdot \beta \text{ for all } \alpha, \beta, \gamma \in S.$$

Note that we do *not* assume the cancellative property

$$\alpha \cdot \gamma = \beta \cdot \gamma \Rightarrow \alpha = \beta,$$

and in consequence we cannot in general infer that

$$\text{if } \alpha < \beta \text{ then } \alpha \cdot \gamma < \beta \cdot \gamma.$$

2.1.3. *Solution of equations.* We define an element α of S to be *definite* if and only if $t = \alpha \cdot t \Rightarrow t = \phi$. Then we assume the following rule of inference:

$$\text{R1 } \psi = \alpha \cdot \psi + \beta \Rightarrow \psi \geq \alpha^* \cdot \beta$$

and furthermore, if α is definite then

$$\psi = \alpha \cdot \psi + \beta \Rightarrow \psi = \alpha^* \cdot \beta$$

It will be observed that for any given α and β , the equation $\psi = \alpha \cdot \psi + \beta$ always has a solution $\psi = \alpha^* \cdot \beta$. The first part of our rule R1 postulates that $\psi = \alpha^* \cdot \beta$ is the minimal solution, and the second part gives a condition under which this solution is unique.

Henceforth we shall denote the set of axioms A1–A11 and the rule of inference R1 by F1, and we shall call any algebra $R = (S, +, \cdot, *)$ such that the set F1 is valid in R a *regular algebra*.

2.1.4. *Square matrices.* Given any regular algebra R we can form a new regular algebra $\mathcal{M}_p(R)$ consisting of all $p \times p$ matrices whose elements belong to R . In the algebra $\mathcal{M}_p(R)$ the operators $+$ and \cdot and the order relation \leq are defined as follows: let $\mathbf{A} = [a_{ij}]$ and $\mathbf{B} = [b_{ij}]$ be any $p \times p$ matrices with elements in R ; then

$$\mathbf{A} + \mathbf{B} = [a_{ij} + b_{ij}], \quad \mathbf{A} \cdot \mathbf{B} = \mathbf{AB} = \left[\sum_{k=1}^p a_{ik} \cdot b_{kj} \right],$$

and

$$\mathbf{A} \leq \mathbf{B} \text{ if and only if } a_{ij} \leq b_{ij} \text{ for all } i, j.$$

The *unit matrix* $\mathbf{E} = [e_{ij}]$ is defined as that $p \times p$ matrix with $e_{ij} = e$ if $i = j$ and $e_{ij} = \phi$ if $i \neq j$. The rows and columns of this matrix are described as *unit vectors*. The *zero or null matrix* \mathbf{N} is that matrix all of whose entries are ϕ .

The powers of a square matrix \mathbf{A} are

$$\mathbf{A}^0 = \mathbf{E}, \quad \mathbf{A}^k = \mathbf{A}^{k-1} \mathbf{A} \quad (k = 1, 2, \dots).$$

Finally, the *closure* of \mathbf{A} is

$$\mathbf{A}^* = \sum_{k=0}^{\infty} \mathbf{A}^k.$$

Assuming the above definitions of $+$, \cdot , and $*$, and with \mathbf{N} replacing ϕ , it is a logical problem to prove (by induction on p) that $\mathcal{M}_p(R)$ forms a regular algebra, i.e. that all of A1–A11 and the rule of inference R1 are valid in $\mathcal{M}_p(R)$. This problem does not concern us here, the interested reader is referred to its discussion by Conway

(1971). However, we shall remark in Section 5 that for those examples of $\mathcal{M}_p(R)$ which concern us, we can infer the validity of the axioms and rule of inference from previous literature.

2.2 An Example

There are various interpretations of S and the operators $+$, $.$, and $*$ each of which gives rise to a regular algebra. In particular, the above axiom system was first put forward for Regular Languages (Salomaa, 1969) which are defined below.

2.2.1. *Regular languages.* Consider any finite non-empty set $V = \{v_1, v_2, \dots, v_m\}$, which we call an *alphabet* or *vocabulary*, and whose elements we call *letters*. A *word* over V is a finite string of zero or more letters of V ; the string consisting of zero letters is called the *empty word*.

The set of all words over V is denoted by V^* . A *language* over V is any subset of V^* . The symbol ϕ denotes the empty set, and $\phi^* = e$ denotes the set consisting of the empty word.

The *sum* $\alpha + \beta$ of two languages α and β is their set union, and the *product* or *concatenation* $\alpha . \beta$ is the set consisting of all words formed by concatenating a word in α with a word in β . The powers of a language α are defined by

$$\alpha^0 = e, \quad \alpha^k = \alpha^{k-1} . \alpha \quad (k = 1, 2, \dots),$$

and the *closure* α^* of α is defined to be $\sum_{k=0}^{\infty} \alpha^k$.

The *regular expressions* over V are the well-formed formulae obtained from the alphabet $V \cup \{\phi\}$, the operators $+$, $.$, and $*$, and the parentheses (and). Thus $(v_1) . (v_4 + v_6)^* . (v_1 . (v_5^*) . v_2)^*$ is a regular expression. Also allowed are expressions in which the dot is omitted, being denoted by juxtaposition, and parentheses are omitted. In this latter case operator precedence is $.$ before $+$, and $*$ before $+$ and $.$

Each regular expression denotes a language over V called a *regular language*. If $S(V)$ is the set of all regular expressions over $V \cup \{\phi\}$, then $R(V) = (S(V), +, ., *)$ is the free regular algebra generated by V .

2.2.2. *Labelled graphs.* A labelled graph $G = (X, \Gamma)$ consists of a set X of p elements x_1, x_2, \dots, x_p together with a subset Γ of the ordered pairs (x_i, x_j) of elements taken from X . The elements of X are called *nodes* and the elements of Γ are called *arcs*. Each arc (x_i, x_j) is said to be *directed* from x_i to x_j , and is *labelled* with some element l_{ij} of a regular algebra R .

A sequence of t arcs

$$\mu = (x_i, x_{k_1}), (x_{k_1}, x_{k_2}), \dots, (x_{k_{t-1}}, x_j)$$

such that the terminal node of each arc coincides with the initial node of the following arc is called a *path* from x_i to x_j , of order t . If $i \neq j$ then the path μ is said to be *open*; whereas if $i = j$, μ is called a *closed path* or *cycle*. A path (open or closed) is *elementary* if it does not traverse any of its nodes more than once. The path product $w(\mu)$ of a path μ is defined as the product of its arc labels:

$$w(\mu) = l_{ik_1} l_{k_1k_2} \cdots l_{k_{t-1}j}.$$

It is well-known that a p -node labelled graph $G = (X, \Gamma)$ can be described by a $p \times p$

matrix $A = [a_{ij}]$ where $a_{ij} = l_{ij}$ if $(x_i, x_j) \in \Gamma$ and $a_{ij} = \phi$ otherwise. Conversely, a $p \times p$ matrix A can always be visualized as a p -node graph.

If we now interpret R as in the previous section, regarding each arc label on a graph G as some regular language, then for any path μ from x_i to x_j the corresponding path product $w(\mu)$ is obtained by concatenating the arc labels of μ . Each word in the resulting language is said to be a *word taking node x_i to node x_j* . The transitive closure $A^* = [a_{ij}^*]$ of the matrix A of G will be such that a_{ij}^* is the set of all words taking node x_i to x_j .

As this example suggests, the central problem in path-finding is to determine particular elements of the closure A^* of a matrix A in some algebra $\mathcal{M}_p(R)$. Some methods of calculating these elements will be presented in the following sections.

3. Some Identities of Regular Algebra and their Analogues in Linear Algebra

If A is a matrix on a regular algebra $\mathcal{M}_p(R)$, then by R1 its closure $A^* = \sum_{k=0}^{\infty} A^k$ is a solution of the equation

$$Y = AY + E \tag{3.1}$$

and moreover, it is the unique solution if A is definite, i.e. if $T = AT \Rightarrow T = 0$. We observe here an analogy with linear algebra, where the equation

$$Y = AY + I \tag{3.2}$$

has the unique solution $Y = (I - A)^{-1}$ if $I - A$ is non-singular, that is to say if $T = AT \Rightarrow T = 0$. With A^* replacing $(I - A)^{-1}$, a surprising amount of the theory of real matrices holds in regular algebra, and several authors have already used variants of methods of linear algebra to solve problems in the algebra of regular expressions (Salomaa, 1969), and also to solve extremal path problems (BAC 71). Here we shall derive general methods—valid in any regular algebra—which are again related to linear algebraic techniques.

For this purpose we need a number of identities in regular algebra, which are listed below. In regular algebra all these identities are well-known, indeed they are often listed as axioms (e.g. Conway, 1971). The identities can all be verified easily, by writing each closure in expanded form and comparing terms on both sides; alternatively, they can be proved formally using the system F1. We also give the analogous identities in linear algebra, obtained by writing $(I - M)^{-1}$ in place of M^* .

In regular algebra

In linear algebra

$$A^*A = AA^* \qquad (I - A)^{-1}A = A(I - A)^{-1} \tag{3.3}$$

$$A(BA)^* = (AB)^*A \qquad A(I - BA)^{-1} = (I - AB)^{-1}A \tag{3.4}$$

$$(A + B)^* = A^*(BA^*)^* \qquad (I - (A + B))^{-1} = (I - A)^{-1}[I - B(I - A)^{-1}]^{-1} \tag{3.5}$$

$$(A + B)^* = (A^*B)^*A^* \qquad (I - (A + B))^{-1} = [I - (I - A)^{-1}B]^{-1}(I - A)^{-1} \tag{3.6}$$

$$(AB)^* = E + A(BA)^*B \qquad (I - AB)^{-1} = I + A(I - BA)^{-1}B \tag{3.7}$$

4. Product Forms for Closure Matrices

In this section we shall use the identities (3.5)–(3.7) to derive product forms for the closure A^* of a $p \times p$ matrix A , analogous to the Jordan product forms and triangular

factor representations of inverse matrices in linear algebra. These product forms yield algorithms analogous to the direct methods of linear algebra, for calculating the minimal solution $Y = A^*B$ of a set of equations of the form $Y = AY + B$. They also provide us with efficient methods of computing particular rows, columns, or other submatrices of A^* , which are frequently required in automata studies (Conway, 1971) and in operational research (BAC 71).

