Kleene Algebra — Lecture 4

ESSLLI 2023

Last lecture

- Automata as language acceptors, and decidability of bisimilarity.
- One half of Kleene's theorem: expressions to automata.
- Antimirov's construction: automaton with expressions as states.
- The Fundamental Theorem of KA.

Today's lecture

- The *other* half of Kleene's theorem: automata to expressions.
- Approach: solving a system of equations using the laws of KA.
- Matrices and vectors over expressions as a helpful tool.

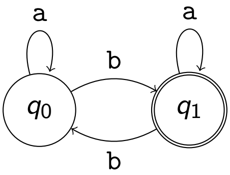
Automata to expressions — statement

Theorem (Kleene '56)

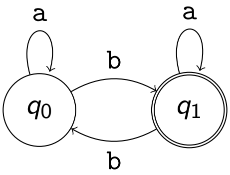
Let $A = \langle Q, \rightarrow, I, F \rangle$ be a finite automaton, with $q \in Q$.

We can construct $e \in \mathbb{E}$ such that $[\![e]\!]_{\mathbb{E}} = L_A(q)$.

Automata to expressions — ad hoc

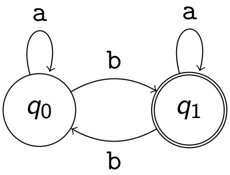


Automata to expressions — ad hoc



From q_0 to q_0, passing through q_0 and q_1: $(\mathtt{a} + \mathtt{b} \cdot \mathtt{a}^* \cdot \mathtt{b})^*$

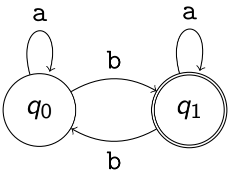
Automata to expressions — ad hoc



From q_0 to q_0, passing through q_0 and q_1: $(\mathtt{a} + \mathtt{b} \cdot \mathtt{a}^* \cdot \mathtt{b})^*$

From q_1 to q_1, passing through q_1 but not through q_0: $\mathtt{a}^*$

Automata to expressions — ad hoc

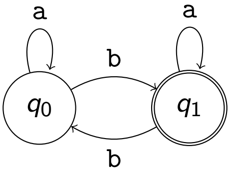


From q_0 to q_0, passing through q_0 and q_1: $(\mathtt{a} + \mathtt{b} \cdot \mathtt{a}^* \cdot \mathtt{b})^*$

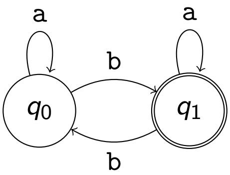
From q_1 to q_1, passing through q_1 but not through q_0: $\mathtt{a}^*$

From q_0 to q_1: $(\mathtt{a} + \mathtt{b} \cdot \mathtt{a}^* \cdot \mathtt{b})^* \cdot \mathtt{b} \cdot \mathtt{a}^*$.

Automata to expressions — solving equations

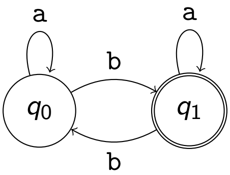


Automata to expressions — solving equations



Suppose $[\![e_0]\!]_{\mathbb{E}} = L(q_0)$, and $[\![e_1]\!]_{\mathbb{E}} = L(q_1)$; then:

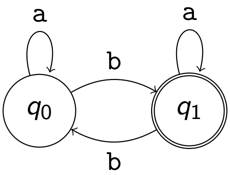
Automata to expressions — solving equations



Suppose $[\![e_0]\!]_{\mathbb{E}} = L(q_0)$, and $[\![e_1]\!]_{\mathbb{E}} = L(q_1)$; then:

$$\mathtt{a} \cdot e_0 \leqq e_0 \qquad \mathtt{b} \cdot e_1 \leqq e_0 \qquad \mathtt{a} \cdot e_1 \leqq e_1 \qquad \mathtt{b} \cdot e_0 \leqq e_1 \qquad 1 \leqq e_1$$

Automata to expressions — solving equations



Suppose $[\![e_0]\!]_{\mathbb{E}} = L(q_0)$, and $[\![e_1]\!]_{\mathbb{E}} = L(q_1)$; then:

$$\begin{aligned} \mathtt{a} \cdot e_0 + \mathtt{b} \cdot e_1 &\leqq e_0 \\ 1 + \mathtt{a} \cdot e_1 + \mathtt{b} \cdot e_0 &\leqq e_1 \end{aligned}$$

