Discrete Mathematics

Supervision 9

Marcelo Fiore   Ohad Kammar   Dima Szamozvancev

14. On inductive definitions

1. Let L be the subset of $\{a, b\}^*$ inductively defined by the axiom $\dfrac{}{\varepsilon}$ and rule $\dfrac{u}{aub}$ for $u \in \{a, b\}^*$.

   a) Use *rule induction* to prove that every string in L is of the form $a^n b^n$ for some $n \in \mathbb{N}$.

   b) Use *mathematical induction* to prove that for all $n \in \mathbb{N}$, $a^n b^n \in L$.

   c) Conclude that $L = \{a^n b^n \mid n \in \mathbb{N}\}$.

   d) Suppose we add the string a to L to get $L' = L \cup \{a\}$. Is L' closed under the axiom and rule? If not, characterise the strings that would be in the smallest set containing L' that is closed under the axiom and rule.

2. Suppose $R\colon X \nrightarrow X$ is a binary relation on a set X. Let $R^\dagger : X \nrightarrow X$ be inductively defined by the following axioms and rules:

$$\frac{}{(x,x) \in R^\dagger}\ (x \in X) \qquad\qquad \frac{(x,y) \in R^\dagger}{(x,z) \in R^\dagger}\ (x \in X \text{ and } y\,R\,z)$$

   a) Show that $R^\dagger$ is reflexive and that $R \subseteq R^\dagger$.

   b) Use rule induction to show that $R^\dagger$ is a subset of

$$S \triangleq \left\{ (y,z) \in X \times X \;\middle|\; \forall x \in X.\, (x,y) \in R^\dagger \implies (x,z) \in R^\dagger \right\}$$

   Deduce that $R^\dagger$ is transitive.

   c) Suppose that $T : X \nrightarrow X$ is a reflexive and transitive binary relation and that $R \subseteq T$. Use rule induction to show that $R^\dagger \subseteq T$.

   d) Deduce from above that $R^\dagger$ is equal to R^*, the reflexive-transitive closure of R.

3. Let L be a subset of $\{a, b\}^*$ inductively defined by the axiom and rules (for $u \in \{a, b\}^*$):

$$\frac{}{ab} \qquad\qquad \frac{au}{au^2} \qquad\qquad \frac{ab^3u}{au}$$

   a) Is ab^5 in L? Give a derivation, or show that there isn't one.

   b) Use rule induction to show that every $u \in L$ is of the form ab^n with $n = 2^k - 3m \geq 0$ for some $k, m \in \mathbb{N}$.

   c) Is ab^3 in L? Give a derivation, or show that there isn't one.

   d) Find an explicit characterisation of the elements of the language as a set comprehension, and prove (along the lines of §14.1) that it coincides with the inductively defined set L.

15. On regular expressions

1. Find regular expressions over $\{0, 1\}$ that determine the following languages:

   a) $\{ u \mid u$ contains an even number of 1's $\}$

   b) $\{ u \mid u$ contains an odd number of 0's $\}$

2. Show that $b^*a(b^*a)^*$ and $(a|b)^*a$ are equivalent regular expressions, that is, a string matches one iff it matches the other. Your reasoning should be rigorous but can be informal.

3. Extend the concrete syntax, abstract syntax, parsing relation of regular expressions, and the matching relation between strings and regular expressions with the following constructs:

   a) $r?$: matches the regex r zero or one times. For example, $ab?c$ is matched by ac and abc, but not $abbc$.

   b) r^+: matches the regex r one or more times. For example, ab^+c is matched by abc and $abbbbc$, but not ac.

   Show that $(r^+)?$ is equivalent to r^*. Is that the case for $(r?)^+$ as well?

16. On finite automata

1. For each of the two languages mentioned in §15.1 (string containing an even number of 1's or an odd number of 0's), find a DFA that accepts exactly that set of strings.