Our techniques for deriving product forms are based on the following simple idea: Given a matrix $A = A^{(0)}$, we can split $A^{(0)}$ into two matrices $C^{(1)}$ and $S^{(1)}$, and using (3.6), write $A^* = A^{(0)*} = (C^{(1)} + S^{(1)})^* = (C^{(1)*}S^{(1)*})^*C^{(1)*} = A^{(1)*}C^{(1)*}$, say. In doing so, the problem of determining the closure of $A^{(0)}$ is turned into the problem of finding the closure of two matrices $A^{(1)}$ and $C^{(1)}$. Our strategy is to choose $C^{(1)}$ and $S^{(1)}$ such that (a) the closure of $C^{(1)}$ can be immediately calculated and (b) $A^{(1)}$ has a "simpler" form than $A^{(0)}$. We can then repeat the process for $A^{(1)}$, reducing the problem of finding $A^{(1)*}$ to that of finding $C^{(2)*}$ and $A^{(2)*}$, and so on. The process is terminated when, after p steps $A^{(p)}$ is of such a form that its closure $A^{(p)*}$ can also be immediately calculated. Using alternative methods of splitting, combined with different identities of regular algebra, we can derive different product forms for A^* .

In the following discussion, the typical elements of a matrix M and its closure M^* will be denoted by m_{ij} and m_{ij}^* respectively, and the closure of an element m_{ij} of M will be denoted by $(m_{ij})^*$. The i th row and the j th column of M will be denoted by m_{i0} and m_{0j} respectively.

4.1. The Jordan Product Forms

4.1.1. *Row and column decompositions.* To obtain a product form for A^* , we first set $A^{(0)} = A$ and express $A^{(0)}$ in terms of its column vectors:

$$A^{(0)} = \sum_{j=1}^p a_{0j}^{(0)} e_{j0}. \tag{4.1}$$

Then we can express $A^{(0)}$ as the matrix sum

$$A^{(0)} = C^{(1)} + S^{(1)}$$

where

$$C^{(1)} = a_{01}^{(0)} e_{10} \quad \text{and} \quad S^{(1)} = \sum_{j=2}^p a_{0j}^{(0)} e_{j0}. \tag{4.2}$$

Hence, from (3.6),

$$A^{(0)*} = (C^{(1)} + S^{(1)})^* = A^{(1)*}C^{(1)*}, \quad \text{where} \quad A^{(1)} = C^{(1)*}S^{(1)}. \tag{4.3}$$

Now since the first column of $S^{(1)}$ is null, the first column of $A^{(1)}$ is null also, so $A^{(1)}$ can in turn be expressed as the sum

$$A^{(1)} = C^{(2)} + S^{(2)}$$

where

$$C^{(2)} = a_{02}^{(1)} e_{20} \quad \text{and} \quad S^{(2)} = \sum_{j=3}^p a_{0j}^{(1)} e_{j0}, \tag{4.4}$$

and applying (3.6) again,

$$A^{(1)*} = (C^{(2)} + S^{(2)})^* = A^{(2)*}C^{(2)*}, \quad \text{where} \quad A^{(2)} = C^{(2)*}S^{(2)}. \tag{4.5}$$

Continuing in a similar manner, setting

$$\begin{aligned} \mathbf{C}^{(k)} &= \mathbf{a}_{0k}^{(k-1)} \mathbf{e}_{k0}, & \mathbf{S}^{(k)} &= \sum_{j=k+1}^p \mathbf{a}_{0j}^{(k-1)} \mathbf{e}_{j0}, \\ \mathbf{A}^{(k)} &= \mathbf{C}^{(k)} * \mathbf{S}^{(k)}, & (k &= 1, 2, \dots, p), \end{aligned} \tag{4.6}$$

we obtain

$$\mathbf{A}^{(k-1)*} = \mathbf{A}^{(k)*} \mathbf{C}^{(k)*}, \quad (k = 1, 2, \dots, p). \tag{4.7}$$

Now $\mathbf{A}^{(p)}$ is null, so $\mathbf{A}^{(p)*} = \mathbf{E}$. Therefore (4.7) gives

$$\mathbf{A}^* = \mathbf{C}^{(p)*} \mathbf{C}^{(p-1)*} \dots \mathbf{C}^{(1)*}. \tag{4.8}$$

We note that from (4.6) and (3.7),

$$\mathbf{C}^{(k)*} = (\mathbf{a}_{0k}^{(k-1)} \mathbf{e}_{k0})^* = \mathbf{E} + \mathbf{a}_{0k}^{(k-1)} (\mathbf{e}_{k0} \mathbf{a}_{0k}^{(k-1)})^* \mathbf{e}_{k0} = \mathbf{E} + \mathbf{a}_{0k}^{(k-1)} (\mathbf{a}_{kk}^{(k-1)})^* \mathbf{e}_{k0}. \tag{4.9}$$

Hence $\mathbf{C}^{(k)*}$ differs from the unit matrix only in its k th column, where

$$c_{ik}^{(k)*} = \begin{cases} \mathbf{a}_{ik}^{(k-1)} (\mathbf{a}_{kk}^{(k-1)})^*, & \text{for } i \neq k, \\ (\mathbf{a}_{kk}^{(k-1)})^*, & \text{for } i = k, \end{cases} \tag{4.10}$$

Also from (4.6) and (4.9),

$$\begin{aligned} \mathbf{A}^{(k)} &= \sum_{j=k+1}^p \mathbf{C}^{(k)*} \mathbf{a}_{0j}^{(k-1)} \mathbf{e}_{j0} & (k &= 1, 2, \dots, p) \\ &= \sum_{j=k+1}^p (\mathbf{E} + \mathbf{a}_{0k}^{(k-1)} (\mathbf{a}_{kk}^{(k-1)})^* \mathbf{e}_{k0}) \mathbf{a}_{0j}^{(k-1)} \mathbf{e}_{j0} & (k &= 1, 2, \dots, p) \\ &= \sum_{j=k+1}^p (\mathbf{a}_{0j}^{(k-1)} + \mathbf{a}_{0k}^{(k-1)} (\mathbf{a}_{kk}^{(k-1)})^* \mathbf{a}_{kj}^{(k-1)}) \mathbf{e}_{j0} & (k &= 1, 2, \dots, p). \end{aligned} \tag{4.11}$$

The non-null columns of $\mathbf{A}^{(k)}$ can therefore be obtained directly from those of $\mathbf{A}^{(k-1)}$, using

$$\begin{aligned} \mathbf{a}_{0j}^{(k)} &= \mathbf{a}_{0j}^{(k-1)} + \mathbf{a}_{0k}^{(k-1)} (\mathbf{a}_{kk}^{(k-1)})^* \mathbf{a}_{kj}^{(k-1)}, \\ &\text{for } k < j \leq p \quad (k = 1, 2, \dots, p-1). \end{aligned} \tag{4.12}$$

The product form (4.8) was derived by repeated application of the relation (3.6), $(\mathbf{P} + \mathbf{Q})^* = (\mathbf{P} * \mathbf{Q}) * \mathbf{P}^*$, to column decompositions. Alternatively, it is possible to apply (3.5), $(\mathbf{P} + \mathbf{Q})^* = \mathbf{P} * (\mathbf{Q} \mathbf{P}^*)^*$, to row decompositions. Corresponding to (4.6)–(4.8), if we set

$$\begin{aligned} \mathbf{R}^{(k)} &= \mathbf{e}_{0k} \mathbf{a}_{k0}^{(k-1)}, & \mathbf{T}^{(k)} &= \sum_{i=k+1}^p \mathbf{e}_{0i} \mathbf{a}_{i0}^{(k-1)}, \\ \mathbf{A}^{(k)} &= \mathbf{T}^{(k)} \mathbf{R}^{(k)*}, & (k &= 1, 2, \dots, p), \end{aligned} \tag{4.13}$$

then

$$\mathbf{A}^{(k-1)*} = \mathbf{R}^{(k)*} \mathbf{A}^{(k)*}, \quad (k = 1, 2, \dots, p), \tag{4.14}$$

hence

$$\mathbf{A}^* = \mathbf{R}^{(1)*} \mathbf{R}^{(2)*} \dots \mathbf{R}^{(p)*}. \tag{4.15}$$

We describe (4.8) and (4.15) as the *Jordan product forms* for \mathbf{A}^* . It will be observed that if $(\mathbf{a}_{kk}^{(k-1)})^*$ is interpreted as $1/(1 - \mathbf{a}_{kk}^{(k-1)})$, then in linear algebra (4.8) and (4.15) become the usual product form representations of the inverse of the matrix $\mathbf{I} - \mathbf{A}$ (Fox, 1964; Reid, 1971).

4.1.2. *Triangular matrices.* For triangular matrices the relations (4.6)–(4.8) and (4.13)–(4.15) defining the Jordan product forms can be greatly simplified. Specifically, in

applying the column decomposition method to a lower triangular matrix \mathbf{L} , (4.12) gives $\mathbf{l}_{0j}^{(k)} = \mathbf{l}_{0j}^{(k-1)} = \dots = \mathbf{l}_{0j}^{(0)}$ for $k < j \leq p$, and so

$$\mathbf{L}^{(k)} = \sum_{j=k+1}^p \mathbf{l}_{0j}^{(0)} \mathbf{e}_{j0}, \quad (k = 1, 2, \dots, p) \quad (4.16)$$

which is simply the original matrix \mathbf{L} with its first k columns nullified. Thus $\mathbf{C}^{(k)}$ is formed directly from the k th column of \mathbf{L} , and corresponding to (4.8) and (4.9) we have

$$\mathbf{L}^* = \mathbf{C}^{(p)*} \mathbf{C}^{(p-1)*} \dots \mathbf{C}^{(1)*}$$

where

$$\mathbf{C}^{(k)*} = \mathbf{E} + \mathbf{l}_{0k} \mathbf{l}_{kk}^* \mathbf{e}_{k0}, \quad (k = 1, 2, \dots, p). \quad (4.17)$$

Similarly for an upper triangular matrix \mathbf{U} , (4.13)–(4.15) give

$$\mathbf{U}^* = \mathbf{R}^{(1)*} \mathbf{R}^{(2)*} \dots \mathbf{R}^{(p)*}$$

where

$$\mathbf{R}^{(k)*} = \mathbf{E} + \mathbf{e}_{0k} \mathbf{u}_{kk}^* \mathbf{u}_{k0}, \quad (k = 1, 2, \dots, p). \quad (4.18)$$

If \mathbf{L} and \mathbf{U} are *strictly* triangular then $\mathbf{l}_{kk}^* = e$ and $\mathbf{u}_{kk}^* = e$ for all k , so (4.17) and (4.18) can be even further simplified, giving the relations

$$\mathbf{L}^* = \mathbf{C}^{(p-1)*} \mathbf{C}^{(p-2)*} \dots \mathbf{C}^{(1)*}, \quad \text{where } \mathbf{C}^{(k)*} = \mathbf{E} + \mathbf{l}_{0k} \mathbf{e}_{k0} \quad (4.19)$$

$$\mathbf{U}^* = \mathbf{R}^{(1)*} \mathbf{R}^{(2)*} \dots \mathbf{R}^{(p-1)*}, \quad \text{where } \mathbf{R}^{(k)*} = \mathbf{E} + \mathbf{e}_{0k} \mathbf{u}_{k0} \quad (4.20)$$

which were derived in BAC 71.

