Kleene Algebra — Lecture 5

Tobias Kappé

ESSLLI 2023

1 Today's lecture

In the previous lecture, we talked about "solving" automata to obtain a rational expression for each state's language. We then built upon the machinery we used to construct solutions to develop a theory of matrices over rational expressions, and we found out that those matrices obey the same laws as the rational expressions they hold. In this final lecture, we will put all of this development to work, and ultimately resolve the question that was raised in the first lecture: *are two rational expressions with the same semantics, also equivalent by the laws of Kleene algebra?* The road towards this goal is built on three crucial insights.

- The first insight is to *exploit a bisimulation between states of an automaton to show that those states have equivalent solutions*; here, we use the solution technique based on matrices discussed in the last lecture.
- The second insight is that *converting an expression to an automaton and then back into an automaton is invariant w.r.t. provable equivalence.* This is called the "round-trip theorem", and we prove it using the first insight.
- The third insight is that the solutions to an automaton can be recovered from the solutions to its powerset automaton, and vice versa. As before, the proof of this property also relies on the first insight.

These three facts will ultimately be tied together to obtain completeness, by showing that expressions with the same language are converted to bisimilar deterministic automata, which must have equivalent solutions by the first point, and be provably equivalent to the original expressions by the second and third point — thus, by transitivity, the expressions are equivalent by the laws of KA.

2 Matrices and bisimulations

We can compute the star of a matrix over rational terms, and this operator behaves similarly to the star of a plain rational term. We are now going to use this operation to show that bisimilar states in automata yield provably equivalent expressions. In a way, this validates our work so far: if you have two *equivalent machines*, in that they can mimic one another in terms of behavior, then converting those machines back into programs gives you *equivalent expressions*.

To state the result, we need to first widen our view of matrices and matrix multiplication to include "rectangular" matrices, as follows.

Definition 5.1. Let S_1, S_2 and S_3 be sets. A *S_1-by-S_2 matrix* is a M function from $S_1 \times S_2$ to $\mathbb{E}$. If M is an S_1-by-S_2 matrix, and N is an S_2-by-S_3 matrix, then their multiplication is the S_1-by-S_3 matrix given by

$$(M \cdot N)(s_1, s_3) = \sum_{s_2 \in S_2} M(s_1, s_2) \cdot N(s_2, s_3)$$

Furthermore, if b is an S_2-vector, then $M \cdot b$ is the S_1-vector given by

$$(M \cdot b)(s_1) = \sum_{s_2 \in S_2} M(s_1, s_2) \cdot b(s_2)$$

Clearly, S-matrices and their operations on other S-matrices or S-vectors as used up to this point are a special case of the above. Specifically, what we have referred to as an S-matrix up to this point is an S-by-S matrix, and multiplication of S-matrices coincides with their multiplications as S-by-S-matrices. This broader view of matrices allows us to encode relations as well.

Definition 5.2. Let S_1 and S_2 be sets, and let $R \subseteq S_1 \times S_2$ be a relation between S_1 and S_2. We write M_R for the matrix given by $M_R(s_1, s_2) = [s_1 \; R \; s_2]$.

Also, recall that when $A = \langle Q, F, \delta \rangle$, we write M_A for the Q-matrix where

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

Given a S_1-by-S_2 matrix M, we will also write M^T for the *transpose* of M, which is the S_2-by-S_1 matrix given by $M^T(s_2, s_1) = M(s_1, s_2)$.

We can now state two useful properties of automata and relations as matrices. The first property is a relation between the acceptance vectors.

Lemma 5.3. *Let $A_i = \langle Q_i, \to_i, I_i, F_i \rangle$ be an automaton for $i \in \{0, 1\}$. Furthermore, let R be a simulation of A_0 by A_1. Then $M_R^T \cdot b_{A_0} \leqq b_{A_1}$.*

Proof. First, let's check our types. We know that M_R^T is a Q_1-by-Q_0 matrix, and b_{A_0} is a Q_0-vector; this makes $M_R \cdot b_{A_0}$ a Q_1-vector, just like b_{A_1}. To show that $M_R^T \cdot b_{A_0} \leqq b_{A_1}$, we need to show that for all $q_1 \in Q_1$, we have

$$\sum_{q_0 \in Q_0} M_R^T(q_1, q_0) \cdot b_{A_0}(q_0) = \sum_{q_0 \in Q_0} [q_0 \; R \; q_1] \cdot [q_0 \in F_0] \leqq [q_1 \in F_1]$$

