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.
Theorem (Kleene ’56)

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

We can construct $e \in E$ such that $[e]_E = L_A(q)$. 
Automata to expressions — ad hoc

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

From $q_1$ to $q_1$, passing through $q_1$ but not through $q_0$: $a^*$

From $q_0$ to $q_1$: $(a + b \cdot a^* \cdot b)^* \cdot b \cdot a^*$.
Automata to expressions — ad hoc

From $q_0$ to $q_0$, passing through $q_0$ and $q_1$: $(a + b \cdot a^* \cdot b)^*$
Automata to expressions — ad hoc

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

From $q_1$ to $q_1$, passing through $q_1$ but not through $q_0$: $a^*$
From $q_0$ to $q_0$, passing through $q_0$ and $q_1$: $(a + b \cdot a^* \cdot b)^*$

From $q_1$ to $q_1$, passing through $q_1$ but not through $q_0$: $a^*$

From $q_0$ to $q_1$: $(a + b \cdot a^* \cdot b)^* \cdot b \cdot a^*$. 
Suppose $J_0 E = L(q_0)$, and $J_1 E = L(q_1)$; then:
Automata to expressions — solving equations

Suppose $\llbracket e_0 \rrbracket_E = L(q_0)$, and $\llbracket e_1 \rrbracket_E = L(q_1)$; then:
Suppose $\llbracket e_0 \rrbracket_E = L(q_0)$, and $\llbracket e_1 \rrbracket_E = L(q_1)$; then:

\[
\begin{align*}
    a \cdot e_0 & \leq e_0 & b \cdot e_1 & \leq e_0 & a \cdot e_1 & \leq e_1 & b \cdot e_0 & \leq e_1 & 1 & \leq e_1
\end{align*}
\]
Suppose $[e_0]_E = L(q_0)$, and $[e_1]_E = L(q_1)$; then:

$$a \cdot e_0 + b \cdot e_1 \leq e_0$$

$$1 + a \cdot e_1 + b \cdot e_0 \leq e_1$$
Automata to expressions — solving equations

Recall the constraints we derived:

\[ a \cdot e_0 + b \cdot e_1 \leq e_0 \]  \hspace{1cm} (1)

\[ 1 + a \cdot e_1 + b \cdot e_0 \leq e_1 \]  \hspace{1cm} (2)
Automata to expressions — solving equations

Recall the constraints we derived:

\[ a \cdot e_0 + b \cdot e_1 \leq e_0 \]  \hspace{1cm} (1)

\[ (1 + b \cdot e_0) + a \cdot e_1 \leq e_1 \]  \hspace{1cm} (2)
Automata to expressions — solving equations

Recall the constraints we derived:

\[ a \cdot e_0 + b \cdot e_1 \leq e_0 \]  \hspace{1cm} (1)

\[ (1 + b \cdot e_0) + a \cdot e_1 \leq e_1 \]  \hspace{1cm} (2)

By the fixpoint axiom:

\[ a^* \cdot (1 + b \cdot e_0) \leq e_1 \]  \hspace{1cm} (3)
Automata to expressions — solving equations

Recall the constraints we derived:

\[ a \cdot e_0 + b \cdot e_1 \leq e_0 \]  \hspace{1cm} (1)

\[ (1 + b \cdot e_0) + a \cdot e_1 \leq e_1 \]  \hspace{1cm} (2)

By the fixpoint axiom:

\[ a^* \cdot (1 + b \cdot e_0) \leq e_1 \]  \hspace{1cm} (3)

Filling (3) into (1)

\[ a \cdot e_0 + b \cdot (a^* \cdot (1 + b \cdot e_0)) \leq e_0 \]  \hspace{1cm} (4)
Automata to expressions — solving equations

Recall the constraints we derived:

\[ a \cdot e_0 + b \cdot e_1 \leq e_0 \]  
(1)

\[ (1 + b \cdot e_0) + a \cdot e_1 \leq e_1 \]  
(2)