4.1.3. *Applications to the solution of equations.* The product form (4.8) immediately yields an algorithm for computing the minimal solution $\mathbf{Y} = \mathbf{A}^* \mathbf{B}$ of the equation $\mathbf{Y} = \mathbf{A} \mathbf{Y} + \mathbf{B}$. From (4.8),

$$\mathbf{A}^* \mathbf{B} = \mathbf{C}^{(p)*} \mathbf{C}^{(p-1)*} \dots \mathbf{C}^{(1)*} \mathbf{B}, \quad (4.21)$$

so if we form the sequence

$$\mathbf{B}^{(0)} = \mathbf{B}, \quad \mathbf{B}^{(k)} = \mathbf{C}^{(k)*} \mathbf{B}^{(k-1)} \quad (k = 1, 2, \dots, p), \quad (4.22)$$

the final term gives the required solution: $\mathbf{B}^{(p)} = \mathbf{A}^* \mathbf{B}$. We note that from (4.9), the successive $\mathbf{B}^{(k)}$ matrices are given by

$$\mathbf{B}^{(0)} = \mathbf{B}, \quad \mathbf{B}^{(k)} = \mathbf{B}^{(k-1)} + \mathbf{a}_{0k}^{(k-1)} (\mathbf{a}_{kk}^{(k-1)})^* \mathbf{b}_{k0}^{(k-1)} \quad (k = 1, 2, \dots, p). \quad (4.23)$$

Hence the solution can be obtained simply by performing p successive transformations of \mathbf{A} and \mathbf{B} , the matrices $\mathbf{A}^{(k)}$ and $\mathbf{B}^{(k)}$ at each stage being obtained from (4.12) and (4.23) respectively. This method is analogous to the Jordan method of solving $\mathbf{Y} = \mathbf{A} \mathbf{Y} + \mathbf{B}$ in linear algebra, with $\mathbf{Y} = \mathbf{A}^{(k)} \mathbf{Y} + \mathbf{B}^{(k)}$ ($k = 1, 2, \dots, p$) being the equivalent system obtained after elimination of the k th \mathbf{Y} -variable.

To obtain the minimal solution $\mathbf{Y} = \mathbf{L}^* \mathbf{B}$ of a lower triangular system $\mathbf{Y} = \mathbf{L} \mathbf{Y} + \mathbf{B}$, (4.17) and (4.22) give the familiar *forward substitution method*

$$\mathbf{B}^{(0)} = \mathbf{B}, \quad \mathbf{B}^{(k)} = \mathbf{B}^{(k-1)} + \mathbf{l}_{0k} \mathbf{l}_{kk}^* \mathbf{b}_{k0}^{(k-1)} \quad (k = 1, 2, \dots, p), \quad (4.24)$$

which does not involve any modifications of \mathbf{L} . For an upper triangular system $\mathbf{Y} = \mathbf{U} \mathbf{Y} + \mathbf{B}$, (4.18) enables us to express the minimal solution as

$$\mathbf{U}^* \mathbf{B} = \mathbf{R}^{(1)*} \mathbf{R}^{(2)*} \dots \mathbf{R}^{(p)*} \mathbf{B} \quad (4.25)$$

which leads to the *back-substitution method*

$$\mathbf{B}^{(0)} = \mathbf{B}, \quad \mathbf{B}^{(k)} = \mathbf{R}^{(p-k+1)*} \mathbf{B}^{(k-1)} \quad (k = 1, 2, \dots, p). \quad (4.26)$$

From (4.18), the $\mathbf{B}^{(k)}$ matrices here are given by

$$\mathbf{B}^{(k)} = \mathbf{B}^{(k-1)} + \mathbf{e}_{0q}(u_{qq})^* \mathbf{u}_{q0} \mathbf{B}^{(k-1)} \tag{4.27}$$

where $q = p - k + 1$; hence they have elements

$$b_{ij}^{(k)} = \begin{cases} b_{ij}^{(k-1)} & \text{for } i \neq q, \\ b_{ij}^{(k-1)} + (u_{qq})^* \sum_{r=q}^p u_{qr} b_{rj}^{(k-1)} & \text{for } i = q. \end{cases} \tag{4.28}$$

4.1.4. *Weak transitive closure matrices.* In regular algebra it is sometimes necessary to compute the matrix $\mathbf{A}^+ = \sum_{k=1}^{\infty} \mathbf{A}^k$, for instance in compiling computer programs

(Barron, 1968). Now since $\mathbf{A}^+ = \mathbf{A}^* \mathbf{A}$, \mathbf{A}^+ is the minimal solution of $\mathbf{Y} = \mathbf{A} \mathbf{Y} + \mathbf{A}$, which can be obtained by the Jordan method as defined above. However, with $\mathbf{B}^{(0)} = \mathbf{A}$ in (4.22), the final $p-k$ columns of $\mathbf{B}^{(k)}$ are identical to the corresponding columns of $\mathbf{A}^{(k)}$. Indeed from (4.6) and (4.22),

$$\mathbf{a}_{0j}^{(k)} = \mathbf{C}^{(k)} * \mathbf{C}^{(k-1)} * \dots * \mathbf{C}^{(1)} * \mathbf{a}_{0j}^{(0)} = \mathbf{b}_{0j}^{(k)}, \text{ for } k < j \leq p. \tag{4.29}$$

Hence, from (4.22) and (4.29) we obtain the simpler algorithm

$$\mathbf{B}^{(0)} = \mathbf{A}, \quad \mathbf{B}^{(k)} = \mathbf{B}^{(k-1)} + \mathbf{b}_{0k}^{(k-1)} (b_{kk}^{(k-1)})^* \mathbf{b}_{k0}^{(k-1)} \quad (k = 1, 2, \dots, p). \tag{4.30}$$

On the two element Boolean algebra, (4.30) is known as Warshall's algorithm (Warshall, 1961). The complete \mathbf{A}^* -matrix is seldom required explicitly, but it can be obtained by applying (4.30) and then using $\mathbf{A}^* = \mathbf{E} + \mathbf{A}^+$.

4.2. The Gauss Product Form

It will now be shown that by alternate applications of the row and column decomposition methods defined above, one can express \mathbf{A}^* as a product of elementary triangular matrices. The resulting product form leads immediately to analogues of the Gauss elimination method and its variants.

4.2.1. *Triangular decomposition.* We again consider a $p \times p$ matrix $\mathbf{A}^{(0)}$, to which we first apply the row decomposition

$$\mathbf{A}^{(0)} = \mathbf{R}^{(1)} + \mathbf{T}^{(1)}$$

where

$$\mathbf{R}^{(1)} = \mathbf{e}_{01} \mathbf{a}_{10}^{(0)} \quad \text{and} \quad \mathbf{T}^{(1)} = \sum_{i=2}^p \mathbf{e}_{0i} \mathbf{a}_{i0}^{(0)}. \tag{4.31}$$

whence

$$\mathbf{A}^{(0)*} = (\mathbf{R}^{(1)} + \mathbf{T}^{(1)})^* = \mathbf{R}^{(1)*} \mathbf{S}^{(1)*}, \text{ where } \mathbf{S}^{(1)} = \mathbf{T}^{(1)} \mathbf{R}^{(1)*}. \tag{4.32}$$

We note that since the first row of $\mathbf{T}^{(1)}$ is null, the first row of $\mathbf{S}^{(1)}$ is null also. We now perform the column decomposition

$$\mathbf{S}^{(1)} = \mathbf{C}^{(1)} + \mathbf{A}^{(1)}$$

where

$$\mathbf{C}^{(1)} = s_{01}^{(1)} \mathbf{e}_{10} \quad \text{and} \quad \mathbf{A}^{(1)} = \sum_{j=2}^p s_{0j}^{(1)} \mathbf{e}_{j0} \tag{4.33}$$

whence

$$\mathbf{S}^{(1)*} = (\mathbf{C}^{(1)} + \mathbf{A}^{(1)})^* = (\mathbf{C}^{(1)*} \mathbf{A}^{(1)*}) * \mathbf{C}^{(1)*}. \tag{4.34}$$

Here both the first column and the first row of $\mathbf{A}^{(1)}$ are null; and since only the first column of $\mathbf{C}^{(1)}$ is non-null, in (4.34) we have $\mathbf{C}^{(1)*} \mathbf{A}^{(1)*} = (\mathbf{E} + \mathbf{C}^{(1)*} \mathbf{C}^{(1)}) \mathbf{A}^{(1)*} = \mathbf{A}^{(1)*}$.

Therefore (4.34) simplifies to

$$\mathbf{S}^{(1)*} = \mathbf{A}^{(1)*}\mathbf{C}^{(1)*}, \tag{4.35}$$

so (4.32) gives

$$\mathbf{A}^{(0)*} = \mathbf{R}^{(1)*}\mathbf{A}^{(1)*}\mathbf{C}^{(1)*}. \tag{4.36}$$

Continuing in a similar fashion, setting

$$\left. \begin{aligned} \mathbf{R}^{(k)} &= \mathbf{e}_{0k}\mathbf{a}_{k0}^{(k-1)}, & \mathbf{T}^{(k)} &= \sum_{i=k+1}^p \mathbf{e}_{0i}\mathbf{a}_{i0}^{(k-1)}, & \mathbf{S}^{(k)} &= \mathbf{T}^{(k)}\mathbf{R}^{(k)*}, \\ \mathbf{C}^{(k)} &= \mathbf{s}_{0k}^{(k)}\mathbf{e}_{k0}, & \mathbf{A}^{(k)} &= \sum_{j=k+1}^p \mathbf{s}_{0j}\mathbf{e}_{j0}, \end{aligned} \right\} k = 1, \dots, p \tag{4.37}$$

we obtain

$$\mathbf{A}^{(k)*} = \mathbf{R}^{(k+1)*}\mathbf{A}^{(k+1)*}\mathbf{C}^{(k+1)*} \quad (k = 1, 2, \dots, p). \tag{4.38}$$

At the p th stage $\mathbf{A}^{(p)}$ and $\mathbf{C}^{(p)}$ are null, so (4.38) gives

$$\mathbf{A}^* = \mathbf{R}^{(1)*}\mathbf{R}^{(2)*} \dots \mathbf{R}^{(p)*}\mathbf{C}^{(p-1)*}\mathbf{C}^{(p-2)*} \dots \mathbf{C}^{(1)*}. \tag{4.39}$$

This decomposition process is illustrated in Fig. 1, which shows the disposition of the non-null elements of the successive $\mathbf{R}^{(k)}$, $\mathbf{C}^{(k)}$, and $\mathbf{A}^{(k)}$ matrices. It will be observed that the $\mathbf{R}^{(k)}$ matrices together form an upper triangular matrix $\mathbf{U} = \sum_{k=1}^p \mathbf{R}^{(k)}$, whose closure by (4.20) is

$$\mathbf{U}^* = \mathbf{R}^{(1)*}\mathbf{R}^{(2)*} \dots \mathbf{R}^{(p)*}, \tag{4.40}$$

and that the $\mathbf{C}^{(k)}$ matrices form the strictly lower triangular matrix $\mathbf{L} = \sum_{k=1}^{p-1} \mathbf{C}^{(k)}$,

whose closure by (4.19) is

$$\mathbf{L}^* = \mathbf{C}^{(p-1)*}\mathbf{C}^{(p-2)*} \dots \mathbf{C}^{(1)*}. \tag{4.41}$$

Hence (4.39) can be written as

$$\mathbf{A}^* = \mathbf{U}^*\mathbf{L}^*. \tag{4.42}$$

The product forms (4.39) and (4.42) both have obvious analogies in linear algebra.

