constructing automata from regular languages

Canonical name	ConstructingAutomataFromRegularLanguages
Date of creation	2013-03-22 19:02:09
Last modified on	2013-03-22 19:02:09
Owner	CWoo (3771)
Last modified by	CWoo (3771)
Numerical id	11
Author	CWoo (3771)
Entry type	Definition
Classification	msc 03D10
Classification	msc 68Q42
Classification	msc 68Q05
Defines	Myhill-Nerode relation

In this entry, we describe how a certain equivalence relation on words gives rise to a deterministic automaton, and show that deterministic automata to a certain extent can be characterized by these equivalence relations.

Constructing the automaton

Let Σ be an alphabet and R a subset of Σ^*, the set of all words over Σ. Consider an equivalence relation $\equiv$ on Σ^* satisfying the following two conditions:

- $\equiv$ is a right congruence: if $u \equiv v$, then $uw \equiv vw$ for any word w over Σ,
- $u \equiv v$ implies that $u \in R$ iff $v \in R$.

An example of this is the Nerode equivalence $\mathcal{N}_R$ of R (in fact, the largest such relation).

We can construct an automaton $A = (S, \Sigma, \delta, I, F)$ based on $\equiv$. Here's how:

- $S = \Sigma^*/\equiv$, the set of equivalence classes of $\equiv$; elements of S are denoted by $[u]$ for any $u \in \Sigma^*$,
- $\delta : S \times \Sigma \to S$ is given by $\delta([u], a) = [ua]$,
- I is a singleton consisting of $[\lambda]$, the equivalence class consisting of the empty word λ,
- F is the set consisting of $[u]$, where $u \in R$.

By condition 1, δ is well-defined, so A is a deterministic automaton. By the second condition above, $[u] \in F$ iff $u \in R$.

By induction, we see that $\delta([u], v) = [uv]$ for any word v over Σ. So

$$u \equiv v \qquad \text{iff} \qquad \delta([u], \lambda) = \delta([v], \lambda).$$

One consequence of this is that A is accessible (all states are accessible).

In addition, $R = L(A)$, as $u \in L(A)$ iff $\delta([\lambda], u) \in F$ iff $[u] \in F$ iff $u \in R$.

Constructing the equivalence relation

Conversely, given a deterministic automaton $A = (S, \Sigma, \delta, \{q_0\}, F)$, a binary relation $\equiv$ on Σ^* may be defined:

$$u \equiv v \qquad \text{iff} \qquad \delta(q_0, u) = \delta(q_0, v).$$

This binary relation is clearly an equivalence relation, and it satisfies the two conditions above, with $R = L(A)$:

- $\delta(q_0, uw) = \delta(\delta(q_0, u), w) = \delta(\delta(q_0, v), w) = \delta(q_0, vw)$,
- if $\delta(q_0, u) = \delta(q_0, v)$, then clearly $u \in L(A)$ iff $v \in L(A)$.

So $[u] = \{v \in S \mid \delta(q_0, v) = \delta(q_0, u)\}$.

Remark. We could have defined the binary relation $u \equiv v$ to mean $\delta(q, u) = \delta(q, v)$ for all $q \in S$. This is also an equivalence relation that satisfies both of the conditions above. However, this is stronger in the sense that $\equiv$ is a congruence: if $u \equiv v$, then $\delta(q, wu) = \delta(\delta(q, w), u) = \delta(\delta(q, w), v) = \delta(q, wv)$ so that $wu \equiv wv$. In this entry, only the weaker assumption that $\equiv$ is a right congruence is needed.

Characterization

Fix an alphabet Σ and a set $R \subseteq \Sigma^*$. Let X the set of equivalence relations satisfying the two conditions above, and Y the set of accessible deterministic automata over Σ accepting R. Define $f : X \to Y$ and $g : Y \to X$ such that $f(\equiv)$ and $g(A)$ are the automaton and relation constructed above.