Automata to expressions — solving equations

Recall the constraints we derived:

$$\mathtt{a} \cdot e_0 + \mathtt{b} \cdot e_1 \leqq e_0 \tag{1}$$

$$1 + \mathtt{a} \cdot e_1 + \mathtt{b} \cdot e_0 \leqq e_1 \tag{2}$$

Automata to expressions — solving equations

Recall the constraints we derived:

$$\mathtt{a} \cdot e_0 + \mathtt{b} \cdot e_1 \leqq e_0 \tag{1}$$

$$(1 + \mathtt{b} \cdot e_0) + \mathtt{a} \cdot e_1 \leqq e_1 \tag{2}$$

Automata to expressions — solving equations

Recall the constraints we derived:

$$\mathtt{a} \cdot e_0 + \mathtt{b} \cdot e_1 \leqq e_0 \tag{1}$$

$$(1 + \mathtt{b} \cdot e_0) + \mathtt{a} \cdot e_1 \leqq e_1 \tag{2}$$

By the fixpoint axiom:

$$\mathtt{a}^* \cdot (1 + \mathtt{b} \cdot e_0) \leqq e_1 \tag{3}$$

Automata to expressions — solving equations

Recall the constraints we derived:

$$\mathtt{a} \cdot e_0 + \mathtt{b} \cdot e_1 \leqq e_0 \tag{1}$$

$$(1 + \mathtt{b} \cdot e_0) + \mathtt{a} \cdot e_1 \leqq e_1 \tag{2}$$

By the fixpoint axiom:

$$\mathtt{a}^* \cdot (1 + \mathtt{b} \cdot e_0) \leqq e_1 \tag{3}$$

Filling (3) into (1)

$$\mathtt{a} \cdot e_0 + \mathtt{b} \cdot (\mathtt{a}^* \cdot (1 + \mathtt{b} \cdot e_0)) \leqq e_0 \tag{4}$$

Automata to expressions — solving equations

Recall the constraints we derived:

$$\mathtt{a} \cdot e_0 + \mathtt{b} \cdot e_1 \leqq e_0 \tag{1}$$

$$(1 + \mathtt{b} \cdot e_0) + \mathtt{a} \cdot e_1 \leqq e_1 \tag{2}$$

By the fixpoint axiom:

$$\mathtt{a}^* \cdot (1 + \mathtt{b} \cdot e_0) \leqq e_1 \tag{3}$$

Filling (3) into (1)

$$\mathtt{b} \cdot \mathtt{a}^* + (\mathtt{a} + \mathtt{b} \cdot \mathtt{a}^* \cdot \mathtt{b}) \cdot e_0 \leqq e_0 \tag{4}$$

Automata to expressions — solving equations

Recall the constraints we derived:

$$\mathtt{a} \cdot e_0 + \mathtt{b} \cdot e_1 \leqq e_0 \tag{1}$$

$$(1 + \mathtt{b} \cdot e_0) + \mathtt{a} \cdot e_1 \leqq e_1 \tag{2}$$

By the fixpoint axiom:

$$\mathtt{a}^* \cdot (1 + \mathtt{b} \cdot e_0) \leqq e_1 \tag{3}$$

Filling (3) into (1)

$$\mathtt{b} \cdot \mathtt{a}^* + (\mathtt{a} + \mathtt{b} \cdot \mathtt{a}^* \cdot \mathtt{b}) \cdot e_0 \leqq e_0 \tag{4}$$

Applying the fixpoint rule to (4):

$$(\mathtt{a} + \mathtt{b} \cdot \mathtt{a}^* \cdot \mathtt{b})^* \cdot \mathtt{b} \cdot \mathtt{a}^* \leqq e_0$$

Automata to expressions — solving automata

Definition (Solution)

Let $A = \langle Q, \rightarrow, I, F \rangle$ be an automaton.

A *solution* to A is a function $s : Q \rightarrow \mathbb{E}$, such that for all $q \in Q$ it holds that

$$[q \in F] + \sum_{q \xrightarrow{\mathtt{a}} q'} \mathtt{a} \cdot s(q') \leqq s(q)$$

Automata to expressions — solving automata

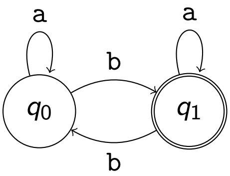
Definition (Solution)

Let $A = \langle Q, \rightarrow, I, F \rangle$ be an automaton.