2. Given an NFA$^\varepsilon$ $M = (Q, \Sigma, \Delta, s, F, T)$, we write $q \overset{u}{\Rightarrow} q'$ to mean that there is a path in M from state q to state q' whose non-ε labels form the string $u \in \Sigma^*$. Show that $L = \left\{ (q, u, q') \,\middle|\, q \overset{u}{\Rightarrow} q' \right\}$ is equal to the subset of $Q \times \Sigma^* \times Q$ inductively defined by the axioms and rules:

$$\frac{}{(q, \varepsilon, q)} \qquad \frac{(q, u, q')}{(q, u, q'')} \text{ if } q' \xrightarrow{\varepsilon} q'' \text{ in } M \qquad \frac{(q, u, q')}{(q, ua, q'')} \text{ if } q' \xrightarrow{a} q'' \text{ in } M$$

   Hint: recall the method from §14.1. for showing that a language defined via set comprehension is equal to an inductively defined set: first show that L is closed under the rules and axioms, then show that every string in L has a derivation.

3. The example of the subset construction given on Slide 58 constructs a DFA with eight states whose language of accepted strings happens to be $L(a^*b^*)$. Give an "optimised" DFA with the same language of accepted strings, but fewer states. Give an NFA with even fewer states that does the same job.

Discrete Mathematics

Supervision 10

Marcelo Fiore Ohad Kammar Dima Szamozvancev

17. On regular languages

1. Why can't the automaton $Star(M)$ used in step (iv) of the proof of part (a) of Kleene's Theorem be constructed by simply taking M, making its start state the only accepting state and adding new ε-transitions back from each old accepting state to its start state?

2. Construct an NFA$^{\varepsilon}$ M satisfying $L(M) = L((\epsilon|b)^* aab^*)$ using Kleene's construction.

3. Show that any finite set of strings is a regular language.

4. Use the construction given in the proof of part (b) of Kleene's Theorem to find a regular expression for the DFA M whose state set is $\{0,1,2\}$, whose start state is 0, whose only accepting state is 2, whose alphabet of input symbols is $\{a,b\}$, and whose next-state function is given by the following table.

δ	a	b
0	1	2
1	2	1
2	2	1

5. If $M = (Q, \Sigma, \Delta, s, F)$ is an NFA, let $Not(M)$ be the NFA $(Q, \Sigma, \Delta, s, Q \setminus F)$ obtained from M by interchanging the role of accepting and nonaccepting states. Give an example of an alphabet Σ and an NFA M with set of input symbols Σ such that $\{u \in \Sigma^* \mid u \notin L(M)\}$ is *not* the same as $L(Not(M))$.

6. Let $r = (a|b)^* ab(a|b)^*$. Find a regular expression that is equivalent to the complement for r over the alphabet $\{a,b\}$ with the property $L(\sim r) = \{u \in \{a,b\}^* \mid u \notin L(r)\}$.

7. Given DFAs $M_i = (Q_i, \Sigma, \delta_i, s_i, F_i)$ for $i = 1, 2$, let $And(M_1, M_2)$ be the DFA

$$(Q_1 \times Q_2, \Sigma, \delta, (s_1, s_2), F_1 \times F_2)$$

where $\delta : (Q_1 \times Q_2) \times \Sigma \to (Q_1 \times Q_2)$ is given by

$$\delta((q_1, q_2), a) = (\delta_1(q_1, a), \delta_2(q_2, a))$$

for all $q_1 \in Q_1, q_2 \in Q_2$ and $a \in \Sigma$. Show that $L(And(M_1, M_2)) = L(M_1) \cap L(M_2)$.

18. On the Pumping Lemma

1. Briefly summarise the proof of the Pumping Lemma in your own words.

2. Consider the language $L \triangleq \{c^m a^n b^n \mid m \geq 1 \wedge n \geq 0\} \cup \{a^m b^n \mid m, n \geq 0\}$. The notes show that L has the pumping lemma property. Show that there is no DFA M which accepts L.

   Hint: argue by contradiction. If there were such an M, consider the DFA M' with the same states as M, with alphabet of input symbols just consisting of a and b, with transitions all those of M which are labelled by a or b, with start state $\delta_M(s_M, c)$ where s_M is the start state of M, and with the same accepting states as M. Show that the language accepted by M' has to be $\{ a^n b^n \mid n \geq 0 \}$ and deduce that no such M can exist.