We can show that this holds by arguing that for each $q_0 \in Q_0$, we have that $[q_0 \; R \; q_1] \cdot [q_0 \in F_0]$ is below $[q_1 \in F_1]$. There are two cases to distinguish. On the one hand, if $q_0 \not R \; q_1$ or $q_0 \notin F_0$, then $[q_0 \; R \; q_1] \cdot [q_0 \in F] \equiv 0$, and so the claim holds immediately. Otherwise, if $q_0 \; R \; q_1$ and $q_0 \in F_0$, then $q_1 \in F_1$, by virtue of R being a simulation. Hence $[q_1 \; R^c \; q_0] \cdot [q_0 \in F_0] \equiv 1 = [q_1 \in F_1]$. □

The second property relates the transition matrices, as follows.

Lemma 5.4. *Let $A_i = \langle Q_i, \to_i, I_i, F_i \rangle$ be an automaton for $i \in \{0, 1\}$. Furthermore, let R be a simulation of A_0 by A_1. Then $M_R^T \cdot M_{A_0} \leqq M_{A_1} \cdot M_R^T$.*

Proof. Let's get our types right first. Since R is a relation between Q_0 and Q_1, we know that M_R^T is a Q_1-by-Q_0 matrix. We also know that M_{A_0} is a Q_0-matrix, and M_{A_1} is a Q_1-matrix. This makes $M_R^T \cdot M_{A_0}$ a Q_1-by-Q_0 matrix, just like $M_{A_1} \cdot M_R^T$. So at least the comparison between them is sensible.

To prove our goal, we need to show that for $q_1 \in Q_1$ and $q_0 \in Q_0$, we have $(M_R^T \cdot M_{A_0})(q_1, q_0) \leqq (M_{A_1} \cdot M_R^T)(q_1, q_0)$, or, expanding out the definitions:

$$\sum_{q_0' \in Q_0} \Big([q_0' \; R \; q_1] \cdot \sum_{q_0' \xrightarrow{\mathtt{a}}_0 q_0} \mathtt{a} \Big) \leqq \sum_{q_1' \in Q_1} \Big(\Big(\sum_{q_1 \xrightarrow{\mathtt{a}}_1 q_1'} \mathtt{a} \Big) \cdot [q_1' \; R^c \; q_0] \Big)$$

Applying distributivity to both ends tells us the above is equivalent to

$$\sum_{q_0' \in Q_0} \sum_{q_0' \xrightarrow{\mathtt{a}}_0 q_0} [q_0' \; R \; q_1] \cdot \mathtt{a} \leqq \sum_{q_1' \in Q_1} \sum_{q_1 \xrightarrow{\mathtt{a}}_1 q_1'} \mathtt{a} \cdot [q_0 \; R \; q_1]$$

To show the above, it suffices to prove that every term in the sum on the left-hand side is below some term on the right-hand side, w.r.t. $\leqq$. To this end, let $q_0' \in Q_0$ and $\mathtt{a} \in \Sigma$ be such that $q_0' \xrightarrow{\mathtt{a}}_0 q_0$. If $q_0' \not R \; q_1$, then $[q_0 \; R \; q_1'] \cdot \mathtt{a} \equiv 0$, and so the claim holds immediately. Otherwise, if $q_0' \; R \; q_1$, then there exists a $q_1' \in Q_1$ such that $q_1 \xrightarrow{\mathtt{a}}_1 q_1'$ and $q_0 \; R \; q_1'$, since R is a simulation. We then find that $[q_0' \; R \; q_1] \cdot \mathtt{a} = 1 \cdot \mathtt{a} \equiv \mathtt{a} \cdot 1 = \mathtt{a} \cdot [q_0 \; R \; q_1']$. The latter is precisely a term on the right-hand side, and so the claim follows. □

As a matter of fact, we can leverage our newly derived facts about the star of a matrix to prove the last fact about transition- and bisimulation matrices.