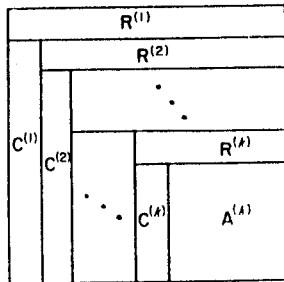


FIG. 1. Triangular decomposition.

To obtain a convenient method of calculating the successive $\mathbf{C}^{(k)}$, $\mathbf{A}^{(k)}$ and $\mathbf{R}^{(k)}$ matrices, we note firstly that from (4.37) and (3.7),

$$\mathbf{R}^{(k)*} = (\mathbf{e}_{0k}\mathbf{a}_{k0}^{(k-1)})^* = \mathbf{E} + \mathbf{e}_{0k}(\mathbf{a}_{kk}^{(k-1)})^*\mathbf{a}_{k0}^{(k-1)} \tag{4.43}$$

and hence

$$S^{(k)} = T^{(k)}R^{(k)*} = \sum_{i=k+1}^p e_{0i}(a_{i0}^{(k-1)} + a_{ik}^{(k-1)}(a_{kk}^{(k-1)})^* a_{k0}^{(k-1)}). \tag{4.44}$$

Therefore, by (4.37), the $C^{(k)}$ and $A^{(k)}$ matrices are given by

$$\begin{aligned} C^{(k)} &= s_{0k}^{(k)} e_{k0} = S^{(k)} e_{0k} e_{k0} \\ &= \sum_{i=k+1}^p e_{0i}(a_{ik}^{(k-1)} + a_{ik}^{(k-1)}(a_{kk}^{(k-1)})^* a_{kk}^{(k-1)}) e_{k0} \\ &= \sum_{i=k+1}^p e_{0i} a_{ik}^{(k-1)} (a_{kk}^{(k-1)})^* e_{k0}, \end{aligned} \tag{4.45}$$

and

$$\begin{aligned} A^{(k)} &= \sum_{j=k+1}^p s_{0j}^{(k)} e_{j0} = \sum_{j=k+1}^p S^{(k)} e_{0j} e_{j0} \\ &= \sum_{j=k+1}^p \sum_{i=k+1}^p e_{0i}(a_{ij}^{(k-1)} + a_{ik}^{(k-1)}(a_{kk}^{(k-1)})^* a_{kj}^{(k-1)}) e_{j0} \\ &= \sum_{j=k+1}^p \sum_{i=k+1}^p e_{0i}(a_{ij}^{(k-1)} + c_{ik}^{(k)} a_{kj}^{(k-1)}) e_{j0}. \end{aligned} \tag{4.46}$$

The matrix $R^{(k)}$ is already defined directly in terms of $A^{(k-1)}$ by (4.37).

Since the non-null elements of $R^{(1)}, R^{(2)}, \dots, R^{(k)}$ and $C^{(1)}, C^{(2)}, \dots, C^{(k)}$ and $A^{(k)}$ all occupy different positions (see Fig. 1), all the $R^{(k)}$ and $C^{(k)}$ matrices can be computed and recorded simply by performing $p-1$ successive transformations of the original A-matrix. Writing $M^{(0)} = A$, we compute $M^{(k)}$ ($k = 1, 2, \dots, p-1$), where the elements of $M^{(k)}$ are obtained using successively

$$m_{ij}^{(k)} = \begin{cases} m_{ik}^{(k-1)}(m_{kk}^{(k-1)})^* & \text{for } k < i \leq p, j = k & (4.47a) \\ m_{ij}^{(k-1)} + m_{ik}^{(k)} m_{kj}^{(k-1)} & \text{for } k < i, j \leq p, & (4.47b) \\ m_{ij}^{(k-1)} & \text{otherwise.} & (4.47c) \end{cases}$$

By comparing (4.47a) with (4.45), it will be seen that (4.47a) forms the non-null elements of $C^{(k)}$, and by comparing (4.47b) with (4.46), it is clear that this forms the non-null elements of $A^{(k)}$ (which include those of $R^{(k+1)}$); (4.47c) simply preserves the non-null elements of $R^{(1)}, R^{(2)}, \dots, R^{(k)}$ and $C^{(1)}, C^{(2)}, \dots, C^{(k-1)}$. Hence on termination, $M^{(p-1)}$ contains the non-null elements of all the $R^{(k)}$ and $C^{(k)}$ matrices, in their appropriate positions. If A is sparse, this fact can be exploited in the computation and storage of M (Knuth, 1968; Reid, 1971).

4.2.2. *The solution of equations.* From (4.42), the minimal solution of $Y = AY + B$ is

$$Y = A*B = U*L*B \tag{4.48}$$

which can be expressed as the minimal solution Y of the coupled system

$$F = LF + B \tag{4.49a}$$

$$Y = UY + F. \tag{4.49b}$$

Hence if we calculate L and U (which are the lower and upper triangles of $M^{(p-1)}$, as obtained by (4.47)), the required solution can be derived by applying the forward substitution method (4.24) to (4.49a), and then applying the back-substitution method

(4.26) to (4.49b), which give in turn $F = L^*B$ and $Y = U^*L^*B$. We note that since L is here *strictly* lower triangular, the forward substitution method (4.24) simplifies to

$$B^{(0)} = B, \quad B^{(k)} = B^{(k-1)} + I_{0k}b_{k0}^{(k-1)} \quad (k = 1, 2, \dots, p-1) \quad (4.50)$$

The above procedure is analogous to the Gauss elimination method in linear algebra.

4.2.3. *The computation of submatrices of A^* .* It is often necessary, for a given graph $G = (X, \Gamma)$, to determine the sum of all words which take node x_i to node x_j , for all $x_i \in V$ and $x_j \in W$, where V and W are subsets of X . This problem arises for instance when it is required to determine all the sequences of inputs which take a finite-state automaton from each of its initial states to each of its terminal states. In terms of the matrix A of G , this problem involves finding a submatrix H of A^* , composed of the intersection of each row a_{i0}^* where $x_i \in V$ with each column a_{0j}^* where $x_j \in W$.

In the particular case where complete columns of A^* are required, these can be obtained by applying the Gauss method to the equation $Y = AY + B$, where B is composed of the corresponding unit column vectors. (For each column a_{0j}^* of A^* can be expressed as A^*e_{0j} , which is the minimal solution of $Y = AY + e_{0j}$). Similarly, particular rows of A^* can be obtained by computing the product BA^* , where B is composed of the corresponding unit row vectors; this product can also be obtained by the Gauss method, since $(BA^*)^T$ is the minimal solution of $Y = A^T Y + B^T$.

To solve the general problem, we observe that any $s \times t$ submatrix H of A^* can be expressed as

$$H = PA^*Q = PU^*L^*Q \quad (4.51)$$

where P is an $s \times p$ matrix composed of s unit row vectors and Q is a $p \times t$ matrix composed of t unit column vectors. The expression (4.51) can be evaluated by a method analogous to the Aitken method (Fox, 1964), involving the formation of L and U , the products PU^* and L^*Q , and the product $(PU^*)(L^*Q)$.

As in linear algebra, the formation of L and U and the calculation of these products can be combined conveniently, by a simple extension of the algorithm (4.47): With

$$\tilde{M}^{(0)} = \begin{bmatrix} A & Q \\ P & \phi \end{bmatrix} \quad (4.52)$$

we form $\tilde{M}^{(k)}$ ($k = 1, 2, \dots, p$) where (cf. (4.47))

$$\tilde{m}_{ij}^{(k)} = \begin{cases} \tilde{m}_{ik}^{(k-1)}(\tilde{m}_{kk}^{(k-1)})^* & \text{for } k < i \leq p+s, j = k \\ \tilde{m}_{ij}^{(k-1)} + \tilde{m}_{ik}^{(k)}\tilde{m}_{kj}^{(k-1)} & \text{for } \begin{cases} k < i \leq p+s \\ k < j \leq p+t \end{cases} \\ \tilde{m}_{ij}^{(k-1)} & \text{otherwise.} \end{cases} \quad (4.53)$$

It is easily verified that at the k th stage of this algorithm,

$$\tilde{M}^{(k)} = \begin{bmatrix} M^{(k)} & Q^{(k)} \\ P^{(k)} & H^{(k)} \end{bmatrix} \quad (4.54)$$

where $M^{(k)}$ is defined in Section 4.2.1, and

$$\left. \begin{aligned} P^{(k)} &= PR^{(1)}R^{(2)} \dots R^{(k)} \\ Q^{(k)} &= C^{(k)}C^{(k-1)} \dots C^{(1)}Q \\ H^{(k)} &= \sum_{i=1}^k P_{0i}^{(i)}Q_{i0}^{(i)} \end{aligned} \right\} \quad (4.55)$$

which on termination give $P^{(p)} = PU^*$, $Q^{(p)} = L^*Q$, and $H^{(p)} = P^{(p)}Q^{(p)} = PU^*L^*Q$.

An application of this algorithm will be demonstrated in Section 6.