A *solution* to A is a function $s : Q \rightarrow \mathbb{E}$, such that for all $q \in Q$ it holds that

$$[q \in F] + \sum_{q \xrightarrow{\mathtt{a}} q'} \mathtt{a} \cdot s(q') \leqq s(q)$$

Example:



$\rightsquigarrow$

$$0 + \mathtt{a} \cdot s(q_0) + \mathtt{b} \cdot s(q_1) \leqq s(q_0)$$

$$1 + \mathtt{a} \cdot s(q_1) + \mathtt{b} \cdot s(q_0) \leqq s(q_1)$$

Automata to expressions — solving automata

Definition (Least solution)

Let A be an automaton, and let s be a solution to A.

We say that s is a *least* solution to A when s is (pointwise) least w.r.t. $\leqq$; i.e:

$$\forall \text{ solutions } s', q \in Q.\ s(q) \leqq s'(q)$$

Automata to expressions — solving automata

Definition (Least solution)

Let A be an automaton, and let s be a solution to A.

We say that s is a *least* solution to A when s is (pointwise) least w.r.t. $\leqq$; i.e:

$$\forall \text{ solutions } s', q \in Q.\ s(q) \leqq s'(q)$$

Lemma

Let $A = \langle Q, \rightarrow, I, F \rangle$ be an automaton, and let $s : Q \rightarrow \mathbb{E}$ be a least solution to A.

Then $[\![s(q)]\!]_{\mathbb{E}} = L(q)$ for all $q \in Q$.

Vectors and matrices

Definition (Vectors and matrices)

Let S be a set.

An *S-vector (over $\mathbb{E}$)* is a function $v : S \to \mathbb{E}$.

An *S-matrix (over $\mathbb{E}$)* is a function $M : S \times S \to \mathbb{E}$.

Vectors and matrices — example

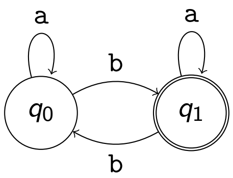
Ex.: let $A = \langle Q, \rightarrow, I, F \rangle$ be an automaton; define:

$$M_A(q, q') = \sum_{q \xrightarrow{\mathtt{a}} q'} \mathtt{a}$$

Vectors and matrices — example

Ex.: let $A = \langle Q, \to, I, F \rangle$ be an automaton; define:

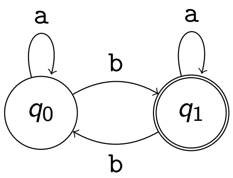
$$M_A(q, q') = \sum_{q \xrightarrow{\mathtt{a}} q'} \mathtt{a}$$



Vectors and matrices — example

Ex.: let $A = \langle Q, \rightarrow, I, F \rangle$ be an automaton; define:

$$M_A(q, q') = \sum_{q \xrightarrow{\mathtt{a}} q'} \mathtt{a}$$



Can write out matrices as tables, vectors as columns:

$$M_A = \begin{bmatrix} \mathtt{a} & \mathtt{b} \\ \mathtt{b} & \mathtt{a} \end{bmatrix} \qquad s = \begin{bmatrix} e_0 \\ e_1 \end{bmatrix}$$

Vectors and matrices — operations

Definition (Operations and equivalence on vectors and matrices)

Let S be a finite set, let s, t be S-vectors, and let M be an S-matrix.

Vectors and matrices — operations

Definition (Operations and equivalence on vectors and matrices)

Let S be a finite set, let s, t be S-vectors, and let M be an S-matrix.

The S-vectors $s + t$ and $M \cdot s$ are defined by

$$(s + t)(x) = s(x) + t(x) \qquad (M \cdot s)(x) = \sum_{y \in S} M(x, y) \cdot s(y)$$

Vectors and matrices — operations

Definition (Operations and equivalence on vectors and matrices)

Let S be a finite set, let s, t be S-vectors, and let M be an S-matrix.

The S-vectors $s + t$ and $M \cdot s$ are defined by

$$(s + t)(x) = s(x) + t(x) \qquad\qquad (M \cdot s)(x) = \sum_{y \in S} M(x, y) \cdot s(y)$$

Lastly, we extend equivalence to S-vectors in a pointwise manner:

$$s \equiv t \iff \forall x \in S.\ s(x) \equiv t(x)$$

Just like before $s \leqq t \iff s + t \equiv t$.

