CS 381	**Introduction to Theory of Computing**	Handout
Summer 2000	By Kevin Hamlen	June 3, 2000

Standard Format for a Constructive Proof that a Language is Regular

Many problems you will see in this course have the following form:

> *Assume A is regular. Define A' to be... (some definition in terms of A). Prove that A' is regular.*

One traditional way to solve this kind of problem is to infer that since A is regular, there exists a DFA, M, that accepts it; then use this DFA to construct an NFA (with or without ϵ-transitions), N, that accepts A'; then prove that N does indeed accept A'. Such a proof almost always has a very standard format. If you don't adhere to that format, it is very easy to get both the proof and the construction wrong. The following document explains the steps that one must usually go through in order to solve problems like the one above.

Constructing the NFA

The construction of your NFA should consist of formal definitions of Q_N, Δ_N, S_N, and F_N. Don't forget that S_N is a *set* of states from Q_N, not just a single state. These definitions will be based on DFA M. Some things to remember about M include:

1. A DFA has exactly one start state, not a set of start states.
2. A DFA may have many final states.
3. A DFA always has a transition for every possible symbol from every possible state.
4. You cannot impose any ordering on the states of Q_M. DFA M may have loops, multiple out-edges from the same node, multiple in-edges to the same node, edges from the same source node to the same target node with different symbols, etc.

Your definition of Δ_N should have a case for every possible state-symbol pair. If you are constructing an NFA with ϵ-transitions, you need to list the value of $\Delta_N(q, \epsilon)$ for every state $q \in Q_N$. Remember that Δ_N returns a *set* of states. So if there is "no transition" from a given state on a given symbol, define the value of Δ_N to be $\emptyset$ for that state and that symbol. Also be sure to remember that your definition of Δ_N can *only* use the function's arguments (q the current state, and c the observed symbol). You cannot mention any other properties specific to the input string since that would require the NFA to "relink" itself every time it sees a new input string.

Proving that $A' \subseteq L(N)$:
The next step is to use your definition above to prove that every string in A' is accepted by your NFA. This proof will almost always have the following format:

1. Let x be an *arbitrary* string in A'. All you can assume at this point is that x is some string in A'. Use the definition of A' to conclude that x can be represented in terms of some string y which is guaranteed to be in A.

2. Since $y \in A$, you know that $y \in L(M)$. State the definition of acceptance for DFA's and substitute y into that definition (i.e. $\hat{\delta}_M(s_M, y) \in F_M$).

3. Use your definition of N to find expressions that can be substituted into the above expression. These expressions will usually involve $\hat{\Delta}_N$. Your formal definition of N should include many set-formulas that are expressed in terms of s_M, δ_M, and F_M. This will allow you to substitute for those terms in the expression above.

4. Simplify and arrive at an expressions of the form $q \in \hat{\Delta}_N(S_N, x)$ and $q \in F_N$ (for the same $q \in Q_N$). State the definition of acceptance of NFAs ($\hat{\Delta}_N(S_N, x) \cap F_N \neq \emptyset$) and conclude that $x \in L(N)$.

Proving that $L(N) \subseteq A'$:
Now you must prove that N accepts *only* strings of A' and nothing else. This half of the proof is usually the more difficult one. Here's the general format that it will usually have:

1. Assume that $x \in L(N)$. At this point you know nothing about x at all. It could be any string. You do *not* know that it is a member of A' or that it has any particular form.

2. State the definition of acceptance for NFAs in terms of x and conclude that there exists an accepting path from some state in S_N to some state in F_N in which the transitions follow the symbols of x in order with any number of ϵ-transitions interspursed.

3. Use your definitions for S_N, F_N, and Δ_N to argue that *all* accepting paths through N have a certain form. This is a very dangerous part of the proof because you will be tempted to rely on what your intuition tells you about how N behaves instead of relying *purely* on the formal definition of N. It may help to say exactly which lines in the definition tell you which things. You will also be tempted to make incorrect assumptions about how NFA's behave. Some things to remember include:

   (a) If an NFA has ϵ-transitions, they are NOT necessarily taken. In general, an accepting path through an NFA may include any number of ϵ-transitions at any points in the path, or may include none at all. Since you are dealing with an arbitrary accepting path, you cannot assume that your path *does* take an ϵ-transition just because it *can* take an ϵ-transition. The same thing goes for multiple transitions from a single state for the same symbol.