4.3. Woodbury's formula

Our method of deriving product forms for closure matrices, using (3.5)–(3.7), is based on the same principles as a method discussed by Householder (1953) for finding inverse matrices in linear algebra, involving repeated use of the formula:

$$(B + URV^T)^{-1} = B^{-1} - B^{-1}U(R^{-1} + V^TB^{-1}U)^{-1}V^TB^{-1}. \quad (4.56)$$

Indeed, by combining our relations (3.6) and (3.7) we obtain the analogous formula:

$$(A + USV^T)^* = A^* + A^*U(SV^TA^*U)^*SV^TA^*, \quad (4.57)$$

which can be verified as follows:

$$\begin{aligned} (A + USV^T)^* &= (A^*USV^T)^*A^* && \text{(by (3.6))} \\ &= (E + A^*U(SV^TA^*U)^*SV^T)A^* && \text{(by (3.7))} \\ &= A^* + A^*U(SV^TA^*U)^*SV^TA^*. && (4.58) \end{aligned}$$

To demonstrate that (4.56) and (4.57) are analogous, we replace the symbolism M^* by $(I - M)^{-1}$ in (4.57), which gives

$$(I - A - USV^T)^{-1} = (I - A)^{-1} + (I - A)^{-1}U(I - SV^T(I - A)^{-1}U)^{-1}SV^T(I - A)^{-1} \quad (4.59)$$

or

$$(I - A - USV^T)^{-1} = (I - A)^{-1} + (I - A)^{-1}U(S^{-1} - V^T(I - A)^{-1}U)^{-1}V^T(I - A)^{-1} \quad (4.60)$$

If in (4.60) we set $I - A = B$, and $S = -R$, we immediately obtain (4.56). It would have been possible to derive our product forms from (4.57), but it is more convenient to apply (3.5)–(3.7) separately.

As in linear algebra, the direct application of (4.57) is not usually to be recommended as a practical method of computing closure matrices, but it is sometimes useful for finding the modification of a closure matrix A^* which results from a change of a single element of A . In particular, from (4.57) the modification of A^* caused by adding σ to the element a_{ij} of A is given by

$$(A + e_{0i}\sigma e_{j0})^* = A^* + a_{0i}^*(\sigma a_{ji}^*)^* \sigma a_{j0}^*. \quad (4.61)$$

A concrete form of (4.61) has been derived from graph-theoretic considerations by Murchland (1967) and Rodionov (1968), who used it to calculate the changes in distances in a transportation network when one of its arc lengths is reduced.

5. Interpretations

In this section we shall consider various interpretations of the operators $+$, \cdot , and $*$ and show that the system F1 is in each case consistent with the interpretation. It is natural to consider first of all the most general form of a regular algebra. To this end, we define a regular algebra $R = (S, +, \cdot, *)$ to be *free* if and only if the only equalities holding between elements of S are those which are deducible using only the axioms A1–A11 and the rule of inference R1. Now consider a finite set V , and consider the set $S(V)$ of all regular expressions over $V \cup \{\phi\}$. Then we shall call the free regular algebra $R_F(V) = (S(V), +, \cdot, *)$ the free algebra *generated* by V .

Any interpretation for which the system F1 is consistent and complete will form

a free regular algebra. In general though $\mathcal{M}_p(R)$ for any algebra R and for $p > 1$ will not form a free algebra. For example, if $J_1 = \begin{bmatrix} \phi & \phi \\ a & \phi \end{bmatrix}$ and $J_2 = \begin{bmatrix} \phi & \phi \\ \phi & b \end{bmatrix}$, then $J_1 J_2 = N$, but this is not deducible from F1 alone.

Before discussing particular interpretations it is useful to note that the condition for uniqueness of solution of equations in regular algebra can be weakened as follows.

LEMMA 5.1. $(\exists T \neq N \text{ s.t. } T = A \cdot T) \Leftrightarrow (\exists T \neq N \text{ s.t. } T \preceq A \cdot T)$.

Proof. \Rightarrow is trivial. So let us assume $\exists T \neq N$ such that $T \preceq A \cdot T$. Then

$$T \preceq AT \Rightarrow A^*T \preceq A^*AT = AA^*T \quad (\text{by 3.3}).$$

But by A10,

$$A^*T \succeq AA^*T.$$

Hence

$$A^*T = A(A^*T),$$

i.e. $T' = A^*T = AT'$, and the lemma is proved.

5.1. Regular Languages

When we interpret $+$ as set union and \cdot as concatenation of words, we obtain the algebra of regular languages (see Section 2.2), denoted here by RL . If we then consider the algebra of all $p \times p$ matrices $\mathcal{M}_p(RL)$ over RL , then RL can be identified with $\mathcal{M}_1(RL)$. The consistency of $\mathcal{M}_p(RL)$ with F1 has been studied by Salomaa (1969). For this case the axioms A1–A11 are relatively easy to verify. However, Salomaa's condition for uniqueness of solutions of equations (rule R1) differs outwardly from ours. The relevant definition and theorem are given below.

Definition (Salomaa). A $p \times p$ matrix $M = [m_{ij}]$ possesses the *empty word property* (ewp) iff there is a sequence of numbers i_1, i_2, \dots, i_k ($k \geq 1$) such that

$$e \in m_{i_v, i_{v+1}} \quad \text{for } 1 \leq v \leq k-1 \quad \text{and} \quad e \in m_{i_k, i_1}.$$

THEOREM 5.1 (Salomaa). *If the matrix M does not possess ewp then the equation $Y = MY + R$ has a unique solution, namely $Y = M^*R$.*

For 1×1 matrices, i.e. regular languages, it is obvious that we have the equivalence: M does not possess ewp $\Leftrightarrow M$ is definite. The equivalence is not so obvious for larger matrices, but it is nevertheless easily proved.

THEOREM 5.2. *Let $A \in \mathcal{M}_p(RL)$. Then A does not possess ewp $\Leftrightarrow A$ is definite.*

Proof. (i) \Leftarrow . Suppose $\exists T \neq N$ such that $T = AT$. Then the equation $T = AT + N$ has more than one solution, namely T and N . Therefore A possesses ewp.

(ii) \Rightarrow . Suppose A possesses ewp. Then the labelled graph $G = (X, \Gamma)$ of A contains a cycle

$$\gamma = (x_{i_1}, x_{i_2}), (x_{i_2}, x_{i_3}), \dots, (x_{i_k}, x_{i_1}) \tag{5.1}$$

such that

$$l_{i_1 i_2} l_{i_2 i_3} \cdots l_{i_k i_1} \succeq e. \tag{5.2}$$

Now let H be the partial graph of G whose arcs are the arcs of γ and let B be the matrix of H . Clearly $B \preceq A$, so we may choose a matrix C such that $B + C = A$.

Now let $T = B^*$. By 5.2,

$$(b_{i_1 i_2} b_{i_2 i_3} \cdots b_{i_k i_1})(b_{i_1 i_2} b_{i_2 i_3} \cdots b_{i_k i_1})^* = (b_{i_1 i_2} b_{i_2 i_3} \cdots b_{i_k i_1})^* \tag{5.3}$$

and it follows that $T = BT$. But then

$$T \leq BT + CT = AT$$

and therefore, by Lemma 5.1, A is not definite.

Since the two characterizations of definiteness are equivalent, one can choose at will which to employ. As a test for definiteness Salomaa's characterization is undoubtedly better, but in proving theorems we have found our own algebraic characterization easier to use.

Finally, we note that F1 forms a complete system for regular languages (as proved also by Salomaa), which in turn means that the regular languages over the vocabulary V form the free regular algebra generated by V .

5.2. Generating Relations

Since any algebra is the homomorphic image of some free algebra, we can construct new examples of regular algebras by considering homomorphisms θ on regular algebras. Given any homomorphism θ on an algebra R we can define a congruence relation q_θ on R by

$$\alpha \equiv \beta(q_\theta) \Leftrightarrow \alpha\theta = \beta\theta$$

and it is well known that the homomorphic image $R\theta$ is isomorphic to the quotient algebra R/q_θ . Thus an alternative and equivalent approach to constructing new regular algebras is to consider congruence relations on the elements of the algebra. We can go one step further still: the quotient algebra R/q_θ may be considered to be the same as the algebra R excepting that, within R/q_θ , elements belonging to the same congruence class are now considered equal. Now, since q_θ is a congruence relation it can be completely specified by stating what equalities hold between the generators v_i of the free algebra R_F . Thus we can specify a quotient algebra by adding to the formal system F1 a list of *generating relations*, which are precisely the above-mentioned equalities holding between generators. The quotient algebra is then the maximal homomorphic image of R_F which is consistent with F1 and the new generating relations.

Some examples are given below.

5.3. Yoeli's Q -semiring

Consider the free regular algebra $R_F(V)$ generated by $V \cup \{\phi\}$ where $V = \{v_1, v_2, \dots, v_m\}$. Let us add to the system F1 the generating relations

$$e + v_i = e, \quad 1 \leq i \leq m. \tag{5.4}$$

Then one deduces that for all words $w = v_{i_1} v_{i_2} \cdots v_{i_k}$

$$e + w = e, \tag{5.5}$$

and hence to be consistent with A11,

$$w^* = e. \tag{5.6}$$

By induction on the number of occurrences of the star operator, one concludes that for all regular expressions α ,

$$e + \alpha = e \quad (5.7)$$

and

$$\alpha^* = e. \quad (5.8)$$

Since by (5.8) the value of α^* is trivial we may eliminate the operator $*$ from the algebra, and consider an algebra with the two operators $+$ and \cdot only. The axioms for this algebra, given by A1–A9 and (5.7) are easily recognized to be those of Yoeli's Q -semirings (Yoeli, 1961), which have been applied to various path-finding problems (Benzaken, 1968; Robert & Ferland, 1968). We shall denote this algebra by R_Q .

Let us now consider the algebra $\mathcal{M}_p(R_Q)$ of all $p \times p$ matrices over R_Q . Let A be any such matrix, and let $G = (X, \Gamma)$ be the corresponding labelled graph. We recall (Yoeli, 1961; BAC 71) that the elements of $A^r = [a_{ij}^r]$ may be expressed as

$$a_{ij}^r = \sum_{\mu \in M_{ij}^r} w(\mu) \quad (5.9)$$

where M_{ij}^r is the set of all paths from x_i to x_j of order r , and hence that $B^{(r)} = [b_{ij}^{(r)}] = E + A + A^2 + \cdots + A^r$ has elements

$$b_{ij}^{(r)} = \sum_{k=0}^r \sum_{\mu \in M_{ij}^k} w(\mu) \quad (5.10)$$

where, by definition, $w(\mu) = \phi$ for every open path μ of order zero and $w(\mu) = e$ for every closed path μ of order zero. Also we recall that (i) the maximal order of any elementary path is $p-1$, and (ii) that if μ' is any non-elementary path from x_i to x_j , then there exists a lower-order elementary path μ from x_i to x_j , which can be obtained from μ' by eliminating some of its arcs, and by (5.4), $w(\mu) + w(\mu') = w(\mu)$. It follows that $B^{(r)} = B^{(p-1)}$ for all $r \geq p-1$. We are therefore entitled to define $A^* = E + A + A^2 + \cdots + A^{p-1}$, and the validity of our axioms is assured by the following well-known theorem.

