COSC 341
Theory of Computing
Lecture 6
Equivalence relations and the Myhill-Nerode theorem

Stephen Cranefield
stephen.cranefield@otago.ac.nz

Lecture slides (mostly) by Michael Albert

Keywords: Equivalence relations,
suffix-equivalence, Myhill-Nerode theorem

Motivation

Recall Question 5 from Tutorial 4:

> *Is there a DFA over the one-letter alphabet* $\{a\}$ *that accepts all, and only, those strings whose length is a power of two?*

Strings in the language:

ϵ
aa + 2 more characters
$aaaa$ + 4 more characters
$aaaaaaaa$ + 8 more characters
$\ldots$

There's something going on here related to the suffixes that must be appended to a word to have it accepted. The Myhill-Nerode theorem is based on this idea.

Equivalence relations

- The concept of *equivalence relation* is one of the most significant in mathematics.
- An equivalence relation is present whenever there is some notion of similarity or sameness of structures that captures some (in context) important part of their nature but is less restrictive than equality.

Definition

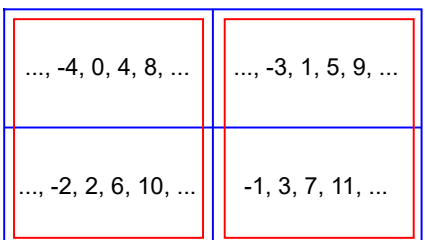
An equivalence relation, $\sim$, on a set X is any binary relation with the following three properties:

- It is reflexive, which means that $x \sim x$ for all $x \in X$.
- It is symmetric, which means that, for all $x, y \in X$ if $x \sim y$ then $y \sim x$.
- It is transitive, which means that, for all $x, y, z \in X$ if $x \sim y$ and $y \sim z$ then $x \sim z$.

Example equivalence relation

Let d be a positive integer. Define the relation $\equiv$ on the set $\mathbb{Z}$ of all integers by:

$$x \equiv_d y \iff d \text{ is a divisor of } y - x.$$



Check that this defines an equivalence relation.

Coarser? Finer?

Given two equivalence relations $\sim$ and $\equiv$ on the same set, we say that $\sim$ is coarser than $\equiv$ (and $\equiv$ is finer than or refines $\sim$) if:

$$x \equiv y \quad \Longrightarrow \quad x \sim y.$$

Example: $\equiv_2$ is coarser than $\equiv_4$ (see previous slide)

- If $\equiv$ is finer than $\sim$, then the $\equiv$-equivalence classes are formed by splitting apart $\sim$-equivalence classes.
- Equality is the finest equivalence relation on a set.
- The "everyone is the same" relation is the coarsest equivalence relation on a set.
- The intersection of two equivalence relations is their coarsest common refinement!

Equivalence classes and partitions

Given an equivalence relation, $\sim$ on a set X and an element $x \in X$, the equivalence class of x under $\sim$ is:

$$[x]_{\sim} = \{y \in X \,:\, x \sim y\}$$

- If two elements are $\sim$-equivalent they have the same equivalence class.
- If two elements are not $\sim$-equivalent their equivalence classes are disjoint.
- This means that the equivalence classes partition X.

State-equivalence

Let $\mathbf{A}$ be a DFA over Σ. Define a relation, $\sim_{\text{state}}$ on Σ^* called state equivalence by:

$$w \sim_{\text{state}} v \iff \begin{array}{l}\text{the state reached in } \mathbf{A} \text{ by processing } v \text{ is} \\ \text{the same as that reached by processing} \\ w.\end{array}$$

- Check that this is an equivalence relation
- How many equivalence classes does it have?
  - The number of reachable states of $\mathbf{A}$.

Suffix-equivalence

Let $\mathbf{A}$ be a DFA over Σ. Define a relation, $\sim_{\text{suffix}}$ on Σ^* called suffix equivalence by:

$$u \sim_{\text{suffix}} v \iff \begin{array}{l}\text{for every word } w\text{, either both } uw \text{ and } vw \\ \text{are accepted by } \mathbf{A} \text{ or neither is}\end{array}$$

That is "the suffixes we can attach to u or v to produce a word in $L_{\mathbf{A}}$ are the same".

- Check that this is an equivalence relation
- **What is the relationship between suffix-equivalence and state-equivalence?**
  - If words w and v are state-equivalent then they are suffix-equivalent.
  - So suffix-equivalence is a coarser equivalence relation than state-equivalence.
  - Therefore, the number of suffix-equivalence classes can be no larger than the number of reachable states of $\mathbf{A}$.

Suffix-equivalence for a language (without a DFA)

Given a language L over alphabet Σ, a distinguishing extension of two words $u, v \in \Sigma^*$ is any word $w \in \Sigma^*$ such that exactly one of uw and vw is in L.

Example: $L = \{a^n : n \text{ is even}\}$. For any k, a is a distinguishing extension of a^k and a^{k+1}.

We define suffix equivalence (modulo L) as follows:

$$u \sim_{\text{suffix}} v \iff \text{there is no distinguishing extension for } u \text{ and } v$$

Alternatively, for any $w \in \Sigma^*$ define the suffix language of w modulo L:

$$\mathit{Suff}(w, L) = \{y \in \Sigma^* : wy \in L\}.$$

Then $u \sim_{\text{suffix}} v$ just means $\mathit{Suff}(u, L) = \mathit{Suff}(v, L)$.

The Myhill-Nerode theorem

Theorem

A language is regular if and only if its suffix-equivalence relation has only finitely many equivalence classes.

Uses of the Myhill-Nerode Theorem

1. Try to show that a language is regular by an exhaustive case analysis. Begin with ϵ and consider increasingly longer strings while trying to find distinguishing extensions until no more equivalence classes can be found.
2. Prove a language is not regular through logical analysis that shows there must be an infinite number of suffix-equivalence classes.

Example for case 2:

$L = \{a^n b^n : n \geq 0\}$.

- Given a^i and a^j for distinct i and j, consider the extension b^i.
- $a^i b^i \in L$ but $a^j b^i \notin L$.
- Thus b_i is a distinguishing extension and a^i and a^j are in different suffix-equivalence classes.