(b) An accepting path may include repeated states (loops), return to a start state several times, pass through final states several times, etc. before it finally stops at some final state.

(c) Two different strings may have different accepting paths that both start in the same start state and end in the same final state. I.e. two *different* strings may end up being accepted in the *same* final state.

(d) A single string accepted by an NFA may have *multiple* distinct accepting paths. These paths may even start at the same start state and end at the same final state but still be distinct.

4. Use the form that, in step 3, you concluded that an accepting path must have, to generate some statements about x in terms of $\hat{\Delta}_N$, S_N, and F_N.

5. Use your definition of N to substitute expressions involving $\hat{\delta}_M$, s_M, and F_M for the expressions derived above.

6. Simplify and arrive at the conclusion that $\hat{\delta}_M(s_M, y) \in F_M$ where y is some string represented in terms of x. Conclude that $y \in L(M) = A$.

7. Observe that y's representation in terms of x matches the definition of A'. Therefore since $y \in A$, it must be that $x \in A'$.

To make these ideas concrete, let us use the example of problem 28 on p. 322 of Kozen. The problem is stated as follows:

> *Given a set $A \subseteq \{0,1\}^*$, let*
>
> $$A' = \{xy | x1y \in A\}.$$
>
> *Show that if A is regular, then so is A'.*

In the following pages I give a solution to this problem using the procedure described above. This proof is a bit pedantic but I explain almost every detail so that you will understand where each step comes from. It is important to notice that when we say "from the definition of N it follows that..." in a proof, we refer to something very specific in the formal definition of N. You cannot make arbitrary statements based on your intuition about how N behaves and claim that this follows from the definition of N. Your intuition will often be incorrect and that is how most proofs go wrong. In this proof I go so far as to number the lines in the definition of N and identify exactly which one I am using at each step. I have also numbered the steps of the proof in accordance with the procedure described previously so that you can follow the motivation behind the argument.

Construction of N:
Since A is regular, there exists a DFA, $M = (Q_M, \{0,1\}, \delta_M, s_M, F_M)$, such that $L(M) = A$. Define an NFA, $N = (Q_N, \{0,1\}, \Delta_N, S_N, F_N)$ as follows:

$$Q_N = Q_M \times \{a, b\} \tag{0}$$
$$\Delta_N((q,a), c) = \{(\delta_M(q,c), a)\} \ \forall q \in Q_M, c \in \{0,1\} \tag{1}$$
$$\Delta_N((q,a), \epsilon) = \{(\delta_M(q,1), b)\} \ \forall q \in Q_M \tag{2}$$
$$\Delta_N((q,b), c) = \{(\delta_M(q,c), b)\} \ \forall q \in Q_M, c \in \{0,1\} \tag{3}$$
$$\Delta_N((q,b), \epsilon) = \emptyset \ \forall q \in Q_M \tag{4}$$
$$S_N = \{(s_M, a)\} \tag{5}$$
$$F_N = F_M \times \{b\} \tag{6}$$

Proof that $A' \subseteq L(N)$**:**

1. Let $z \in A'$ be given. From the definition of A', we know that z can be written as xy for some $x, y \in \{0,1\}^*$ such that $x1y \in A$.

2. Since $x1y \in A$, we know that $x1y \in L(M)$. The definition of acceptance for DFAs tells us that $\hat{\delta}_M(s_M, x1y) \in F_M$.

3. From properties of $\hat{\delta}$ that we've proved in class and on homeworks, we know that $\hat{\delta}_M(s_M, x1y) = \hat{\delta}_M(\delta_M(\hat{\delta}_M(s_M, x), 1), y)$. Let's give names to these subexpressions. Define the following:

$$p = \hat{\delta}_M(s_M, x) \tag{7}$$
$$q = \delta_M(p, 1) \tag{8}$$
$$r = \hat{\delta}_M(q, y) \tag{9}$$

Substituting*(7) into (1) results in

$$(p, a) \in \hat{\Delta}_N(\{(s_M, a)\}, x). \tag{10}$$

Substituting (8) into (3) results in

$$(q, b) \in \Delta_N((p, a), \epsilon). \tag{11}$$

*Technically this is not actually a blind substitution of one expression into another. (1) talks about Δ_N while (7) talks about $\hat{\Delta}_N$. A trivial inductive argument will allow you to perform this substitution, however. In your proofs you can treat this inductive argument as "obvious" and not show it. But you should still be careful when you do something like this. In this case the induction works because (1) is quantified over *all* $q \in Q_M$. If any transitions of M had been deleted in our copies, this would no longer be true! So be wary.