THEOREM 5.3. *Let $A \in \mathcal{M}_p(R_Q)$. Then the series $E + A + A^2 + \cdots$ is finitely convergent, with*

$$E + A + A^2 + \cdots + A^r = E + A + A^2 + \cdots + A^{p-1} = A^*, \text{ for all } r \geq p-1.$$

This algebra is applicable to several different types of path-finding problems, for instance (i) the determination of shortest or least-cost paths in transportation networks (subject to the restriction that all arc costs are non-negative) and (ii) the determination of routes with least probability of blockage in communication networks. (For details of these, and further references, see BAC 71, Section 2.1). Also, Benzaken (1968) has shown that this algebra can be used to enumerate the paths on a directed graph; this application will be discussed in detail in Section 7.

Unfortunately, for Q -semirings in general, it seems impossible to obtain a test for definiteness of the type which Salomaa has given for regular languages. However, it is possible to characterize definiteness for one very important class of Q -semirings—the distributive lattices—as will be shown below.

5.4. Distributive Lattices

Let us add to the axiom system R_Q the generating relations

$$v_i \cdot v_j = v_j \cdot v_i, \quad 1 \leq i, j \leq m, \quad (5.11)$$

and

$$v_i \cdot v_i = v_i, \quad 1 \leq i \leq m. \tag{5.12}$$

Now since (5.8) holds, we need only consider regular expressions formed from elements of V , the operators $+$ and \cdot , and parentheses; and furthermore, since we have the distributive laws A4 and A5, each of these expressions can be considered as a sum of words over V . It is therefore evident that by (5.11), for every pair of regular expressions α and β ,

$$\alpha \cdot \beta = \beta \cdot \alpha \tag{5.13}$$

and that by (5.11) and (5.12), for every regular expression α ,

$$\alpha \cdot \alpha = \alpha. \tag{5.14}$$

The axioms of R_Q together with (5.13) and (5.14) form the axiom system of distributive lattices, which we denote by R_{DL} .

In order to characterize definiteness for distributive lattices, we present the following.

THEOREM 5.4. *If the graph of a matrix $A \in \mathcal{M}_p(R_{DL})$ is acyclic then the equation $Y = AY + B$ has a unique solution, namely A^*B .*

Proof. Let Y_0 be an arbitrary solution of $Y = AY + B$, i.e. let

$$Y_0 = AY_0 + B. \tag{5.15}$$

Then by substitution we obtain

$$Y_0 = A(AY_0 + B) + B = A^2Y_0 + (E + A)B, \tag{5.16}$$

and by successive substitutions,

$$Y_0 = A^kY_0 + (E + A + A^2 + \dots + A^{k-1})B, \quad \text{for all } k \geq 1. \tag{5.17}$$

Hence by Theorem 5.3,

$$Y_0 = A^kY_0 + A^*B, \quad \text{for all } k \geq p. \tag{5.18}$$

But if the graph of A is acyclic then A^k is null for all $k \geq p$, in which case $Y_0 = A^*B$.

This theorem is the counterpart of Salomaa's Theorem 5.1 for regular languages; the counterpart of Theorem 5.2, which characterizes definiteness, is given below.

THEOREM 5.5. *Let $A \in \mathcal{M}_p(R_{DL})$ and let G be the graph of A . Then A is definite iff G is acyclic.*

Proof. Suppose A is not definite. Then $\exists Y \neq N$ such that $Y = AY$, and therefore the equation $Y = AY + N$ has more than one solution. Hence by Theorem 5.4, G is not acyclic.

Now suppose that G is not acyclic. Let γ be any cycle on G , let H be the partial graph of G whose arcs form γ , and let B be the matrix of H . Since $B \preceq A$, we may also choose some matrix C such that $B + C = A$. Let us denote the order of γ by r ; then it follows from (5.13) and (5.14) that

$$B^{r+s} = B^{kr+s}, \quad \text{for all } k \geq 1, s \geq 0. \tag{5.19}$$

Hence

$$B^qB^* = B^rB^*, \quad \text{for all } q \geq r. \tag{5.20}$$

If we now set $T = B^rB^*$, we have by (5.20) that $T = BT$. It follows that

$$T \preceq BT + CT = AT,$$

and therefore A is not definite.

As important examples of R_{DL} we have the Boolean algebras, which have many

applications in Automata Theory and Operational Research (Hammer & Rudeanu, 1968). Another example is the algebra proposed by Hu (1961) for finding maximal-capacity routes through networks.

5.5. *Benzaken's Algebra*

Our view of generating relations is similar to that of Benzaken (1968). As well as considering R_Q , he proposed the following algebra for enumerating the paths on a graph:

Consider a vocabulary $V = \{v_1, v_2, \dots, v_p\}$ and let R_B be the free regular algebra generated by V on which the following generating relations are imposed:

$$v_i \cdot \alpha \cdot v_i = v_i \cdot v_i = \phi, \quad (i = 1, 2, \dots, p) \tag{5.21}$$

for all languages α . In this algebra one can prove that

$$\alpha^* = e + \alpha, \tag{5.22}$$

and so once again the operator $*$ can be discarded.

To enumerate the elementary paths on a p -node graph $G = (X, \Gamma)$, we give a name v_i to each node $x_i \in X$, and we label each arc of G with the name of its terminal node, i.e. we set $l_{ij} = v_j$ for all $(x_i, x_j) \in \Gamma$. Then within the algebra $\mathcal{M}_p(R_B)$, the closure A^* of the matrix A of G gives all elementary paths on G : specifically, each product $\{v_i\} \cdot a_{ij}^*$ is a language of sequences of node names, each of these sequences defining an elementary path from x_i to x_j .

In this context, one well-known method of obtaining A^* is to set $M = E + A$ and then to compute successively M^2, M^4, \dots, M^{2^r} , where r is the first integer such that $2^r \geq p - 1$; then by Theorem 5.3, $M^{2^r} = A^*$. This is the "Latin multiplication method" first proposed by Kaufmann & Malgrange (1963) and subsequently re-invented by several authors. It would of course be less laborious to calculate A^* by one of the methods of Section 4; however an even more effective method, using R_Q , will be demonstrated in Section 7.

6. **A Comparison with our Network Routing Algebra**

There is obviously great similarity between regular algebra and the algebra presented in BAC 71. In particular, the definition of definiteness and the condition for uniqueness of solutions of equations in BAC 71 are almost identical to those given by Salomaa for regular languages (see Section 5.1 above). However, before we can make a precise comparison we must remove the obstacles caused by differences between the definitions used here and in BAC 71.

The earlier paper was concerned exclusively with the solution of extremal path problems, and its definition of A^* was tailored to this purpose. Let us here define \tilde{A} to be the matrix whose (i, j) th element is the sum of the path products of all elementary paths from x_i to x_j on the graph $G = (X, \Gamma)$ of A ; the matrix \tilde{A} as defined here corresponds to A^* in BAC 71 (Section 3.2). Now to relate \tilde{A} to the closure A^* of A we recall our previous definition of *semi-definiteness*, which can be paraphrased as follows: *Let A be a $p \times p$ matrix with graph G ; then A is semi-definite iff there is no closed path γ in G with path-product $w(\gamma) \succ e$.*

Now let R_C denote the algebra proposed in BAC 71. Then in addition to A1-A9 the following were assumed:

- (a) commutativity of multiplication, $\alpha \cdot \beta = \beta \cdot \alpha, \quad \forall \alpha, \beta,$
- (b) the order relation \leq is total, i.e. for any $\alpha, \beta,$ either $\alpha \leq \beta$ or $\beta \leq \alpha,$
- (c) the cancellation property:

$$\alpha \cdot \beta = \alpha \cdot \gamma \Rightarrow \beta = \gamma \quad \forall \gamma \neq \phi.$$

With the above properties holding in $R_C,$ the correspondence between \tilde{A} and our new definition of A^* is given by Theorem 4.1 of BAC 71, which we rephrase accordingly below.

THEOREM 6.1. *Let A be a $p \times p$ semi-definite matrix. Then the series $E + A + A^2 + \dots$ is finitely convergent, with*

$$E + A + A^2 + \dots + A^r = \tilde{A} = A^*, \quad \text{for all } r \geq p - 1.$$

We can now attempt to obtain R_C as a homomorphic image of regular algebra, in the following way. Consider any p -node graph G and its matrix $A.$ There are at most p^2 arcs in $G,$ and so we can take as a generating set $V = \{v_1, v_2, \dots, v_m\}$ where each v_i is a distinct label (or "measure" in the terminology of BAC 71) of some arc of $G,$ and $1 \leq m \leq p^2.$ To the axioms of regular algebra we can then add generating relations of the form

$$v_{i_1} + v_{i_2} = v_{i_1} \tag{6.1}$$

which give the order relation existing between every possible combination of elements of $V.$ We can also add the generating relations

$$v_i \cdot v_j = v_j \cdot v_i, \quad 1 \leq i, j \leq m. \tag{6.2}$$

to obtain commutativity of multiplication.

However, if we postulate the cancellative property (c), then when we attempt to define α^* for $\alpha > e$ we encounter difficulties. For $\alpha > e \Rightarrow \alpha\alpha^* \geq \alpha^*.$ But since $\alpha^* \geq \alpha\alpha^*$ by A10, we conclude that $\alpha^* = \alpha\alpha^*,$ and this equality violates the assumption (c) of cancellation. Thus we find that the axioms of regular algebra together with the additional axioms (a)–(c) form a consistent system only if we preclude the existence of α^* for $\alpha > e.$

It will be observed however that in BAC 71, the derivation of algorithms for calculating \tilde{A} and for solving equations of the form $Y = AY + B$ was given only for the case where A is semi-definite. Here, for any matrix A which is semi-definite, the closure A^* remains well-defined when we postulate the cancellative property, since Theorem 6.1 assures the validity of the axioms of regular algebra for such matrices. Furthermore if A is semi-definite, it can be proved that our derivations of algorithms in Section 4 all remain valid even when we preclude the existence of α^* for $\alpha > e.$ For this purpose we first prove the following.

THEOREM 6.2. *Let $A, B, C \in \mathcal{M}_p(R_C),$ and let $B, C \leq A.$ Then if A is semi-definite, all of B, C, B^*C and BC^* are also semi-definite.*

Proof. Let us assume that A is semi-definite. Then:

- (i) let G and H be the graphs of A and B respectively. By comparing the measures of corresponding elementary cycles on G and $H,$ it is clear that the maximal elementary cycle measure on H is not greater than the maximal elementary cycle measure on $G.$ Hence if A is semi-definite, B must be semi-definite. Equally C is semi-definite.