Corollary 5.5. *Let $A_i = \langle Q_i, \to_i, I_i, F_i \rangle$ be an automaton for $i \in \{0, 1\}$, and let R be simulation of A_0 by A_1. Then $M_R^T \cdot M_{A_1}^* \leqq M_{A_0}^* \cdot M_R^T$.*

Proof sketch. By Lemma 5.4 and the fact that the laws of KA also apply to matrices. More precisely, it is analogous to the proof that if $e, f, g \in \mathbb{E}$ with $e \cdot f \leqq g \cdot e$, then $e \cdot f^* \leqq g^* \cdot e$, which is part of today's homework. □

These two facts now allow us to reach the desired conclusion, namely that expressions obtained for two bisimilar states are provably equivalent.

Theorem 5.6. *Let $A_i = \langle Q_i, \to_i, I_i, F_i \rangle$ be an automaton for $i \in \{0, 1\}$, and let R be a simulation of A_0 by A_1. If $q_0 \; R \; q_1$, and $e_0, e_1 \in \mathbb{E}$ are obtained from the automata-to-expressions procedure for q_0 and q_1, then $e_0 \leqq e_1$.*

Proof. From our automata-to-expressions procedure, we know that for both

$i \in \{0,1\}$ that $e_i = (M^*_{A_i} \cdot b_{A_i})(q_i)$. This then allows us to derive as follows:

$$\begin{aligned}
e_0 &= (M^*_{A_0} \cdot b_{A_0})(q_0) \\
&\equiv [q_0 \ R \ q_1] \cdot (M^*_{A_0} \cdot b_{A_0})(q_0) && \text{(since } q_0 \ R \ q_1\text{)} \\
&\leqq \sum_{q_0' \in Q_0} [q_0' \ R \ q_1] \cdot (M^*_{A_0} \cdot b_{A_0})(q_0') \\
&\leqq \sum_{q_0' \in Q_0} M_R^T(q_1, q_0') \cdot (M^*_{A_0} \cdot b_{A_0})(q_0') && \text{(def. } M_R^T\text{)} \\
&= (M_R^T \cdot M^*_{A_0} \cdot b_{A_0})(q_1) \\
&\leqq (M^*_{A_1} \cdot M_R^T \cdot b_{A_0})(q_1) && \text{(Corollary 5.5)} \\
&\leqq (M^*_{A_1} \cdot b_{A_1})(q_1) && \text{(Lemma 5.3)} \\
&= e_1 && \square
\end{aligned}$$

Theorem 5.7. *Let $A_i = \langle Q_i, \to_i, I_i, F_i \rangle$ be an automaton for $i \in \{0,1\}$, and let R be a bisimulation between A_0 by A_1. If $q_0 \ R \ q_1$, and $e_0, e_1 \in \mathbb{E}$ are obtained from the automata-to-expressions procedure for q_0 and q_1, then $e_0 \equiv e_1$.*

3 The round-trip theorem

We know how to obtain an automaton from an expression, and vice versa. This means that we can transform one expression into another (equivalent) expression, which raises the question: is "round-tripped" expression equivalent to the initial expression *by the laws of KA*, or is the equivalence lost in translation? More precisely: for each $e \in \mathbb{E}$, let's write $K(e)$ for the least solution to the *state* e in the Antimirov automaton for e; what we will show is that $e \equiv K(e)$.

The first step leverages the Fundamental Theorem to show that we can trivially obtain a solution to each Antimirov automaton, covering one direction.

Lemma 5.8. *Let $e \in \mathbb{E}$. Now $K(e) \leqq e$.*

Proof. Let $A_e = \langle \hat{\rho}(e), \to_{\mathbb{E}}, \{e\}, \mathbb{A} \cap \hat{\rho}(e) \rangle$ be the Antimirov automaton for e, and let s be the identity on $\hat{\rho}(e)$. Now s is a solution to A_e, i.e., for $e' \in \hat{\rho}(e)$:

$$[e' \in \mathbb{A}] + \sum_{e' \xrightarrow{\mathtt{a}}_{\mathbb{E}} e''} \mathtt{a} \cdot e'' \leqq e'$$

This follows immediately from the Fundamental Theorem. Because $K(e)$ is the *least* solution to $e \in \hat{\rho}(e)$ in A_e, it follows that $K(e) \leqq s(e) = e$. $\square$

For the other direction, we first consider another technical lemma, which shows that we can interrelate several round-tripped expressions easily.