Vectors and matrices — operations

$$\left.\begin{aligned} 0 + \mathtt{a} \cdot s(q_0) + \mathtt{b} \cdot s(q_1) &\leqq s(q_0) \\ 1 + \mathtt{b} \cdot s(q_0) + \mathtt{a} \cdot s(q_1) &\leqq s(q_1) \end{aligned}\right\} \iff \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} \mathtt{a} & \mathtt{b} \\ \mathtt{b} & \mathtt{a} \end{bmatrix} \cdot \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix} \leqq \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix}$$

Vectors and matrices — operations

$$\left.\begin{aligned} 0 + \mathtt{a} \cdot s(q_0) + \mathtt{b} \cdot s(q_1) &\leqq s(q_0) \\ 1 + \mathtt{b} \cdot s(q_0) + \mathtt{a} \cdot s(q_1) &\leqq s(q_1) \end{aligned}\right\} \iff \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} \mathtt{a} & \mathtt{b} \\ \mathtt{b} & \mathtt{a} \end{bmatrix} \cdot \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix} \leqq \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix}$$

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} \mathtt{a} & \mathtt{b} \\ \mathtt{b} & \mathtt{a} \end{bmatrix} \cdot \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix}$$

Vectors and matrices — operations

$$\left.\begin{aligned} 0 + \mathtt{a} \cdot s(q_0) + \mathtt{b} \cdot s(q_1) &\leqq s(q_0) \\ 1 + \mathtt{b} \cdot s(q_0) + \mathtt{a} \cdot s(q_1) &\leqq s(q_1) \end{aligned}\right\} \iff \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} \mathtt{a} & \mathtt{b} \\ \mathtt{b} & \mathtt{a} \end{bmatrix} \cdot \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix} \leqq \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix}$$

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} \mathtt{a} & \mathtt{b} \\ \mathtt{b} & \mathtt{a} \end{bmatrix} \cdot \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} \mathtt{a} \cdot s(q_0) + \mathtt{b} \cdot s(q_1) \\ \mathtt{b} \cdot s(q_0) + \mathtt{a} \cdot s(q_1) \end{bmatrix}$$

Vectors and matrices — operations

$$\left.\begin{array}{ll} 0 + \mathtt{a} \cdot s(q_0) + \mathtt{b} \cdot s(q_1) & \leqq s(q_0) \\ 1 + \mathtt{b} \cdot s(q_0) + \mathtt{a} \cdot s(q_1) & \leqq s(q_1) \end{array}\right\} \iff \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} \mathtt{a} & \mathtt{b} \\ \mathtt{b} & \mathtt{a} \end{bmatrix} \cdot \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix} \leqq \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix}$$

$$\begin{aligned} \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} \mathtt{a} & \mathtt{b} \\ \mathtt{b} & \mathtt{a} \end{bmatrix} \cdot \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix} &= \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} \mathtt{a} \cdot s(q_0) + \mathtt{b} \cdot s(q_1) \\ \mathtt{b} \cdot s(q_0) + \mathtt{a} \cdot s(q_1) \end{bmatrix} \\ &= \begin{bmatrix} 0 + \mathtt{a} \cdot s(q_0) + \mathtt{b} \cdot s(q_1) \\ 1 + \mathtt{b} \cdot s(q_0) + \mathtt{a} \cdot s(q_1) \end{bmatrix} \end{aligned}$$

Solutions to automata, via matrices

Lemma

Let $A = \langle Q, \rightarrow, I, F \rangle$ *be an automaton, and define*

$$M_A(q, q') = \sum_{q \xrightarrow{\mathtt{a}} q'} \mathtt{a} \qquad\qquad b_A(q) = [q \in F]$$

A Q*-vector* s *is a solution to* A *if and only if* $b_A + M_A \cdot s \leqq s$.

Solutions to automata, via matrices

Lemma

Let $A = \langle Q, \to, I, F \rangle$ be an automaton, and define

$$M_A(q, q') = \sum_{q \xrightarrow{\mathtt{a}} q'} \mathtt{a} \qquad\qquad b_A(q) = [q \in F]$$

A Q-vector s is a solution to A if and only if $b_A + M_A \cdot s \leqq s$.

Corollary

Let s be a Q-vector. The following are equivalent:

1. *s is the least solution to A*
2. *s is the least Q-vector such that $b_A + M_A \cdot s \leqq s$.*

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct the least Q-vector s such that $b + M \cdot s \leqq s$.

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct the least Q-vector s such that $b + M \cdot s \leqq s$.

Definition

Let S be a set, let b be an S-vector, and let $e \in \mathbb{E}$.

We write $b \fatsemi e$ for the S-vector given by $(b \fatsemi e)(s) = b(s) \cdot e$.

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Definition

Let S be a set, let b be an S-vector, and let $e \in \mathbb{E}$.

We write $b \fatsemi e$ for the S-vector given by $(b \fatsemi e)(s) = b(s) \cdot e$.

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof.

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof.

By induction on Q. In the base, where $Q = \emptyset$, the claim holds immediately.

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof.

For the inductive step, let $Q = Q' \cup \{p\}$, with $p \notin Q'$.