By the fixpoint axiom:

\[ a^* \cdot (1 + b \cdot e_0) \leq e_1 \]  
(3)

Filling (3) into (1)

\[ b \cdot a^* + (a + b \cdot a^* \cdot b) \cdot e_0 \leq e_0 \]  
(4)
Automata to expressions — solving equations

Recall the constraints we derived:

\[ a \cdot e_0 + b \cdot e_1 \leq e_0 \quad (1) \]

\[ (1 + b \cdot e_0) + a \cdot e_1 \leq e_1 \quad (2) \]

By the fixpoint axiom:

\[ a^* \cdot (1 + b \cdot e_0) \leq e_1 \quad (3) \]

Filling (3) into (1)

\[ b \cdot a^* + (a + b \cdot a^* \cdot b) \cdot e_0 \leq e_0 \quad (4) \]

Applying the fixpoint rule to (4):

\[ (a + b \cdot a^* \cdot b)^* \cdot b \cdot a^* \leq e_0 \]
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 $s : Q \rightarrow E$, such that for all $q \in Q$ it holds that

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

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

**Example:**

![Automaton Diagram]

$$0 + a \cdot s(q_0) + b \cdot s(q_1) \leq s(q_0)$$

$$1 + a \cdot s(q_1) + b \cdot s(q_0) \leq s(q_1)$$
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. $\leq$; i.e:

$$\forall \text{ solutions } s', q \in Q. \quad s(q) \leq s'(q)$$
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. $\leq$; i.e:

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

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 $\llbracket s(q) \rrbracket_{\mathbb{E}} = L(q)$ for all $q \in Q$. 
Vectors and matrices

Definition (Vectors and matrices)
Let $S$ be a set.

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

An *$S$-matrix (over $E$)* is a function $M : S \times S \to E$. 
Vectors and matrices — example

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

$$M_A(q, q') = \sum_{q \xrightarrow{a} q'} a$$
Vectors and matrices — example

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

\[
M_A(q, q') = \sum_{q \xrightarrow{a} q'} a
\]

Can write out matrices as tables, vectors as columns:

\[
M_A = \begin{pmatrix}
a & b \\
b & a
\end{pmatrix}
\]

\[
s = \begin{pmatrix}
e_0 \\
e_1
\end{pmatrix}
\]
Vectors and matrices — example

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

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

Can write out matrices as tables, vectors as columns:

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

\[
(s + t)(x) = s(x) + t(x) \quad \quad (M \cdot s)(x) = \sum_{y \in S} M(x, y) \cdot s(y)
\]

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 $s \leq t \iff s + t \equiv t$. 
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

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

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 $s \leq t \iff s + t \equiv t$. 
Vectors and matrices — operations

\[
\begin{align*}
0 + a \cdot s(q_0) + b \cdot s(q_1) & \leq s(q_0) \\
1 + b \cdot s(q_0) + a \cdot s(q_1) & \leq s(q_1)
\end{align*}
\] \iff
\[
\begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} a & b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix} \leq \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix}
\]
Vectors and matrices — operations

\[
\begin{align*}
0 + a \cdot s(q_0) + b \cdot s(q_1) & \leq s(q_0) \\
1 + b \cdot s(q_0) + a \cdot s(q_1) & \leq s(q_1)
\end{align*}
\]

\[
\begin{align*}
& \iff \\
& \left\{ \begin{array}{c}
0 + a \cdot s(q_0) + b \cdot s(q_1) \\
1 + b \cdot s(q_0) + a \cdot s(q_1)
\end{array} \right\} \iff \begin{bmatrix} 0 & 1 \\ a & b \end{bmatrix} \cdot \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix} \leq \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix}
\end{align*}
\]

\[
\begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} a & b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix}
\]
Vectors and matrices — operations

\[\begin{align*}
0 + a \cdot s(q_0) + b \cdot s(q_1) & \leq s(q_0) \\
1 + b \cdot s(q_0) + a \cdot s(q_1) & \leq s(q_1)
\end{align*}\]