- (ii) Since every elementary cycle on G has a measure not greater than e , every non-elementary cycle on G also has a measure not greater than e . And since every elementary cycle on the graph G^* of A^* corresponds to a cycle on G , A^* must be semi-definite.

Now since B and C are semi-definite, their closures are well-defined, by Theorem 6.1. And since $B \preceq A$ and $C \preceq A$, $B^*C \preceq A^*A \preceq A^*$. It follows by argument (i) above that since A^* is semi-definite, B^*C must be semi-definite. Similarly, $BC^* \preceq AA^* \preceq A^*$, so BC^* is semi-definite.

From this theorem it follows that in (4.6), (4.13), and (4.37), the property of semi-definiteness is preserved in constructing $A^{(k)}$ from $A^{(k-1)}$. Accordingly, the graph $G^{(k-1)}$ of $A^{(k-1)}$ never contains any loop l with $w(l) > e$, so we never have $a_{kk}^{(k-1)} > e$, and hence in all the algorithms of Section 4, the closure of each pivotal element $a_{kk}^{(k-1)}$ always exists.

In BAC 71, the concept of semi-definiteness was given the following physical interpretation. Consider the concrete form of $R_C = (S, +, \cdot)$ where S is the set of real numbers together with $+\infty$, $a+b$ is defined as $\min(a, b)$, and $a \cdot b$ is the arithmetic sum of a and b . Also, let G be a graph whose arc labels represent length, and let A be the matrix of G . Now if A is semi-definite, $A^* = \tilde{A}$, and so each element a_{ij}^* of A^* is the distance (i.e. the length of a shortest path) from x_i to x_j . If A is not semi-definite, G contains at least one cycle of negative length, and the concept of distance becomes meaningless. In these circumstances it is not surprising that the series $E + A + A^2 + \dots$ fails to converge, and we would not expect A^* to exist. Thus we find that in BAC 71, methods of solving the equation $Y = AY + B$ are derived only for those cases where it is meaningful, and for those cases our present derivations using regular algebra remain valid.

7. An Illustrative Example: The Enumeration of Paths on a Graph

To illustrate some of the results of earlier sections of the paper we shall now consider the following problems: Given a graph $G = (X, \Gamma)$ and two specified subsets X_1 and

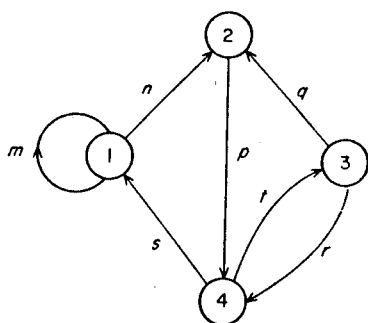


FIG. 2.

X_2 of X , find for each node $x_i \in X_1$ and each node $x_j \in X_2$, (a) the set of all paths from x_i to x_j , and (b) the set of all elementary paths from x_i to x_j . As specific examples, we shall solve these problems for the graph of Fig. 2, with $X_1 = \{x_3\}$ and $X_2 = \{x_2, x_4\}$.

Let us give the arcs of G distinct names (Fig. 2). If we consider these arc labels as regular languages, then in $\mathcal{M}_p(RL)$ each element a_{ij}^* of the closure A^* of the matrix A corresponding to G is the set of all words taking node x_i to x_j (see Section 2.2.2); and since the arc labels on G are distinct, there is a one-one correspondence between words in a_{ij}^* and paths from x_i to x_j . Hence problem (a) involves finding the elements a_{32}^* and a_{34}^* , using $\mathcal{M}_p(RL)$.

These elements can be found efficiently by using the Gauss method to form the third row of A^* , or alternatively, by applying the Aitken method (4.53) to the matrix

$$\tilde{M}^{(0)} = \left[\begin{array}{cccc|cc} m & n & \phi & \phi & \phi & \phi \\ \phi & \phi & \phi & p & e & \phi \\ \phi & q & \phi & r & \phi & \phi \\ s & \phi & t & \phi & \phi & e \\ \hline \phi & \phi & e & \phi & \phi & \phi \end{array} \right]$$

where $e = \phi^*$. Following the latter procedure, we obtain successively

$$\tilde{M}^{(1)} = \left[\begin{array}{cccc|cc} m & n & \phi & \phi & \phi & \phi \\ \phi & \phi & \phi & p & e & \phi \\ \phi & q & \phi & r & \phi & \phi \\ sm^* & sm^*n & t & \phi & \phi & e \\ \hline \phi & \phi & e & \phi & \phi & \phi \end{array} \right],$$

$$\tilde{M}^{(2)} = \left[\begin{array}{cccc|cc} m & n & \phi & \phi & \phi & \phi \\ \phi & \phi & \phi & p & e & \phi \\ \phi & q & \phi & r+qp & q & \phi \\ sm^* & sm^*n & t & sm^*np & sm^*n & e \\ \hline \phi & \phi & e & \phi & \phi & \phi \end{array} \right],$$

$$\tilde{M}^{(3)} = \left[\begin{array}{cccc|cc} m & n & \phi & \phi & \phi & \phi \\ \phi & \phi & \phi & p & e & \phi \\ \phi & q & \phi & r+qp & q & \phi \\ sm^* & sm^*n & t & sm^*np+t(r+qp) & sm^*n+ tq & e \\ \hline \phi & \phi & e & r+qp & q & \phi \end{array} \right].$$

The final matrix $\tilde{M}^{(4)}$ is identical to $\tilde{M}^{(3)}$ except in the last three elements of its final row, which are

$$\begin{aligned} \tilde{m}_{54}^{(4)} &= (r+qp)(sm^*np+t(r+qp))^*, \\ \tilde{m}_{55}^{(4)} &= q+(r+pq)(sm^*np+t(r+qp))^*(sm^*n+ tq), \\ \tilde{m}_{56}^{(4)} &= (r+qp)(sm^*np+t(r+qp))^*. \end{aligned}$$

The last two of these define the required paths, since $\tilde{m}_{55}^{(4)} = a_{32}^*$ and $\tilde{m}_{56}^{(4)} = a_{34}^*$. It is to be noted that in general, if one re-orders the nodes of G (or simultaneously permutes rows and columns of A) then one obtains different regular expressions for the set of paths between a specified pair of nodes, although of course all such expressions are equivalent.

Considering now problem (b), it follows from our discussion in Section 5.3 that this problem can be solved in the same manner as problem (a), but using in place of RL the homomorphic image of RL having the additional axioms (5.7) and (5.8), viz. $e + \alpha = e$ and $\alpha^* = e$. The Aitken method (4.53) then takes the simpler form

$$\tilde{m}_{ij}^{(k)} = \begin{cases} \tilde{m}_{ij}^{(k-1)} + \tilde{m}_{ik}^{(k-1)}\tilde{m}_{kj}^{(k-1)} & \text{for } \begin{cases} k < i \leq p+s, \\ k < j \leq p+t, \end{cases} \\ \tilde{m}_{ij}^{(k-1)} & \text{otherwise,} \end{cases} \quad (7.1)$$

and applying this to the matrix $\tilde{M}^{(0)}$ defined above we obtain

$$\tilde{M}^{(1)} = \left[\begin{array}{cccc|cc} m & n & \phi & \phi & \phi & \phi \\ \phi & \phi & \phi & p & e & \phi \\ \phi & q & \phi & r & \phi & \phi \\ s & sn & t & \phi & \phi & e \\ \hline \phi & \phi & e & \phi & \phi & \phi \end{array} \right],$$

$$\tilde{M}^{(2)} = \left[\begin{array}{cccc|cc} m & n & \phi & \phi & \phi & \phi \\ \phi & \phi & \phi & p & e & \phi \\ \phi & q & \phi & r+qp & q & \phi \\ s & sn & t & snp & sn & e \\ \hline \phi & \phi & e & \phi & \phi & \phi \end{array} \right],$$

$$\tilde{M}^{(3)} = \left[\begin{array}{cccc|cc} m & n & \phi & \phi & \phi & \phi \\ \phi & \phi & \phi & p & e & \phi \\ \phi & q & \phi & r+qp & q & \phi \\ s & sn & t & snp+tr+qtp & sn+ tq & e \\ \hline \phi & \phi & e & r+qp & q & \phi \end{array} \right],$$

$$\tilde{M}^{(4)} = \left[\begin{array}{cccc|cc} m & n & \phi & \phi & \phi & \phi \\ \phi & \phi & \phi & p & e & \phi \\ \phi & q & \phi & r+qp & q & \phi \\ s & sn & t & snp+tr+qtp & sn+ tq & e \\ \hline \phi & \phi & e & r+qp & q+rsn & r+qp \end{array} \right].$$

Hence there are two elementary paths from x_3 to x_2 , viz. “ q ” and “ rsn ”, and there are also two elementary paths from x_3 to x_4 , viz. “ r ” and “ qp ”.

It is important to note that in applying (7.1), the concatenation $\tilde{m}_{ik}^{(k-1)}\tilde{m}_{kj}^{(k-1)}$ in general contains words which represent non-elementary paths, and that to eliminate all such words from the solution it is necessary to apply (5.7), i.e. to perform all possible absorptions of the type

$$a_1 a_2 \cdots a_r + b_1 a_1 \cdots b_k a_k \cdots a_r b_{r+1} = a_1 a_2 \cdots a_r. \quad (7.2)$$

For instance, in forming $\tilde{m}_{35}^{(4)}$ in the above example we have

$$\tilde{m}_{34}^{(3)}\tilde{m}_{45}^{(3)} = (r+qp)(sn+ tq) = rsn+rtq+qpsn+qptq,$$

giving

$$\begin{aligned} \tilde{m}_{55}^{(3)} &= q + rsn + rtq + qpsn + qptq \\ &= q + rsn, \quad \text{by (7.2).} \end{aligned}$$

In our very simple example, words representing non-elementary paths are generated only in the calculation of $\tilde{M}^{(4)}$, but in general this can happen at any stage of the computation, and for larger graphs the work involved in applying (7.2) is quite prohibitive.

However, with the Aitken method in particular—which involves only a sequence of eliminations and no back-substitutions—it is easy to prevent the generation of unwanted words. We shall give an indication of how this can be done, because the resulting path enumeration method is the most efficient one known to us.

