CS 361 Meeting 11 — 3/4/20

Announcements

1. Homework 4 is due Friday.

Distinguishable Prefixes

1. Consider the relation "distinguishable" that exists between strings over an alphabet relative to some language L.

   Definition: We say that $w, v \in \Sigma^*$ are *distinguishable* by a language L if for some $z \in \Sigma^*$, exactly one of wz and vz is a member of L.

   - It may help to first think about what it would mean for two strings to be "distinguishable" in a human language. Interestingly, human languages are so rich with nuance that I found it hard to think of examples that were not distinguishable.
     - One simple example is our definite and indefinite articles. The set of strings that can validly follow "A" is different from those that can follow "An".
     - One might think words we think of as synonyms would serve as counter examples, but the pair "big" an "large" don't quite work because "big bird met ernie" just isn't the same as "large bird met ernie".
   - We, of course, will be interested in how the term "distinguishable" applies to more exciting, formal languages like:

     $$L_{Div5} = \{w \mid w \in \{0,1\}^*, \text{ value of } w \text{ is divisible by } 5 \}$$

     - For this language, the strings
       10110
       10000
       are distinguishable by L_{Div5} because
       101101 is 45 which is divisible by 5
       100001 is 33 which is not divisible by 5
       while
       10110 = 32
       10001 = 27
       are indistinguishable by L_{Div5} because they are both equal to 2 mod 5 so any digits that one could add to 10110 to make it divisible by 5 would also extend 10001 into a number that was divisible by 5.

Equivalence Relations

1. Three of the "prerequisites" that you were supposed to review when you read Chapter 0 of the text are *relations* (in general), *binary relations* and *equivalence relations* (in particular).

   - A binary relation is a subset of the set $A \times A$ of all pairs of elements of some set A. Familiar examples include those induced on sets of numbers by relational operators
     - The "less than" relation is the set $\{(x, y) \mid x < y\}$
     - The "equals" relation is the set $\{(x, y) \mid x = y\}$
   - In general, if $R \subset A \times A$ we write $xRy \iff (x, y) \in R$.
   - An equivalence relation is a binary relation the satisfies three properties that seem to be key to the notion of equality:
     reflexive $\forall x \in A, xRx$.
     symmetric $\forall x, y \in A, xRy \iff yRx$.
     transitive $\forall x, y, z \in A, xRy$ and $yRz \Rightarrow xRz$.
   - If R is an equivalence relation we often write $x \equiv_R y$.
   - Some familiar examples of equivalence relations include simple equality of number, equality mod n, has the same birthday as (which is sort of equality mod 365).
   - With our interest in strings, we can also consider some equivalence relationships on strings. To keep things simple, let's consider strings of 0s and 1s.
     - equality

Click here to view the slides for this class

- same length as
- same number of 1s
- represents the same binary number (considering leading 0s insignificant)

2. Given an equivalence relation, we can define the notion of an equivalence class:

$$[x]_R = \{y \mid y \equiv_R x\}$$

- If xRy then $[x] = [y]$.
- Note that if x is not equivalent to x, then $[x] \cap [y] = \emptyset$.
- Every element belongs to some equivalence class.
- The equivalence classes therefore form a partition of the set of all values.

Equivalence Relations and Languages

1. The relation "indistinguishable by L" defined by

   Definition: We say that $w, v \in \Sigma^*$ are *indistinguishable* by language L if for all $z \in \Sigma^*, wz \in L \iff vz \in L$ and we write $w \equiv_L v$.

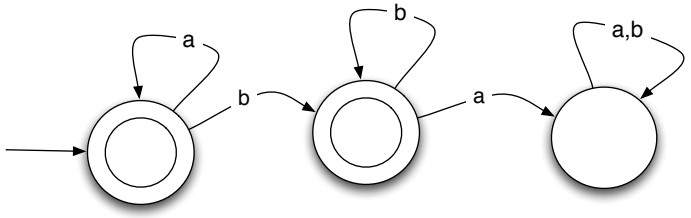
   is an equivalence relation on strings.

   - This claim is fairly obvious, but Sipser thought it was non-obvious enough to make a homework problem out of it (1.51) so...
     - It must be reflexive since $wz \in L \iff wz \in L$.
     - It must be symmetric since if $w \equiv_L v$ then for all z, $wz \in L \iff vz \in L$ which is equivalent to saying $vz \in L \iff wz \in L$ so $v \equiv_L w$.
     - Similarly, if $w \equiv_L v$ and $v \equiv_L x$ then for all z, $wz \in L \iff vz \in L \iff xz \in L$ so $w \equiv_L x$.