\[\begin{align*}
\left\{ \begin{array}{c}
0 + a \cdot s(q_0) + b \cdot s(q_1) \\
1 + b \cdot s(q_0) + a \cdot s(q_1)
\end{array} \right\} & \iff
\begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} a & b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix} \leq \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix}
\end{align*}\]

\[\begin{align*}
\begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} a & b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} s(q_0) \\ s(q_1) \end{bmatrix} & = \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} a \cdot s(q_0) + b \cdot s(q_1) \\ b \cdot s(q_0) + a \cdot s(q_1) \end{bmatrix}
\end{align*}\]
Vectors and matrices — operations

\[
\begin{align*}
0 + a \cdot s(q_0) + b \cdot s(q_1) & \leq s(q_0) \\
1 + b \cdot s(q_0) + a \cdot s(q_1) & \leq s(q_1)
\end{align*}
\]
Solutions to automata, via matrices

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

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

$$b_A(q) = [q \in F]$$

A $Q$-vector $s$ is a solution to $A$ if and only if $b_A + M_A \cdot s \leq s$. 
Solutions to automata, via matrices

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

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

$$b_A(q) = [q \in F]$$

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

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 $b_A + M_A \cdot s \leq s$. 
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 $b + M \cdot s \leq s$. 

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 $b + M \cdot s \leq s$.

Definition

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

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

$$b + M \cdot s \leq s \quad \forall t, e. \ b \diamond e + M \cdot t \leq t \implies s \circ e \leq t$$

Definition
Let $S$ be a set, let $b$ be an $S$-vector, and let $e \in \mathbb{R}$.
We write $b \diamond e$ for the $S$-vector given by $(b \diamond e)(s) = b(s) \cdot e.$
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:

$$b + M \cdot s \leq s \forall t, e. \ b \circ e + M \cdot t \leq t \implies s \circ e \leq t$$

Proof.
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:

$$b + M \cdot s \leq s \quad \forall t, e. \quad b \circ e + M \cdot t \leq t \implies s \circ e \leq t$$

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:*

\[
\forall t, e. \quad b + M \cdot s \leq s, \quad e + M \cdot t \leq t \implies s \cdot e \leq t
\]

**Proof.**

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

$$b + M \cdot s \leq s \quad \forall t, e. \quad b \cdot e + M \cdot t \leq t \implies s \cdot e \leq t$$

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:

\[
\begin{align*}
  b + M \cdot s & \leq s & \forall t, e. \quad b \cdot e + M \cdot t & \leq t \implies s \cdot e \leq t \\
\end{align*}
\]

**Proof (cont’d).**

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

\[
\begin{align*}
  b' + M' \cdot s' & \leq s' & \forall t', e. \quad b' \cdot e + M' \cdot t' & \leq t' \implies s' \cdot e \leq t' \\
\end{align*}
\]
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:

$$b + M \cdot s \leq s \quad \forall t, \ e. \ b \circ e + M \cdot t \leq t \implies s \circ e \leq t$$

Proof (cont’d).

Define the $Q$-vector $s$ by

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

$$b + M \cdot s \leq s \quad \forall t, e. \quad b \circ e + M \cdot t \leq t \implies s \circ e \leq t$$

Proof (cont’d).

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

$$b + M \cdot s \leq s \quad \forall t, e \quad b \preceq e + M \cdot t \leq t \implies s \preceq e \leq t$$

Proof (cont’d).

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

$$b + M \cdot s \leq s \quad \forall t, e. \quad b \circ e + M \cdot t \leq t \implies s \circ e \leq t$$

Proof (cont’d).

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

$$+ \sum_{q' \in Q'} M(q, q') \cdot s(q') \quad (†)$$
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:

\[ b + M \cdot s \leq s \quad \forall t, \text{ e. } b \odot e + M \cdot t \leq t \implies s \odot e \leq t \]

Proof (cont’d).