Lemma 5.9. *The following hold for all $e, f, g \in \mathbb{E}$:*

$$K(e), K(f) \leqq K(e + f) \qquad K(e \cdot g + f \cdot g) \leqq K((e + f) \cdot g)$$

$$K(e \cdot (f \cdot g)) \leqq K((e \cdot f) \cdot g) \qquad K((1 + e \cdot e^*) \cdot f) \leqq K(e^* \cdot f)$$

$$K(1 \cdot e) \leqq K(e) \qquad K(e \cdot 1) \leqq K(e)$$

Proof. By Theorem 5.6, it suffices to demonstrate a simulation of the Antimirov automaton for the expression under K on the left by that on the right.

For each of the properties, we propose the necessary relation; showing that this yields a simulation that fits our needs is left as an exercise.

- For $K(e) \leqq K(e+f)$, take $R = \{\langle e, e+f\rangle\} \cup \{\langle e', e'\rangle : e' \in \rho(e)\}$. For $K(f) \leqq K(e+f)$, take the same R but relate f to $e+f$ instead.
- For $K(e \cdot g + f \cdot g) \leqq K((e+f) \cdot g)$, take the following relation:

$$\begin{aligned} R = &\{\langle e \cdot g + f \cdot g, (e+f) \cdot g\rangle\} \\ &\cup \{\langle e' \cdot g, e' \cdot g\rangle : e' \in \rho(e)\} \\ &\cup \{\langle f' \cdot g, f' \cdot g\rangle : e' \in \rho(f)\} \\ &\cup \{\langle g', g'\rangle : g' \in \rho(g)\} \end{aligned}$$

- For $K(e \cdot (f \cdot g)) \leqq K((e \cdot f) \cdot g)$, take the following relation:

$$\begin{aligned} R = &\{\langle e \cdot (f \cdot g), (e \cdot f) \cdot g\rangle\} \\ &\cup \{\langle e' \cdot (f \cdot g), (e' \cdot f) \cdot g\rangle : e' \in \rho(e)\} \\ &\cup \{\langle f' \cdot g, f' \cdot g\rangle : f' \in \rho(f)\} \\ &\cup \{\langle g', g'\rangle : g' \in \rho(g)\} \end{aligned}$$

- For $K((1 + e \cdot e^*) \cdot f) \leqq K(e^* \cdot f)$, take the following relation:

$$R = \{\langle (1 + e \cdot e^*) \cdot f, e^* \cdot f\rangle\} \cup \{\langle e' \cdot e^* \cdot f, e' \cdot e^* \cdot f\rangle : e' \in \rho(e)\}$$

- For $K(1 \cdot e) \leqq K(e)$, take $R = \{\langle 1 \cdot e, e\rangle\} \cup \{\langle e', e'\rangle : e' \in \rho(e)\}$.
- For $K(e \cdot 1) \leqq K(e)$, take $R = \{\langle e \cdot 1, e\rangle\} \cup \{\langle e' \cdot 1, e'\rangle : e' \in \rho(e)\}$. □

This lemma then allows us to show the other direction of the round-trip property we were looking for. Key to the proof here is that we first prove a slightly more general property, which makes the inductive argument possible.

Lemma 5.10. *Let $e \in \mathbb{E}$. Now $e \leqq K(e)$.*

Proof. We claim that, for all $f \in \mathbb{E}$, it holds that $e \cdot K(f) \leqq K(e \cdot f)$. To see this, we proceed by induction on e. In the base, there are three cases to consider.