Substituting (9) into (4) results in

$$(r, b) \in \hat{\Delta}_N(\{(q, b)\}, y). \tag{12}$$

Substituting (10) into (11) and (11) into (12) results in

$$(r, b) \in \hat{\Delta}_N(\hat{\Delta}_N(\hat{\Delta}_N(\{(s_M, a)\}, x), \epsilon), y) = \hat{\Delta}_N(\{(s_M, a)\}, x\epsilon y) = \hat{\Delta}_N(\{(s_M, a)\}, xy).$$

Using (5) to substitute for $\{(s_M, a)\}$ in the expression yields

$$(r, b) \in \hat{\Delta}_N(S_N, xy).$$

Remembering that $r = \hat{\delta}_M(s_M, x1y) \in F_M$, we conclude from (6) that $(r, b) \in F_N$.

4. Thus $\hat{\Delta}_N(S_N, xy) \cap F_N \neq \emptyset$ (because (r, b) is in both sets). So by the definition of acceptance for NFA's, $z = xy \in L(N)$.

Proof that $L(N) \subseteq A'$:

1. Let $z \in L(N)$ be given.
2. By the definition of acceptance for NFA's, $\hat{\Delta}_N(S_N, z) \cap F_N \neq \emptyset$. Thus there exists a path from some state in S_N to some state in F_N that follows transitions for the symbols of z in proper order *possibly* with ϵ-transitions interspursed.
3. From (5) we know that this path must start in (s_M, a). From (6) we know that this path must end in some state of the form (r, b) for some $r \in F_M$. Therefore at some point there must be a transition from some state of the form (p, a) $(p \in Q_M)$ to some state of the form (q, b) $(q \in Q_M)$. (We don't yet know how many times this may happen but we know it happens at least once.) Looking at lines (1), (2), (3), and (4), we observe that there are no transitions from states that end in b to states that end in a. Thus once we are in state (q, b), all remaining states in the path must end in b. From this we conclude that the transition from an a state to a b state happens no more than once. Therefore such a transition happens exactly once.
4. Thus we have determined that this accepting path must have the following form:
   (a) It starts in (s_M, a).
   (b) Next it makes zero or more transitions which stay in a states until it gets to (p, a). So

   $$(p, a) \in \hat{\Delta}_N(\{(s_M, a)\}, x) \tag{13}$$

   for some $x \in \{0, 1\}^*$.

(c) Next it jumps from (p, a) to (q, b). So

$$(q, b) \in \Delta_N((p, a), c) \tag{14}$$

for some $c \in \{0, 1, \epsilon\}$.

(d) Finally it makes zero or more transitions which stay in b states until it gets to (r, b). So

$$(r, b) \in \hat{\Delta}_N(\{(q, b)\}, y) \tag{15}$$

for some $y \in \{0, 1\}^*$. Also recall that $r \in F_M$.

It is important to note that since this path by assumption is an accepting path for z, it must be that $z = xcy$.

5. Looking at lines (1), (2), (3), and (4), we see that there is only one kind of transition that would allow us to go from a state in the a copy of M to another state in the a copy as described in (a), and that is given by line (1). Thus substituting[†] (13) into (1) results in

$$\hat{\delta}_M(s_M, x) = p. \tag{16}$$

Again looking at lines (1) through (4), we see that there is only one kind of transition that allows us to go from a state in the a copy to a state in the b copy as described in (b), and that is given by line (2). Substituting (14) into (2) tells us that

$$\delta_M(p, 1) = q. \tag{17}$$

And finally, the only line of lines (1) through (4) that allows us to go from a state in the b copy to another state in the b copy as in (c) is line (3). Substituting (15) into (3) gives us

$$\hat{\delta}_M(q, y) = r. \tag{18}$$

6. Substituting (16) into (17) and (17) into (18) results in

$$r = \hat{\delta}_M(\delta_M(\hat{\delta}_M(s_M, x), 1), y) = \hat{\delta}_M(s_M, x1y).$$

Remember that $r \in F_M$. So by the definition of acceptance for DFA's, $x1y \in L(M) = A$.

7. By the definition of A', if $x1y \in A$ then $z = xy \in A'$.

[†]Again, this is substitution applied inductively as described earlier. It works because (1) is quantified over *all* $q \in Q_M$.