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

\[
\begin{align*}
(b + M \cdot s)(q) & \equiv b(q) + M(q, p) \cdot M(p, p)^* \cdot b(p) \\
& \quad + M(q, p) \cdot M(p, p)^* \cdot \sum_{q' \in Q'} M(p, q') \cdot s'(q') \\
& \quad + \sum_{q' \in Q'} M(q, q') \cdot s'(q')
\end{align*}
\]
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:

\[ b + M \cdot s \leq s \quad \forall t, \quad e \vdash e + M \cdot t \leq t \implies s \vdash e \leq t \]

Proof (cont’d).
If $q \in Q'$, then we can derive:

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

$$b + M \cdot s \leq s \quad \forall t, e. b \circ e + M \cdot t \leq t \implies s \circ e \leq t$$

Proof (cont’d).
If $q \in Q'$, then we can derive:

$$(b + M \cdot s)(q) \equiv b(q) + M(q, p) \cdot M(p, p)^* \cdot b(p)$$

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

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

$$b + M \cdot s \leq s \quad \forall t, e. \ b \neq e + M \cdot t \leq t \implies s \neq e \leq t$$

Proof (cont’d).
If $q \in Q'$, then we can derive:

$$(b + M \cdot s)(q) \equiv b(q) + M(q, p) \cdot M(p, p)^* \cdot b(p)$$

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

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

\[
\forall t, e. \ b + M \cdot s \leq s \\
\Rightarrow \ b + e + M \cdot t \leq t \implies s \cdot e \leq t
\]

Proof (cont’d).
If \( q \in Q' \), then we can derive:

\[
(b + M \cdot s)(q) \equiv b(q) + M(q, p) \cdot M(p, p)^* \cdot b(p) \\
+ \sum_{q' \in Q'} (M(q, q') + M(q, p) \cdot M(p, p)^* \cdot M(p, q')) \cdot s'(q') \\
\equiv b'(q) + \sum_{q' \in Q'} M'(q, q') \cdot s'(q') = (b' + M' \cdot s')(q) \leq s'(q)
\]
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:

$$b + M \cdot s \leq s$$
$$\forall t, e. \ b \circ e + M \cdot t \leq t \implies s \circ e \leq t$$

Proof (cont’d).
If $q \in Q'$, then we can derive:

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

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

$$b + M \cdot s \leq s \quad \forall t, e. \quad b \circ e + M \cdot t \leq t \implies s \circ e \leq t$$

Proof (cont’d).

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

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

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

\[
b + M \cdot s \leq s \quad \forall t, e. \quad b \circ e + M \cdot t \leq t \implies s \circ e \leq t
\]

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:

$$b + M \cdot s \leq s \quad \forall t, \quad e \cdot b \leq e + M \cdot t \leq t \implies s \leq t$$

Proof (cont’d).
If $q = p$, then we can derive:

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

$$b + M \cdot s \leq s \quad \forall t, \text{ e. } b \circ e + M \cdot t \leq t \implies s \circ e \leq t$$

Proof (cont’d).
If $q = p$, then we can derive:

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

$$= s(p)$$
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:

$$b + M \cdot s \leq s \quad \forall t, e \quad b \preceq e + M \cdot t \leq t \implies s \preceq e \leq t$$

Proof (cont’d).
So, we know that $b + M \cdot s \leq s$.
What about the second condition?
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:

$$b + M \cdot s \leq s$$

for all $t, e$. $b \odot e + M \cdot t \leq t \implies s \odot e \leq t$

Proof (cont’d).

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

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:

$$b + M \cdot s \leq s \quad \forall t, e. \; b \cdot e + M \cdot t \leq t \implies s \cdot e \leq t$$

Proof (cont’d).
Let $e \in E$, and suppose $t$ is a $Q$-vector such that $b \cdot e + M \cdot t \leq t$.

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

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

\[ b + M \cdot s \leq s \quad \forall t, e. \quad b \cdot e + M \cdot t \leq t \implies s \cdot e \leq t \]

Proof (cont’d).