To obtain the process, it is convenient to consider the Aitken method in graph-theoretic terms: We observe that the application of (7.1) to the matrix $\tilde{M}^{(0)} = \begin{bmatrix} \mathbf{A} & \mathbf{Q} \\ \mathbf{P} & \Phi \end{bmatrix}$

is equivalent to the application of the algorithm

$$\tilde{m}_{ij}^{(k)} = \begin{cases} \tilde{m}_{ij}^{(k-1)} + \tilde{m}_{ik}^{(k-1)}\tilde{m}_{kj}^{(k-1)} & \text{for } k < i, j \leq p+s+t, \\ \tilde{m}_{ij}^{(k-1)} & \text{otherwise} \end{cases} \quad (7.3)$$

to the matrix

$$\tilde{M}^{(0)} = \begin{bmatrix} \mathbf{A} & \Phi_{12} & \mathbf{Q} \\ \mathbf{P} & \Phi_{22} & \Phi_{23} \\ \Phi_{31} & \Phi_{32} & \Phi_{33} \end{bmatrix} \quad (7.4)$$

where Φ_{22} and Φ_{33} are square matrices of order s and t respectively, in that at the k th stage (for $k = 1, 2, \dots, p$) we have (cf. (4.54)):

$$\tilde{M}^{(k)} = \begin{bmatrix} \mathbf{M}^{(k)} & \Phi_{12} & \mathbf{Q}^{(k)} \\ \mathbf{P}^{(k)} & \Phi_{22} & \mathbf{H}^{(k)} \\ \Phi_{31} & \Phi_{32} & \Phi_{33} \end{bmatrix}. \quad (7.5)$$

With \mathbf{P} and \mathbf{Q} defined as in Section 4.2.3, the augmented matrix $\tilde{M}^{(0)}$ of (7.4) has a graph $G^a = (X \cup X'_1 \cup X'_2, \Gamma \cup \psi_1 \cup \psi_2)$ where $X'_1 = \{x'_{i1}, x'_{i2}, \dots, x'_{is}\}$ and $X'_2 = \{x'_{j1}, x'_{j2}, \dots, x'_{jt}\}$ are sets of "duplicates" of the nodes of $X_1 = \{x_{i1}, x_{i2}, \dots, x_{is}\}$ and $X_2 = \{x_{j1}, x_{j2}, \dots, x_{jt}\}$ respectively, ψ_1 is a set of arcs joining each node $x'_{ik} \in X'_1$ to the corresponding node $x_{jk} \in X_1$, and ψ_2 is a set of arcs joining each node $x_{jk} \in X_2$ to the corresponding node $x'_{ik} \in X'_2$, each arc of ψ_1 and ψ_2 being labelled with $e = \phi^*$.

Now with reference to the augmented matrix (7.4) and its graph G^a , it is clear that in the Aitken method, each element $\tilde{m}_{ij}^{(k)}$ for $i, j > k$ is the sum of all words corresponding to paths from x_i to x_j whose intermediate nodes (if any) all belong to the set $S_k = \{x_1, x_2, \dots, x_k\}$. This has two important consequences concerning the execution of the method.

(a) Since the absorption rule (7.2) holds, in forming each element $\tilde{m}_{ij}^{(k)}$ using (7.1) it is not necessary to add to $\tilde{m}_{ij}^{(k-1)}$ any word $\alpha\beta$ of the concatenation

$$\tilde{m}_{ik}^{(k-1)}\tilde{m}_{kj}^{(k-1)} = \{\alpha\beta \mid \alpha \in \tilde{m}_{ik}^{(k-1)}, \quad \beta \in \tilde{m}_{kj}^{(k-1)}\} \quad (7.6)$$

for which the corresponding path $\mu(\alpha\beta)$ is non-elementary.

(b) If the words of $\tilde{M}^{(k-1)}$ all represent elementary paths (and this is evidently true for $\tilde{M}^{(0)}$), then it is easy to determine whether any word $\alpha\beta$ of the concatenation (7.6) represents a non-elementary path, which in turn makes it possible to exclude words representing non-elementary paths from $\tilde{M}^{(k)}$. For if $\mu(\alpha)$ and $\mu(\beta)$ are both elementary, then $\mu(\alpha\beta)$ is non-elementary only if $\mu(\alpha)$ and $\mu(\beta)$ have at least one of their intermediate nodes in common. But then α and β can each be split into two subwords: $\alpha = \alpha_1\alpha_2$ and $\beta = \beta_1\beta_2$, such that $\mu(\alpha_2\beta_1)$ is an elementary cycle. In this case $\mu(\beta_1\alpha_2)$ is also an elementary cycle; and since it has initial and terminal nodes x_k and all its intermediate nodes belong to S_{k-1} , $\beta_1\alpha_2 \in \tilde{m}_{kk}^{(k-1)}$. Conversely, it is evident that if α and β have splittings $\alpha = \alpha_1\alpha_2$ and $\beta = \beta_1\beta_2$ such that $\beta_1\alpha_2 \in \tilde{m}_{kk}^{(k-1)}$, then $\mu(\alpha\beta)$ is non-elementary.

Thus we can execute (7.1), excluding all words representing non-elementary paths, in the following manner. For each word $\alpha \in \tilde{m}_{ik}^{(k-1)}$ in turn,

(a) Form the set T_α as follows: For each $\gamma \in \tilde{m}_{kk}^{(k-1)}$, find its longest final subword γ_f which is also a final subword of α ; if this subword is non-empty then assign to T_α the word γ_a obtained by removing γ_f from γ .

(b) For each word $\beta \in m_{kj}^{(k-1)}$, add $\alpha\beta$ to $\tilde{m}_{ij}^{(k-1)}$ if and only if no word of T_α is an initial subword of β .

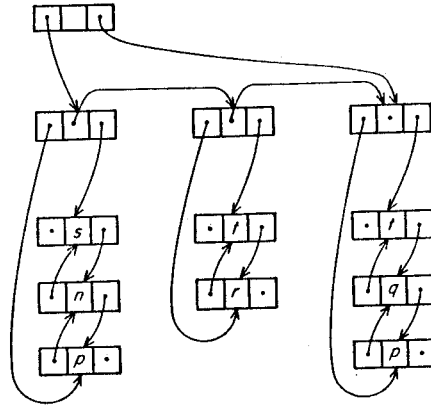


FIG. 3. List representation of $\tilde{m}_{44}^{(3)}$.

This process can be performed conveniently on a computer by representing words by doubly-linked lists (Knuth, 1968) of the form shown in Fig. 3. Using this type of representation the performance of the Aitken method compares favourably with that of the well-known search method employing a stack (Kroft, 1967). For instance, for a 24-node graph representing an electrical switching network (Fig. 5 of Carré & Ladley, 1972), the time taken for the reduction of its A-matrix by the Aitken method is equivalent to that used by the stack method for only five origin-destination pairs. For each additional column of \tilde{M} , the average time required is one-quarter of that used by the stack method for a single origin-destination pair.

Finally we note that some methods of enumerating elementary paths which have been presented by other authors are also related to methods of Section 4. For instance

the methods of Benzaken (1968) and Murchland (1965) are both applications of the Jordan method to the equation $Y = AY + A$.

8. Conclusions

It is remarkable how much of the theory of real matrices holds in regular algebra. One might speculate about the possibility of defining concepts similar to those of eigenvectors and eigenvalues for matrices on regular algebras, where the latter could be related to path products of cycles on the graphs of these matrices. This possibility can be dismissed however, because the existence of eigenvectors and eigenvalues is tautologous with the Cayley–Hamilton theorem, which depends for its proof on the notion of linear dependence in a p -dimensional vector space. But in regular algebra one has in general no notion of linear dependence.

Most of our methods of solving equations will be recognized by regular algebraists as techniques which have been in use for some years. However, the derivation of the methods in terms of product forms is perhaps helpful in relating the methods to each other, and to their counterparts in linear algebra. Of course we have not attempted to catalogue all the possibilities, and there are several other well-known methods which can be derived from results in Section 4. For instance the escalator method, which has been used both in automata theory (Eggan, 1963) and in operational research (BAC 71), can be regarded as a reverse application of triangular decomposition, and the formulae defining this method can be derived directly from (4.38).

Finally, it is interesting to observe that most, if not all, path-finding algebras can be regarded as homomorphic images of free regular algebras. The results of Sections 3 and 4 therefore have numerous practical applications outside the context of regular languages.

R. C. Backhouse would like to acknowledge the Science Research Council for financial support for this work, and also thank his supervisor Mr R. J. Cunningham for his help and encouragement while the work was in progress.

B. A. Carré is grateful to the Centre National de la Recherche Scientifique and the Délégation Générale à la Recherche Scientifique et Technique for their financial support.

REFERENCES

- BARRON, D. W. 1968 *Recursive techniques in programming*. London: Macdonald.
 BENZAKEN, C. 1968 In (G. Biorci (Ed.)) *Network and switching theory*. New York: Academic Press.
 CARRÉ, B. A. 1971 *J. Inst. Maths Applics* **7**, 273–294.
 CARRÉ, B. A. & LADLEY, R. B. 1972 *Proc. IEE* **119**, 1188–1196.
 CONWAY, J. H. 1971 *Regular algebra and finite machines*. London: Chapman and Hall.
 EGGAN, L. C. 1963 *Mich. math. J.* **10**, 385–397.
 FOX, L. 1964 *An introduction to numerical linear algebra*. Oxford: Clarendon Press.
 HAMMER, P. L. & RUDEANU, S. 1968 *Boolean methods in operational research*. Berlin: Springer-Verlag.
 HOUSEHOLDER, A. S. 1953 *Principles of numerical analysis*. New York: McGraw-Hill.
 HU, T. C. 1961 *Op. Res.* **9**, 898–900.
 KAUFMANN, A. & MALGRANGE, Y. 1963 *Revue fr. Rech. Opér.* No. 26, 61–73.

- KNUTH, D. E. 1968 *The art of computer programming, Vol. 1. Fundamental algorithms*. Reading, Mass.: Addison-Wesley.
- KROFT, D. 1967 *Proc. IEEE* **55**, 88-90.
- MURCHLAND, J. D. 1965 *Report LSE-TNT-22*. London School of Economics.
- MURCHLAND, J. D. 1967 *Report LSE-TNT-26*. London School of Economics.
- REID, J. K. (Ed.) 1971 *Large sparse sets of linear equations (Proc. I. M. A. Conf., Oxford, 1970)*. London: Academic Press.
- RODIONOV, V. V. 1968 *USSR Comput. Math. math. Phys.* **8**, 336-343.
- ROBERT, F. & FERLAND, J. 1968 *Revue fr. Informat. Rech. Opér.* **2**, 71-85.
- SALOMAA, A. 1969 *Theory of automata*. Oxford: Pergamon Press.
- WARSHALL, S. 1962 *J. Assoc. Comput. Mach.* **9**, 11-13.
- YOELI, M. 1961 *Am. math. Monthly* **68**, 552-557.