- If $e = 0$, then the claim holds immediately.
- If $e = 1$, then we derive using Lemma 5.9 as follows:

$$e \cdot K(f) = 1 \cdot K(f) \equiv K(f) \leqq K(1 \cdot f) = K(e \cdot f)$$

- If $e = \mathtt{a}$ for some $\mathtt{a} \in \Sigma$, then note that $R = \{\langle f, 1 \cdot f\rangle\} \cup \{\langle f', f'\rangle : f' \in \rho(f)\}$ is a simulation of A_f by $A_{\mathtt{a} \cdot f}$. Thus, if s_f is the least solution to the former and $s_{\mathtt{a} \cdot f}$ is the least solution to the latter, then $s_f(f) \leqq s_{\mathtt{a} \cdot f}(1 \cdot f)$

by Theorem 5.6. We can then derive as follows:

$$\begin{aligned} e \cdot K(f) &= \mathtt{a} \cdot s_f(f) \\ &\leqq \mathtt{a} \cdot s_{\mathtt{a}\cdot f}(1 \cdot f) \\ &\leqq [\mathtt{a} \cdot f \in \mathbb{A}] + \sum_{\mathtt{a}\cdot f \xrightarrow{\mathtt{a}} f'} \mathtt{a} \cdot s_{\mathtt{a}\cdot f}(f') \\ &\leqq s_{\mathtt{a}\cdot f}(\mathtt{a} \cdot f) \\ &= K(e \cdot f) \end{aligned}$$

For the inductive step, there are again three cases to consider, based on the top-level compositional operator. For each case, our induction hypothesis is that the claim holds for each of the direct subexpressions.

- If $e = e_0 + e_1$, then derive

$$\begin{aligned} e \cdot K(f) &= (e_0 + e_1) \cdot K(f) \\ &\equiv e_0 \cdot K(f) + e_1 \cdot K(f) \\ &\leqq K(e_0 \cdot f) + K(e_1 \cdot f) && \text{(IH)} \\ &\leqq K(e_0 \cdot f + e_1 \cdot f) && \text{(Lemma 5.9)} \\ &\leqq K((e_0 + e_1) \cdot f) && \text{(Lemma 5.9)} \\ &= K(e \cdot f) \end{aligned}$$

- If $e = e_0 \cdot e_1$, then derive

$$\begin{aligned} e \cdot K(f) &= (e_0 \cdot e_1) \cdot K(f) \\ &\equiv e_0 \cdot (e_1 \cdot K(f)) \\ &\leqq e_0 \cdot K(e_1 \cdot f) && \text{(IH)} \\ &\leqq K(e_0 \cdot (e_1 \cdot f)) && \text{(IH)} \\ &\leqq K((e_0 \cdot e_1) \cdot f) && \text{(Lemma 5.9)} \\ &= K(e \cdot f) \end{aligned}$$

- If $e = e_0^*$, then we derive as follows:

$$\begin{aligned} K(f) + e_0 \cdot K(e \cdot f) &\leqq K(f) + K((e_0 \cdot e) \cdot f) && \text{(IH)} \\ &\leqq K(f) + K(e_0 \cdot (e \cdot f)) && \text{(Lemma 5.9)} \\ &\leqq K(f + (e_0 \cdot e) \cdot f) && \text{(Lemma 5.9)} \\ &\leqq K((1 + e_0 \cdot e) \cdot f) && \text{(Lemma 5.9)} \\ &\leqq K(e \cdot f) && \text{(Lemma 5.9)} \end{aligned}$$

  It then follows that $e \cdot K(f) = e_0^* \cdot K(f) \leqq K(e \cdot f)$.

To reach the claim, we note that $1 \leqq K(1)$ since $1 \in \mathbb{A}$; thus, by Lemma 5.9,

$$e \equiv e \cdot 1 \leqq e \cdot K(1) \leqq K(e \cdot 1) \equiv K(e) \qquad \square$$

These two lemmas together now imply the property we were looking for.

Theorem 5.11 (Round-trip)**.** *Let $e \in \mathbb{E}$. Now $e \equiv K(e)$.*

4 Solutions to powerset automata

We now arrive at the final bit of insight that we need to establish completeness. Here, the idea is that since the powerset construction preserves the language of an automaton, the solutions should also be interrelated. This is indeed the case, in a strong sense: the least solution to a compound state in the powerset automaton is obtained by summing together the solutions to its components in in the original automaton. More formally, we can show the following.