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof.

For the inductive step, let $Q = Q' \cup \{p\}$, with $p \notin Q'$.

Choose the Q'-matrix M' and Q'-vector b' by setting

$$M'(q, q') = M(q, q') + M(q, p) \cdot M(p, p)^* \cdot M(p, q')$$

$$b'(q) = b(q) + M(q, p) \cdot M(p, p)^* \cdot b(p)$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

By induction, we can compute a Q'-vector s', satisfying

$$b' + M' \cdot s' \leqq s' \qquad\qquad \forall t', e.\ b' \fatsemi e + M' \cdot t' \leqq t' \implies s' \fatsemi e \leqq t'$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \mathbin{;} e + M \cdot t \leqq t \implies s \mathbin{;} e \leqq t$$

Proof (cont'd).

Define the Q-vector s by

$$s(q) = \begin{cases} s'(q) & q \in Q' \\ M(p,p)^* \cdot \left(b(p) + \sum_{q' \in Q'} M(p,q') \cdot s'(q') \right) & q = p \end{cases}$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

$$(b + M \cdot s)(q) = b(q) + \sum_{q' \in Q} M(q, q') \cdot s(q')$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad \qquad \forall t, e.\ b \,⨾\, e + M \cdot t \leqq t \implies s \,⨾\, e \leqq t$$

Proof (cont'd).

$$(b + M \cdot s)(q) \equiv b(q) + M(q, p) \cdot s(p) + \sum_{q' \in Q'} M(q, q') \cdot s(q')$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \mathbin{;} e + M \cdot t \leqq t \implies s \mathbin{;} e \leqq t$$

Proof (cont'd).

$$(b + M \cdot s)(q) \equiv b(q) + M(q,p) \cdot M(p,p)^* \cdot \Big(b(p) + \sum_{q' \in Q'} M(p,q') \cdot s'(q')\Big) + \sum_{q' \in Q'} M(q,q') \cdot s(q') \tag{†}$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q \in Q'$, then we can derive:

$$\begin{aligned}(b + M \cdot s)(q) \equiv b(q) &+ M(q, p) \cdot M(p, p)^* \cdot b(p) \\ &+ M(q, p) \cdot M(p, p)^* \cdot \sum_{q' \in Q'} M(p, q') \cdot s'(q') \\ &+ \sum_{q' \in Q'} M(q, q') \cdot s'(q')\end{aligned}$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q \in Q'$, then we can derive:

$$\begin{aligned}(b + M \cdot s)(q) \equiv\ & b(q) + M(q,p) \cdot M(p,p)^* \cdot b(p) \\ & + \sum_{q' \in Q'} (M(q,q') + M(q,p) \cdot M(p,p)^* \cdot M(p,q')) \cdot s'(q')\end{aligned}$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q \in Q'$, then we can derive:

$$\begin{aligned}(b + M \cdot s)(q) &\equiv b(q) + M(q, p) \cdot M(p, p)^* \cdot b(p) \\ &\qquad + \sum_{q' \in Q'} (M(q, q') + M(q, p) \cdot M(p, p)^* \cdot M(p, q')) \cdot s'(q') \\ &\equiv b'(q) + \sum_{q' \in Q'} M'(q, q') \cdot s'(q')\end{aligned}$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q \in Q'$, then we can derive:

$$\begin{aligned}(b + M \cdot s)(q) &\equiv b(q) + M(q,p) \cdot M(p,p)^* \cdot b(p) \\ &\qquad + \sum_{q' \in Q'} (M(q,q') + M(q,p) \cdot M(p,p)^* \cdot M(p,q')) \cdot s'(q') \\ &\equiv b'(q) + \sum_{q' \in Q'} M'(q,q') \cdot s'(q') = (b' + M' \cdot s')(q)\end{aligned}$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q \in Q'$, then we can derive:

$$\begin{aligned}(b + M \cdot s)(q) &\equiv b(q) + M(q,p) \cdot M(p,p)^* \cdot b(p) \\ &\qquad + \sum_{q' \in Q'} (M(q,q') + M(q,p) \cdot M(p,p)^* \cdot M(p,q')) \cdot s'(q') \\ &\equiv b'(q) + \sum_{q' \in Q'} M'(q,q') \cdot s'(q') = (b' + M' \cdot s')(q) \leqq s'(q)\end{aligned}$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q \in Q'$, then we can derive:

