Lecture #4: DFA Design and Verification — Part Two

Key Concepts

During the previous lecture, a ***design process*** was proposed, which can be followed to design a deterministic finite automaton for a given language.

- This is process is *not* guaranteed to succeed. One way for it to fail involves a discovery that one or more transitions, for the DFA being developed, would not be well-defined.
- If this happens then the ***reason*** for this kind of failure should be carefully examined, to see whether *additional information* about the string processed, so far, was missed on a previous attempt — and should now be added to the information that is being used to design a DFA.
- At this point the design process should be "rolled back" to the beginning and repeated.
- Since this involves additional information, or detail, this can be (arguably) be seen as one form of ***refinement*** — something that is also useful for other design processes.

Students should be able to understand — and use — the following result, to prove that a given DFA has a given language, after following the design process that has been given. It is not necessary for students to understand (or describe) this result's proof, even though students might be able to do that:

Theorem 1 (Correctness of a DFA)**.** *Let $L \subseteq \Sigma^\star$, for an alphabet Σ, and let*

$$M = (Q, \Sigma, \delta, q_0, F)$$

be a deterministic finite automaton with the same alphabet Σ. Suppose that (after renaming states, if needed)

$$Q = \{q_0, q_1, \ldots, q_{n-1}\}$$

where $n = |Q| \geq 1$. Suppose, as well, that

$$S_0, S_1, \ldots, S_{n-1}$$

are subsets of $\Sigma^\star$ such that the following properties are satisfied.

(a) Every string in $\Sigma^\star$ belongs to **exactly one** *of $S_0, S_1, \ldots, S_{n-1}$.*

(b) $\lambda \in S_0$.

(c) $S_i \subseteq L$ for every integer i such that $0 \leq i \leq n-1$ and $q_i \in F$.

(d) $S_i \cap L = \emptyset$ for every integer i such that $0 \leq i \leq n-1$ and $q_i \notin F$.

(e) The following property is satisfied, for every integer i such that $0 \leq i \leq n-1$ and for every symbol $\sigma \in \Sigma$:

> *"Suppose that $q_j = \delta(q_i, \sigma)$ (so that $0 \leq j \leq n-1$). Then*
>
> $$\{\omega \cdot \sigma \mid \omega \in S_i\} \subseteq S_j."$$

Then $L(M) = L$.