Myhill–Nerode Theorem

Recall : An equivalence relation $\equiv$ on Σ^* is called a MN relation for R if

1. Right congruence : $x \equiv y \Rightarrow xa \equiv ya \quad \forall a \in \Sigma$

   $x \equiv y \Rightarrow xz \equiv yz \quad \forall z \in \Sigma^*$ [induction on $|z|$]

2. $\equiv$ refines R : $x \equiv y \Rightarrow (x \in R \Leftrightarrow y \in R)$
3. $\equiv$ has finite index.

An equivalence relation $\equiv$ on Σ^* is called a MN' relation for R if $\equiv$ satisfies 1 and 2.

Recall (a) $M \longmapsto \equiv_M$ (b) $\equiv \longmapsto M_{\equiv}$

inverses of one another

$\equiv$ on $\Sigma^* \longrightarrow$ a machine (DFA) involved

Def: Let $R \subseteq \Sigma^*$ (not necessarily regular). Define $\equiv_R$ as:

$$x \equiv_R y \iff \forall z \in \Sigma^* \left(xz \in R \iff yz \in R \right).$$

Lemma: $\equiv_R$ is an MN' relation.

Proof: 1. (Right congruence) $\quad z = aw$

$$x \equiv_R y \implies \forall a \in \Sigma \; \forall w \in \Sigma^* \left(\underline{xa}w \in R \iff \underline{ya}w \in R \right)$$

$$\implies \forall a \in \Sigma \; \left[xa \equiv_R ya \right]$$

2. $\equiv_R$ refines R $\quad$ Take $z = \epsilon$.

Def: $\equiv_1$ and $\equiv_2$ are two equivalence relations. $\equiv_1$ refines $\equiv_2$ if $\equiv_1 \subseteq \equiv_2$.

Example: cong mod 6 refines cong mod 3 [equiv rel on $\mathbb{Z}$]

Lemma: If $\equiv$ is an MN' relation for R, then $\equiv$ refines $\equiv_R$.

Proof: $x \equiv y \Rightarrow \forall z\,(xz \equiv yz) \Rightarrow \forall z\,(xz \in R \Leftrightarrow yz \in R)$

$\Rightarrow x \equiv_R y$.

a

$\equiv_R$ is the coarsest MN' relation for R.

$\equiv_1, \equiv_2 \rightarrow$ coarsest MN' relations for R

$\equiv_1 \subseteq \equiv_2$ and $\equiv_2 \subseteq \equiv_1 \Rightarrow \equiv_1 = \equiv_2$.

Myhill-Nerode Theorem : For a language $R \subseteq \Sigma^*$, the following are equivalent :

(a) R is regular

(b) R has an MN relation

(c) $\equiv_R$ has finite index.

An if and only if condition
— Both regularity and non-regularity

Proof : $[(a) \Rightarrow (b)]$ DFA M for R. $\equiv_M$ is a MN relation for R.

$[(b) \Rightarrow (c)]$ $\equiv$ is a MN relation for R

$\Rightarrow$ $\equiv$ refines $\equiv_R$

$\equiv$ → finite index

$\equiv_R$ ↪ no finer than $\equiv$ ↪ also of finite index.

$[(c) \Rightarrow (a)]$ $\equiv_R$ is of finite index

$\equiv_R \longmapsto M_{\equiv_R} \longleftarrow$ a DFA. ◀

Application 1

Let $R \subseteq \Sigma^*$ be regular. Let M be a collapsed DFA for R.
(without any inaccessible states)

Then $\equiv_M \; = \; \equiv_R$.

Proof:

$$p \approx q \iff \forall z \left(\hat{\delta}(p,z) \in F \iff \hat{\delta}(q,z) \in F \right)$$

$$\iff p = q.$$

$x \equiv_R y$

$$\iff \forall z \in \Sigma^* \left(xz \in R \iff yz \in R \right)$$

$$\iff \forall z \in \Sigma^* \left(\hat{\delta}(s, xz) \in F \iff \hat{\delta}(s, yz) \in F \right)$$

$$\iff \forall z \in \Sigma^* \left(\hat{\delta}(\underbrace{\hat{\delta}(s,x)}_{p}, z) \in F \iff \hat{\delta}(\underbrace{\hat{\delta}(s,y)}_{q}, z) \in F \right)$$

$$\iff \hat{\delta}(s,x) \approx \hat{\delta}(s,y)$$

$$\iff \hat{\delta}(s,x) = \hat{\delta}(s,y) \iff x \equiv_M y.$$

Minimized DFA is unique.

Application 2

$A = \{ a^n b^n \mid n \geq 0 \}$ is not regular.

Proof: $\equiv_A$ is not of finite index.

$$[a^k] \neq [a^l] \qquad k \neq l$$

$z = b^k$ $\qquad a^k b^k \in A$ but $a^k b^l \notin A$

There are at least these many equivalence classes:

$$[a^0], [a^1], [a^2], [a^3], \ldots$$

$\Rightarrow$ $\equiv_A$ is not of finite index.

$\Rightarrow$ A is not regular.

What about "minimization of NFA"?

— See Kozen.