Lemma 5.12. *Let $A = \langle Q, \to, I, F\rangle$ be an automaton and let $A' = \langle 2^Q, \to'$ $, \{I\}, F'\rangle$ be its powerset automaton. Furthermore, let s and s' be the least solutions to A and A' respectively. For $S \subseteq Q$ we have that $s'(S) \equiv \sum_{q\in S} s(q)$.*

Proof. Let $t' : 2^Q \to \mathbb{E}$ be given by $t(S) = \sum_{q\in S} s(q)$. We claim that t' is a solution to A'. To this end, we need to argue the following:

1. if $S \in F'$ then $1 \leqq t'(S)$; and
2. if $S \xrightarrow{\mathtt{a}}{}' S'$, then $\mathtt{a} \cdot t'(S') \leqq t'(S)$.

For the first property, note that if $S \in F'$ then there exists a $q \in S$ such that $q \in F$, by construction of F'. It then follows that $1 \leqq s(q) \leqq t'(S)$.

For the second property, we can expand the definition of t' to find that it suffices to show that if $q' \in S'$, then $\mathtt{a}\cdot s(q') \leqq s(q)$ for some $q \in S$. By definition of the powerset construction, we have that $S' = \{q' : \exists q \in S.\ q \xrightarrow{\mathtt{a}} q'\}$; thus, if $q' \in S'$ then we can choose $q \in S$ such that $q \xrightarrow{\mathtt{a}} q'$, and $q \xrightarrow{\mathtt{a}} q'$; since s is a solution to A, the latter implies that $\mathtt{a} \cdot s(q') \leqq s(q)$.

Now, since t' is a solution to A' and s' is the least solution to A', we have that $s'(S) \leqq t'(S)$ for all $S \subseteq Q$, or in other words that $s'(S) \leqq \sum_{q\in S} s(q)$ for all $S \subseteq Q$. This establishes one half of our claim.

For the other half, first note that if $R = \{\langle q, S\rangle : q \in S \subseteq Q\}$, then R is a simulation of A by A' — after all, if $q \in F$ and $q\ R\ S$ then $S \in F'$ by construction, and if $q \xrightarrow{\mathtt{a}} q'$ and $q\ R\ S$, then choose $S' = \{q' \in Q : q \xrightarrow{\mathtt{a}} q'\}$ to find that $S \xrightarrow{\mathtt{a}} S'$ and $q' \in S'$. By Theorem 5.6 it follows that if $q \in S \subseteq Q$, then $s(q) \leqq s'(S)$. This implies that if $S \subseteq Q$, then $\sum_{q\in S} s(q) \leqq s'(S)$. □

5 Completeness

Finally, we have every ingredient in place to reap the fruit of our labors.

Theorem 5.13 (Completeness)**.** *Let $e, f \in \mathbb{E}$. If $[\![e]\!]_{\mathbb{E}} = [\![f]\!]_{\mathbb{E}}$, then $e \equiv f$.*

Proof. Because $[\![e]\!]_{\mathbb{E}} = [\![f]\!]_{\mathbb{E}}$, we know that $L_{A_e}(e) = L_{A_f}(f)$, and therefore $L_{A'_e}(\{e\}) = L_{A'_f}(\{f\})$. Since A'_e and A'_f are deterministic, there exists a bisimulation that relates their initial states. Now, let s'_e and s'_f be the least solutions to A'_e and A'_f respectively. By Theorem 5.7, we then have that $s'_e(\{e\}) \equiv s'_f(\{f\})$. Next, let s_e and s_f be the least solutions to A_e and A_f respectively. By Lemma 5.12, we have that $s_e(e) \equiv s'_e(\{e\})$ and $s_f(f) \equiv s'_f(\{f\})$, and thus by transitivity that $K(e) = s_e(e) \equiv s_f(f) = K(f)$. By Theorem 5.11, we have that $e \equiv K(e)$ and $f \equiv K(f)$, and hence that $e \equiv f$. □

Some remarks are in order. First, note that the theorem we have is strictly about *equations*. There is a more general claim you can make, and we have seen it pop up in some form a number of times: the *Horn equation*, of the form

$$e_0 \equiv f_0 \wedge \cdots \wedge e_{n-1} \equiv f_{n-1} \implies e \equiv f$$

There are several of these that hold in Kleene Algebra, such as $e \cdot f \leqq g \cdot e \implies e \cdot f^* \leqq g^* \cdot e$. However, Theorem 5.13 does *not* guarantee that they are all provable. The study of *Kleene Algebra with Hypotheses* is dedicated to finding out which kinds of premises can be used to recover a completeness result.