2. The number of distinct equivalence classes of strings under the indistinguishable relationship has an interesting relationship to regularity.

- Given a language L and a set X of strings over L's alphabet, we say that the X is pairwise distinguishable by L if every pair of strings in X is distinguishable by L.
- The *index* of a language L is the size of the largest set of strings X that is pairwise distinguishable by L. Equivalently, the index of a language is the size of the set of equivalence classes induced by the "indistinguishable" relation relative to the language.
  - Note: The index of a language can be infinite.
  - If L is $\{a^n b^n \mid n \geq 0\}$ then $X = \{a^n \mid n \geq 0\}$ is pairwise distinguishable by L since for any $i \neq j$, a^i is distinguished from a^j by b^i since $a^i b^i \in L$ but $a^j b^i \notin L$.
  - Consider the index of a^*b^*:
    Every string in Σ^* falls in one of three equivalence classes:
    * $[\epsilon] = [a^*]$.
    * $[a^*b] = [a^*bb^*]$
    * $[(a \cup b)^*ba]$

    Therefore, a^*b^* must be of index 3.
  - Interestingly, the index of a^*b^* corresponds to the number of states in the "obvious" DFA for the language.



The Myhill-Nerode Theorem

1. This bring us to the big Theorem (introduced through problem 1.52 in Sipser):

   Theorem (Myhill-Nerode): A language L is regular iff it has finite index and each regular language is accepted by a DFA whose description includes as many states as the index of the language.

2. First, I want you to understand how this theorem can serve as a substitute for the pumping lemma when you goal is to show that a language is not regular.

   - The theorem shows that a regular language must have finite index. So, if you can show that there exists some infinite set of mutually distinguishable strings (relative to the language), then the language cannot be regular.
   - As a simple example, we earlier observed that if L is $\{a^n b^n \mid n \geq 0\}$ then all the strings in the set $X = \{a^n \mid n \geq 0\}$ are pairwise distinguishable from one another by L. This is true because for any $i \neq j$, a^i is distinguished from a^j by b^i since $a^i b^i \in L$ but $a^j b^i \notin L$.
   - This implies the index of L is infinite so L cannot be regular.
   - You may recall that the example $L_{NEQ} = \{1^n \neq 1^m \mid n \neq m\}$ is not regular but showing this with the pumping lemma required a tricky proof involving p!.
   - Consider the set $X = \{1^n \neq \ \mid n \geq 1\}$. Any two elements $w = 1^n \neq$ and $v = 1^m \neq$ of this set such that $m \neq n$ are distinguishable relative to L_{NEQ} by the string $z = 1^n$ because $wz = 1^n \neq 1^n \notin L_{NEQ}$ while $vz = 1^n \neq 1^m \notin L_{NEQ}$. Thus X is an infinite set of mutually distinguishable strings. This implies that L_{NEQ} has infinite index and must not be regular.

3. Now consider how we can prove one direction of the Myhill-Nerode theorem, namely that regularity implies finite index.

   Proof:

   (a) Suppose that L is regular.
   - Then there is some DFA $D = (Q, \Sigma, \delta, s, F)$ such that $L = L(D)$.
   - Suppose that X is a set of strings that is pairwise distinguishable by L with $w, v \in X$.
   - Consider $\hat{\delta}(s, w)$ and $\hat{\delta}(s, v)$.
   - If $\hat{\delta}(s, w) = \hat{\delta}(s, v)$ then for all $z \in \Sigma^*$, $\hat{\delta}(s, wz) = \hat{\delta}(s, vz)$. But $wz \in L \iff \hat{\delta}(s, wz) \in F \iff \hat{\delta}(s, vz) \in F \iff vz \in L$ which would imply that w and z were indistinguishable by L.
   - Since the members of X are pairwise distinguishable, this cannot be the case so for all w, v it must be the case that $\hat{\delta}(s, w) \neq \hat{\delta}(s, v)$.
   - This implies that the number of elements in X cannot exceed the number of elements in Q since otherwise there would have to be at least two strings in X such that $\hat{\delta}(s, w) = \hat{\delta}(s, v)$. Therefore, if L is regular it is of finite index.