Proposition 1. *$g \circ f = 1_X$ and $f(g(A))$ is isomorphic to A.*

Proof. Suppose $\equiv_1 \overset{f}{\mapsto} A \overset{g}{\mapsto} \equiv_2$. Then $u \equiv_1 v$ iff $\delta([u], \lambda) = \delta([v], \lambda)$ iff $\delta([\lambda], u) = \delta([\lambda], v)$ iff $u \equiv_2 v$.

Conversely, suppose $A_1 = (S_1, \Sigma, \delta_1, q_1, F_2) \overset{g}{\mapsto} \equiv \overset{f}{\mapsto} A_2 = (S_2, \Sigma, \delta_2, q_2, F_2)$. Then $S_2 = \Sigma^*/\equiv$, $q_2 = [\lambda]$, and F_2 consists of all $[u]$ such that $u \in L(A_1)$. As a result, $u \in L(A_2)$ iff $\delta_2([\lambda], u) = \delta_2(q_2, u) \in F_2$ iff $[u] = \delta_2([u], \lambda) \in F_2$ iff $u \in L(A_1)$. This shows that A_1 is equivalent to A_2.

To show A_1 is isomorphic to A_2, define $\phi : S_2 \to S_1$ by $\phi([u]) = \delta_1(q_1, u)$. Then

- ϕ is well-defined by the definition of $\equiv$, and it is injective for the same reason. Now, let $s \in S$, then since A_1 is accessible, there is a word u such that $\delta_1(q_1, u) = s$, so that $\phi([u]) = s$. This shows that ϕ is a bijection.

- $\phi(q_2) = \phi([\lambda]) = \delta_1(q_1, \lambda) = q_1$.

- $\phi([u]) \in F_1$ iff $\delta_1(q_1, u) \in F_1$ iff $u \in L(A_1) = L(A_2)$ iff $[u] \in F_2$. Therefore, $\phi(F_2) = F_1$.

- Finally, $\phi(\delta_2([u], a)) = \phi([ua]) = \delta_1(q_1, ua) = \delta_1(\delta_1(q_1, u), a) = \delta_1(\phi([u]), a)$.

Thus, ϕ is a homomorphism from A_1 to A_2, together with the fact that ϕ is a bijection, A_1 is isormorphic to A_2. $\square$

Proposition 2. *If $\equiv$ is the Nerode equivalence of R, then the $f(\equiv)$ is a reduced automaton. If A is reduced, then $g(A)$ is the Nerode equivalence of R.*

Proof. Suppose $\equiv$ is the Nerode equivlance. If $f(\equiv)$ is not reduced, reduce it to a reduced automaton A. Then $\equiv \subseteq g(A)$. Since $g(A)$ satisfies the two conditions above and $\equiv$ is the largest such relation, $\equiv = g(A)$. Therefore $f(\equiv) = f(g(A))$ is isomorphic to A. But A is reduced, so must $f(\equiv)$.

On the other hand, suppose A is reduced. Then $g(A) \subseteq \mathcal{N}_R$. Conversely, if $u\mathcal{N}_R v$, then $uw \in R$ iff $vw \in R$ for any word w, so that $\delta(q_0, uw) = \delta(q_0, vw)$, or $\delta(\delta(q_0, u), w) = \delta(\delta(q_0, v), w)$, which implies $\delta(q_0, u)$ and $\delta(q_0, v)$ are indistinguishable. But A is reduced, this means $\delta(q_0, u) = \delta(q_0, v)$. As a result $ug(A)v$, or $g(A) = \mathcal{N}_R$. $\square$

Definition. A *Myhill-Nerode relation* for $R \subseteq \Sigma^*$ is an equivalence relation $\equiv$ that satisfies the two conditions above, and that $\Sigma^*/\equiv$ is finite.

Combining from what we just discussed above, we see that a language R is regular iff its Nerode equivalence is a Myhill-Nerode relation, which is the essence of Myhill-Nerode theorem.