$$\begin{aligned}(b + M \cdot s)(q) &\equiv b(q) + M(q,p) \cdot M(p,p)^* \cdot b(p) \\ &\qquad + \sum_{q' \in Q'} (M(q,q') + M(q,p) \cdot M(p,p)^* \cdot M(p,q')) \cdot s'(q') \\ &\equiv b'(q) + \sum_{q' \in Q'} M'(q,q') \cdot s'(q') = (b' + M' \cdot s')(q) \leqq s'(q) = s(q)\end{aligned}$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q = p$, then we can derive:

$$(b + M \cdot s)(p) \equiv b(p) + M(p,p) \cdot M(p,p)^* \cdot \Big(b(p) + \sum_{q' \in Q'} M(p,q') \cdot s'(q')\Big)$$
$$+ \sum_{q' \in Q'} M(p,q') \cdot s(q')$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \mathbin{;} e + M \cdot t \leqq t \implies s \mathbin{;} e \leqq t$$

Proof (cont'd).

If $q = p$, then we can derive:

$$(b + M \cdot s)(p) \equiv (1 + M(p,p) \cdot M(p,p)^*) \cdot \left(b(p) + \sum_{q' \in Q'} M(p,q') \cdot s'(q') \right)$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q = p$, then we can derive:

$$(b + M \cdot s)(p) \equiv M(p,p)^* \cdot \left(b(p) + \sum_{q' \in Q'} M(p,q') \cdot s'(q')\right)$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q = p$, then we can derive:

$$\begin{aligned}(b + M \cdot s)(p) &\equiv M(p,p)^* \cdot \Big(b(p) + \sum_{q' \in Q'} M(p,q') \cdot s'(q')\Big) \\ &= s(p)\end{aligned}$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

So, we know that $b + M \cdot s \leqq s$.

What about the second condition?

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

Let $e \in \mathbb{E}$, and suppose t is a Q-vector such that $b \fatsemi e + M \cdot t \leqq t$.

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

Let $e \in \mathbb{E}$, and suppose t is a Q-vector such that $b \fatsemi e + M \cdot t \leqq t$.

$$b(p) \cdot e + M(p,p) \cdot t(p) + \sum_{q' \in Q'} M(p,q') \cdot t(q')$$

$$\equiv b(p) \cdot e + \sum_{q' \in Q} M(p,q') \cdot s(q') \leqq t(p)$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

Let $e \in \mathbb{E}$, and suppose t is a Q-vector such that $b \fatsemi e + M \cdot t \leqq t$.

$$M(p,p)^* \cdot \Big(b(p) \cdot e + \sum_{q' \in Q'} M(p,q') \cdot t(q')\Big) \leqq t(p) \tag{§}$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

Let the Q'-vector t' be given by $t'(q) = t(q)$.

Claim: $b' \fatsemi e + M' \cdot t' \leqq t'$.

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \mathbin{;} e + M \cdot t \leqq t \implies s \mathbin{;} e \leqq t$$

Proof (cont'd).

If $q \in Q'$, we derive as follows:

$$(b' \mathbin{;} e + M' \cdot t')(q) = b'(q) \cdot e + \sum_{q' \in Q'} M'(q, q') \cdot t'(q')$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q \in Q'$, we derive as follows:

$$\begin{aligned}(b' \fatsemi e + M' \cdot t')(q) \equiv\ & b(q) \cdot e + M(q,p) \cdot M(p,p)^* \cdot b(p) \cdot e \\ & + \sum_{q' \in Q'} (M(q,q') + M(q,p) \cdot M(p,p)^* \cdot M(p,q')) \cdot t'(q')\end{aligned}$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q \in Q'$, we derive as follows:

$$(b' \fatsemi e + M' \cdot t')(q) \equiv b(q) \cdot e + M(q,p) \cdot M(p,p)^* \cdot \Big(b(p) \cdot e + \sum_{q' \in Q'} M(p,q') \cdot t(q') \Big) + \sum_{q' \in Q'} M(q,q') \cdot t(q')$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q \in Q'$, we derive as follows:

$$(b' \fatsemi e + M' \cdot t')(q) \leqq b(q) \cdot e + M(q, p) \cdot t(p) + \sum_{q' \in Q'} M(q, q') \cdot t(q')$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q \in Q'$, we derive as follows:

$$(b' \fatsemi e + M' \cdot t')(q) \leqq b(q) \cdot e + \sum_{q' \in Q} M(q, q') \cdot t(q')$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q \in Q'$, we derive as follows:

$$\begin{aligned}(b' \fatsemi e + M' \cdot t')(q) &\leqq b(q) \cdot e + \sum_{q' \in Q} M(q, q') \cdot t(q') \\ &\equiv (b \fatsemi e + M \cdot t)(q) \leqq t(q) = t'(q)\end{aligned}$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q \in Q'$, we derive as follows:

$$\begin{aligned}(b' \fatsemi e + M' \cdot t')(q) &\leqq b(q) \cdot e + \sum_{q' \in Q} M(q, q') \cdot t(q') \\ &\equiv (b \fatsemi e + M \cdot t)(q) \leqq t(q) = t'(q)\end{aligned}$$

Now $b' \fatsemi e + M' \cdot t' \leqq t$. By the induction hypothesis, $s' \fatsemi e \leqq t'$.

