CSE 531
Automata, Computability, Complexity

Minimizing Finite Automata

Paul Beame 6 October 1999

Given a DFA $M = (Q, \Sigma, \delta, s, F)$ such that $A = L(M)$ how do we find a DFA M' of minimal size such that $A = L(M')$? We know that such a DFA has precisely one state for each equivalence class of $\equiv_A$ and that each equivalence class of $\equiv_A$ is a union of equivalence classes of $\equiv_M$. All that we would need to do is to figure out how to group the states of M so that their corresponding equivalence classes lie in a single equivalence class of $\equiv_A$. In order to do this, rather than starting with individual states and clumping them together we will instead begin by grouping states together and separate them only when necessary. When we have finished we will have produced the minimal DFA for A.

Definition 0.1: For each $i \geq 0$, define an equivalence relation $\equiv_i$ on the set of *states* Q of M by $p \equiv_i q$ if and only if for all strings $z \in \Sigma^*$ with $|z| \leq i$, $\delta^*(p, z) \in F \Leftrightarrow \delta^*(q, z) \in F$.

Now lets get some intuition for this definition.

Lemma 1: Let $p, q \in Q$ and suppose that every state of M is reachable from the start state s. Then $p \equiv_i q$ for all $i \geq 0$ if and only if the equivalence classes of $\equiv_M$ corresponding to p and q lie in the same equivalence class of $\equiv_A$.

Proof Suppose that $p \equiv_i q$ for all values of $i \geq 0$. Then for all $z \in \Sigma^*$, if $\delta^*(s, x) = p$ and $\delta^*(s, y) = q$ then $xz \in A \Leftrightarrow yz \in A$. Therefore any two strings that reach p and q are in the same equivalence class of $\equiv_A$.

Suppose that $p \not\equiv_i q$ for some i. Then there is some z with $|z| \leq i$ such only one of $\delta^*(p, z)$, $\delta^*(q, z)$ is in F. Since p and q are both reachable from s, there are strings x and y with $\delta^*(s, x) = p$ and $\delta^*(s, y) = q$. Therefore only one of $\delta^*(s, xz), \delta^*(yz)$ is in F and so only one of xz, yz is in A. This means that the classes of $\equiv_M$ corresponding to p and q are not in the same equivalence class of $\equiv_A$. $\square$

That's all very well but how can we figure out when states are equivalent to each other under $\equiv_i$?

Observe first that we can figure out the equivalence classes of $\equiv_0$ quite easily since in this case $z = \varepsilon$ and its two equivalence classes are therefore F and $Q \setminus F$.

Also, given $\equiv_i$ it is fairly easy to figure out $\equiv_{i+1}$: First of all, equivalent states under $\equiv_{i+1}$ must be equivalent under $\equiv_i$ since they must agree for all strings z of length up to i. To also make sure that they agree for all strings z' up to $i+1$, we just check that after reading the first character of z' we arrive at states that are equivalent for all strings of length up to i. More precisely, $p \equiv_{i+1} q$ if and only if $p \equiv_i q$ and for all $a \in \Sigma$, $\delta(p,a) \equiv_i \delta(q,a)$.

Now suppose at any point that we find that $\equiv_{j+1}$ is the same as $\equiv_j$, i.e. we haven't split any classes of $\equiv_j$ based on the outgoing arcs. Then running through the definitions we see that $\equiv_{j+2}$ will also be the same and in fact $\equiv_i$ for all $i \geq j$ will be the same. (This is called a *fixed point*.) Also observe that because $p \equiv_j q$ implies that $p \equiv_{j-1} q$ etc., $p \equiv_j q \Leftrightarrow p \equiv_i q$ for all $i \geq 0$.

Therefore, to figure out the minimal DFA for A we begin with $\equiv_0$ and repeatedly create $\equiv_{i+1}$ from $\equiv_i$ up until it reaches a fixed point $\equiv_j$. To obtain the minimal DFA for A we collapse all states in each equivalence class of $\equiv_j$ into a single state. By construction none of the arcs will have labels that conflict with each other. (That is, for all $a \in \Sigma$, all arcs out of any collapsed state will lead to the same collapsed state.)

How many steps does this take? Well, each time $\equiv_{i+1}$ is different from $\equiv_i$ there is a least one more equivalence class. Since the number of equivalence classes is never more than $|Q|$, a fixed point is reached after at most $|Q| - 1$ steps.