Let $e \in E$, and suppose $t$ is a $Q$-vector such that $b \cdot e + M \cdot t \leq t$.

\[
M(p, p)^* \cdot \left( b(p) \cdot e + \sum_{q' \in Q'} M(p, q') \cdot t(q') \right) \leq t(p) \tag{§}
\]
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:

\[
 b + M \cdot s \leq s \quad \forall t, e. \quad b + e + M \cdot t \leq t \implies s + e \leq t
\]

Proof (cont’d).
Let the \( Q' \)-vector \( t' \) be given by \( t'(q) = t(q) \).
Claim: \( b' + e + M' \cdot t' \leq t' \).
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:

$$b + M \cdot s \leq s \quad \forall t, \; e \cdot b + e + M \cdot t \leq t \implies s \cdot e \leq t$$

Proof (cont’d).
If $q \in Q'$, we derive as follows:

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

$$b + M \cdot s \leq s \quad \forall t, e. \quad b \circ e + M \cdot t \leq t \implies s \circ e \leq t$$

Proof (cont’d).
If $q \in Q'$, we derive as follows:

$$(b' \circ e + M' \cdot t')(q) \equiv b(q) \cdot e + M(q, p) \cdot M(p, p)^* \cdot b(p) \cdot e$$

$$+ \sum_{q' \in Q'} (M(q, q') + M(q, p) \cdot M(p, p)^* \cdot M(p, q')) \cdot t'(q')$$
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:

$$b + M \cdot s \leq s \quad \forall t, \ e. \ b \odot e + M \cdot t \leq t \implies s \odot e \leq t$$

**Proof (cont’d).**

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

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

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

$$b + M \cdot s \leq s$$
$$\forall t, e. \; b \circ e + M \cdot t \leq t \implies s \circ e \leq t$$

Proof (cont’d).

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

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

$$b + M \cdot s \leq s$$
$$\forall t, e. \ b \cdot e + M \cdot t \leq t \implies s \cdot e \leq t$$

Proof (cont’d).

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

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

$$b + M \cdot s \leq s$$  \hspace{1cm} \forall t, \; e. \; b \; \# \; e + M \cdot t \leq t \implies s \; \# \; e \leq t$$

Proof (cont’d).
If $q \in Q'$, we derive as follows:

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

$$\equiv (b \; \# \; e + M \cdot t)(q) \leq t(q) = t'(q)$$
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:

$$b + M \cdot s \leq s \quad \forall t, e. \ b \circ e + M \cdot t \leq t \implies s \circ e \leq t$$

Proof (cont’d).
If $q \in Q'$, we derive as follows:

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

$$\equiv (b \circ e + M \cdot t)(q) \leq t(q) = t'(q)$$

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

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:

\[ b + M \cdot s \leq s \quad \forall t, e. \quad b \cdot e + M \cdot t \leq t \implies s \cdot e \leq t \]

Proof (cont’d).
If $q = p$, then we derive:

\[ s(p) \cdot e \equiv M(p, p)^\ast \cdot \left( b(p) + \sum_{q' \in Q'} M(p, q') \cdot s'(q') \right) \cdot e \]
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:

$$b + M \cdot s \leq s \quad \forall t, \quad e \cdot b + M \cdot t \leq t \quad \Rightarrow \quad s \cdot e \leq t$$

Proof (cont’d).
If $q = p$, then we derive:

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

\[
\begin{align*}
    b + M \cdot s &\leq s \\
    \forall t, e. \quad b \otimes e + M \cdot t &\leq t \implies s \otimes e \leq t
\end{align*}
\]

Proof (cont’d).

If \( q = p \), then we derive:

\[
s(p) \cdot e \leq M(p, p)^* \cdot \left( b(p) \cdot e + \sum_{q' \in Q'} M(p, q') \cdot t'(q') \right)
\]
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:

\[ b + M \cdot s \leq s \quad \forall t, e. \quad b \circ e + M \cdot t \leq t \Rightarrow s \circ e \leq t \]

Proof (cont’d).