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \mathbin{;} e + M \cdot t \leqq t \implies s \mathbin{;} e \leqq t$$

Proof (cont'd).

If $q = p$, then we derive:

$$s(p) \cdot e \equiv M(p,p)^* \cdot \Big(b(p) + \sum_{q' \in Q'} M(p,q') \cdot s'(q') \Big) \cdot e$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \mathbin{;} e + M \cdot t \leqq t \implies s \mathbin{;} e \leqq t$$

Proof (cont'd).

If $q = p$, then we derive:

$$s(p) \cdot e \equiv M(p,p)^{*} \cdot \Big(b(p) \cdot e + \sum_{q' \in Q'} M(p, q') \cdot s'(q') \cdot e \Big)$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \mathbin{;} e + M \cdot t \leqq t \implies s \mathbin{;} e \leqq t$$

Proof (cont'd).

If $q = p$, then we derive:

$$s(p) \cdot e \leqq M(p,p)^* \cdot \left(b(p) \cdot e + \sum_{q' \in Q'} M(p,q') \cdot t'(q') \right)$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \mathbin{⨾} e + M \cdot t \leqq t \implies s \mathbin{⨾} e \leqq t$$

Proof (cont'd).

If $q = p$, then we derive:

$$\begin{aligned} s(p) \cdot e &\leqq M(p,p)^* \cdot \Big(b(p) \cdot e + \sum_{q' \in Q'} M(p,q') \cdot t'(q') \Big) \\ &\leqq t(p) \end{aligned}$$

Solutions to automata, via matrices

Theorem

Let Q be a finite set, with M a Q-matrix and b a Q-vector.

We can construct a Q-vector s such that both of the following hold:

$$b + M \cdot s \leqq s \qquad\qquad \forall t, e.\ b \fatsemi e + M \cdot t \leqq t \implies s \fatsemi e \leqq t$$

Proof (cont'd).

If $q = p$, then we derive:

$$\begin{aligned} s(p) \cdot e &\leqq M(p,p)^* \cdot \Big(b(p) \cdot e + \sum_{q' \in Q'} M(p,q') \cdot t'(q') \Big) \\ &\leqq t(p) \end{aligned}$$

Conclusion: $s \fatsemi e \leqq t$, as desired. □

The fruits of our labor

Given an automaton A with state q, we can compute e such that $L_A(q) = [\![e]\!]_{\mathbb{E}}$:

- Compute the matrix M_A and the vector b_A.
- Construct the least vector s such that $b_A + M_A \cdot s \leqq s$.
- This vector solves A; we can choose $e = s(q)$.

Some linear algebra

Given a Q-matrix M, we can compute for each Q-vector b a least Q-vector s such that $b + M \cdot s \leqq s$. This induces a map solve_M on Q-vectors.

Some linear algebra

Given a Q-matrix M, we can compute for each Q-vector b a least Q-vector s such that $b + M \cdot s \leqq s$. This induces a map solve_M on Q-vectors.

In fact, this map is *linear* in the sense that

$$\mathrm{solve}_M(b \fatsemi e) = \mathrm{solve}_M(b) \fatsemi e \qquad \mathrm{solve}_M(b_1 + b_2) = \mathrm{solve}_M(b_1) + \mathrm{solve}_M(b_2)$$

Some linear algebra

Given a Q-matrix M, we can compute for each Q-vector b a least Q-vector s such that $b + M \cdot s \leqq s$. This induces a map solve_M on Q-vectors.

In fact, this map is *linear* in the sense that

$$\mathrm{solve}_M(b \fatsemi e) = \mathrm{solve}_M(b) \fatsemi e \qquad \mathrm{solve}_M(b_1 + b_2) = \mathrm{solve}_M(b_1) + \mathrm{solve}_M(b_2)$$

Linear algebra tells us that solve_M is represented by a matrix!

Star of a matrix

Lemma

Let M be a Q-matrix. We can construct a matrix M^* such that the following hold:

(i) *if s and b are Q-vectors such that $b + M \cdot s \leqq s$, then $M^* \cdot b \leqq s$; and*

(ii) $\mathbf{1} + M \cdot M^* \equiv M^*$*, where* $\mathbf{1}$ *is the Q-matrix given by* $\mathbf{1}(q, q') = [q = q']$.