Second, the pattern of the proof in Theorem 5.13 is actually quite common in the realm of completeness results: given that the semantics of two expressions are equivalent, first show that you can convert them into some kind of equivalent "normal form" — in this case, $K(e)$ and $K(f)$ — and then argue that the semantic equivalence of terms in normal form implies that they are provably equivalent. We see a similar pattern in, for example, the completeness proof of Boolean Algebra, or several similar results within Process Algebra.

Lastly, note that the completeness result, when composed with decidability of language equivalence, gives us a new decidability result, namely that given $e, f \in \mathbb{E}$, it is decidable whether $e \equiv f$: simply decide whether $[\![e]\!]_{\mathbb{E}} = [\![f]\!]_{\mathbb{E}}$. In effect, this gives us a road towards *proof mechanization*: if you want to prove that $e \equiv f$, you do not need to finagle with axioms, but can instead ask an algorithm to figure it out for you. This is particularly useful when you are working through a larger proof about your program, and want to verify whether a certain equivalence holds in general. Proof assistants such as Coq can be scripted to try and automatically prove statements of Kleene Algebra.

6 Homework

1. Let $e, f, g \in \mathbb{E}$ be such that $e \cdot f \leqq g \cdot e$. Show that $e \cdot f^* \leqq g^* \cdot e$.
2. Show that each of the relations proposed in Lemma 5.9 is a simulation.
3. Let R and S be relations. Show that $M_{R \circ S} \equiv M_R \cdot M_S$.
4. Let R be a relation. Show that $M_{R^*} \equiv M_R^*$.

   Hint: show that $M_R^* \leqq M_{R^*}$ and $M_{R^*} \leqq M_R^*$. For both inclusions, you need to use facts about the star of a matrix, but the implication is only necessary for one of them.

7 Bibliographical notes

The proof that solutions to automata are invariant w.r.t. bisimilarity is adapted from Jacobs's account [Jac06], who credits the idea to Kozen [Koz01]. A version of the round trip theorem can be found in both papers.

There are a number of completeness results for laws about programs, including those by Salomaa [Sal66], Conway [Con71], Krob [Kro90], Boffa [Bof90], and Kozen [Koz94]. The result discussed in this lecture was first shown by Kozen [Koz94], but his tactic was rather different. The presentation we used is adapted from Jacobs [Jac06], who credits the proofs to Kozen [Koz01]. Palka showed that the finite model property can also be recovered [Pal05].

References

[Bof90] Maurice Boffa. Une remarque sur les systèmes complets d'identités rationnelles. *ITA*, 24:419–428, 1990.

[Con71] John Horton Conway. *Regular Algebra and Finite Machines*. Chapman and Hall, Ltd., London, 1971.

[Jac06] Bart Jacobs. A bialgebraic review of deterministic automata, regular expressions and languages. In *Algebra, Meaning, and Computation, Essays Dedicated to Joseph A. Goguen on the Occasion of His 65th Birthday*, pages 375–404, 2006. doi:10.1007/11780274_20.

[Koz94] Dexter Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Inf. Comput.*, 110(2):366–390, 1994. doi:10.1006/inco.1994.1037.

[Koz01] Dexter Kozen. Myhill-Nerode relations on automatic systems and the completeness of Kleene algebra. In *STACS*, pages 27–38, 2001. doi:10.1007/3-540-44693-1_3.

[Kro90] Daniel Krob. A complete system of b-rational identities. In *ICALP*, pages 60–73, 1990. doi:10.1007/BFb0032022.

[Pal05] Ewa Palka. On finite model property of the equational theory of Kleene algebras. *Fundam. Informaticae*, 68(3):221–230, 2005. URL: http://content.iospress.com/articles/fundamenta-informaticae/fi68-3-02.

[Sal66] Arto Salomaa. Two complete axiom systems for the algebra of regular events. *J. ACM*, 13(1):158–169, 1966. doi:10.1145/321312.321326.