If $q = p$, then we derive:

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

\[ \leq t(p) \]
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:

$$b + M \cdot s \leq s \quad \forall t, \quad e. \quad b \circ e + M \cdot t \leq t \implies s \circ e \leq t$$

Proof (cont’d).
If $q = p$, then we derive:

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

$$\leq t(p)$$

Conclusion: $s \circ e \leq t$, as desired.
Given an automaton $A$ with state $q$, we can compute $e$ such that $L_A(q) = \begin{bmatrix} e \end{bmatrix}_E$:

- Compute the matrix $M_A$ and the vector $b_A$.
- Construct the least vector $s$ such that $b_A + M_A \cdot s \leq s$.
- 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 $b + M \cdot s \leq s$. This induces a map $\text{solve}_M$ on $Q$-vectors.
Given a $Q$-matrix $M$, we can compute for each $Q$-vector $b$ a least $Q$-vector $s$ such that $b + M \cdot s \leq s$. This induces a map $\text{solve}_M$ on $Q$-vectors.

In fact, this map is linear in the sense that

$$\text{solve}_M(b \circ e) = \text{solve}_M(b) \circ e \quad \text{solve}_M(b_1 + b_2) = \text{solve}_M(b_1) + \text{solve}_M(b_2)$$
Some linear algebra

Given a $Q$-matrix $M$, we can compute for each $Q$-vector $b$ a least $Q$-vector $s$ such that $b + M \cdot s \leq s$. This induces a map $\text{solve}_M$ on $Q$-vectors.

In fact, this map is linear in the sense that

$$\text{solve}_M(b \oplus e) = \text{solve}_M(b) \oplus e \quad \text{solve}_M(b_1 + b_2) = \text{solve}_M(b_1) + \text{solve}_M(b_2)$$

Linear algebra tells us that $\text{solve}_M$ is represented by 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 $b + M \cdot s \leq s$, then $M^* \cdot b \leq s$; and

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

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 $b + M \cdot s \leq s$, then $M^* \cdot b \leq s$; and

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

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 $u_q + M \cdot s_q \leq s_q$. 
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 $b + M \cdot s \leq s$, then $M^* \cdot b \leq s$; and

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

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 $u_q + M \cdot s_q \leq s_q$.

Choose $M^*(q, q') = s_{q'}(q)$.

\qed
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 $b + M \cdot s \leq s$, then $M^* \cdot b \leq s$; and
(ii) $1 + M \cdot M^* \equiv M^*$, where $1$ is the $Q$-matrix given by $1(q, q') = [q = q']$.

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 $u_q + M \cdot s_q \leq s_q$.
Choose $M^*(q, q') = s_{q'}(q)$.

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

Lemma

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

$$1 + M^\dagger \cdot M = M^\dagger \quad B + S \cdot M \leq S \implies B \cdot M^\dagger \leq S$$
Lemma

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

\[ 1 + M^\dagger \cdot M = M^\dagger \]

\[ B + S \cdot M \leq S \implies B \cdot M^\dagger \leq S \]

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
\[
1 + M^\dagger \cdot M = M^\dagger \quad \text{and} \quad B + S \cdot M \leq S \implies B \cdot M^\dagger \leq S
\]

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

Proof sketch.
Show that $1 + M \cdot M^\dagger \leq M^\dagger$ and $1 + M^* \cdot M \leq M^\dagger$. □
Lemma
Let $M$ be a $Q$-matrix. We can construct a matrix $M^\dagger$ satisfying

$$1 + M^\dagger \cdot M = M^\dagger \quad B + S \cdot M \leq S \implies B \cdot M^\dagger \leq S$$

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

Proof sketch.
Show that $1 + M \cdot M^\dagger \leq M^\dagger$ and $1 + M^* \cdot M \leq M^\dagger$.

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.