Proof sketch.

For $q \in Q$, let u_q be the Q-vector given by $u_q(q') = [q = q']$.

Star of a matrix

Lemma

Let M be a Q-matrix. We can construct a matrix M^* such that the following hold:

(i) *if s and b are Q-vectors such that $b + M \cdot s \leqq s$, then $M^* \cdot b \leqq s$; and*

(ii) $\mathbf{1} + M \cdot M^* \equiv M^*$, *where $\mathbf{1}$ is the Q-matrix given by $\mathbf{1}(q, q') = [q = q']$.*

Proof sketch.

For $q \in Q$, let u_q be the Q-vector given by $u_q(q') = [q = q']$.

Let s_q be the least Q-vector such that $u_q + M \cdot s_q \leqq s_q$.

Star of a matrix

Lemma

Let M be a Q-matrix. We can construct a matrix M^* such that the following hold:

(i) *if s and b are Q-vectors such that $b + M \cdot s \leqq s$, then $M^* \cdot b \leqq s$; and*

(ii) $\mathbf{1} + M \cdot M^* \equiv M^*$, *where $\mathbf{1}$ is the Q-matrix given by $\mathbf{1}(q, q') = [q = q']$.*

Proof sketch.

For $q \in Q$, let u_q be the Q-vector given by $u_q(q') = [q = q']$.

Let s_q be the least Q-vector such that $u_q + M \cdot s_q \leqq s_q$.

Choose $M^*(q, q') = s_{q'}(q)$. □

Star of a matrix

Lemma

Let M be a Q-matrix. We can construct a matrix M^* such that the following hold:

(i) *if s and b are Q-vectors such that $b + M \cdot s \leqq s$, then $M^* \cdot b \leqq s$; and*

(ii) *$\mathbf{1} + M \cdot M^* \equiv M^*$, where $\mathbf{1}$ is the Q-matrix given by $\mathbf{1}(q, q') = [q = q']$.*

Proof sketch.

For $q \in Q$, let u_q be the Q-vector given by $u_q(q') = [q = q']$.

Let s_q be the least Q-vector such that $u_q + M \cdot s_q \leqq s_q$.

Choose $M^*(q, q') = s_{q'}(q)$. □

Corollary

Let M, B and S be Q-matrices. If $B + M \cdot S \leqq S$, then $M^* \cdot B \leqq S$.

Dagger of a matrix

Lemma

Let M be a Q-matrix. We can construct a matrix $M^\dagger$ satisfying

$$1 + M^\dagger \cdot M = M^\dagger \qquad\qquad B + S \cdot M \leqq S \implies B \cdot M^\dagger \leqq S$$

Dagger of a matrix

Lemma

Let M be a Q-matrix. We can construct a matrix $M^\dagger$ satisfying

$$1 + M^\dagger \cdot M = M^\dagger \qquad\qquad B + S \cdot M \leqq S \implies B \cdot M^\dagger \leqq S$$

Corollary

Let M be a Q-matrix. Now $M^* = M^\dagger$.

Dagger of a matrix

Lemma

Let M be a Q-matrix. We can construct a matrix $M^\dagger$ satisfying

$$1 + M^\dagger \cdot M = M^\dagger \qquad\qquad B + S \cdot M \leqq S \implies B \cdot M^\dagger \leqq S$$

Corollary

Let M be a Q-matrix. Now $M^* = M^\dagger$.

Proof sketch.

Show that $1 + M \cdot M^\dagger \leqq M^\dagger$ and $1 + M^* \cdot M \leqq M^\dagger$. □

Dagger of a matrix

Lemma

Let M be a Q-matrix. We can construct a matrix $M^\dagger$ satisfying

$$1 + M^\dagger \cdot M = M^\dagger \qquad\qquad B + S \cdot M \leqq S \implies B \cdot M^\dagger \leqq S$$

Corollary

Let M be a Q-matrix. Now $M^* = M^\dagger$.

Proof sketch.

Show that $1 + M \cdot M^\dagger \leqq M^\dagger$ and $1 + M^* \cdot M \leqq M^\dagger$. □

The upshot: matrices of KA terms satisfy the laws of KA!

Next lecture

- Connect least solutions and (bi)simulations.

Next lecture

- Connect least solutions and (bi)simulations.
- The round-trip theorem.

Next lecture

- Connect least solutions and (bi)simulations.
- The round-trip theorem.
- The completeness theorem.