Limitations of Finite Automata

(LECTURE 6)

Limitations of FAs

Problem: Is there any set not regular ?

ans: yes!

example: $B = \{a^n b^n \mid n \geq 0 \} = \{e,ab,aabb,aaabbb,\ldots\}$

Intuition: Any machine accepting B must be able to remember the number of a's it has scanned before encountering the first b, but this requires infinite amount of memory (states) and is beyond the capability of any FA , which has only a finite amount of memory (states).

The proof

Lemma 1: Let M = (Q, S, d, s, F) be any DFA accepting B. Then for all non-negative numbers m, n , m$\neq$ n implies D(s, a^m) $\neq$ D(s, a^n).

pf: Assume D(s, a^m) = D(s, a^n) from some m $\neq$ n. Then D(s, $a^m b^n$) = D(D(s, a^m), b^n)

= D(D(s, a^n), b^n) = D(s, a^n b^n)$\in$F

It implies $a^m b^n$ $\in$L(M) = B. But $a^m b^n$ $\notin$ B since m $\neq$ n. Hence D(s, a^m) $\neq$ D(s, a^n) for all m$\neq$ n.

Theorem: B is not regular.

Pf: Assume B is regular and accepted by some DFA M with k states.

But by Lemma1, M must have an infinite number of states (

since all D(s, a^m)$\in$Q (m = 0,1,2,...) must be distinct.). This contradicts the requirement that the state set Q of M is finite.

Another nonregular set

- $C = \{a^{2^n} \mid n > 0\} = \{a, aa, aaaa, aaaaaaaa, \ldots \}$ is nonregular

pf: assume C is regular and is accepted by a DFA with k states.

Let $n > k$ and $x = a^{2^n} \in C$. Now consider the sequence of states: $D(s,a), D(s,aa), \ldots, D(s,a^n)$,

$s - a - s_1 - a - s_2 - \ldots \quad s_i - a - s_{i+1} - a\ldots \text{--}\ s_{i+d}\ \text{--}\ a\ \text{--}\ \ldots\ \text{--}\ s_n$.

by pigeonhole principle, there are $0<i<i+d \le n$ s.t.

$D(s,a^i) = D(s,a^{i+d})$ [= p]

let $2^n = i + d + m$.

=> $D(s, a^{2^n+d}) = D(s, a^i a^d a^d a^m) = D(s,a^i a^d a^m) = D(s, a^{2^n}) \in F$.

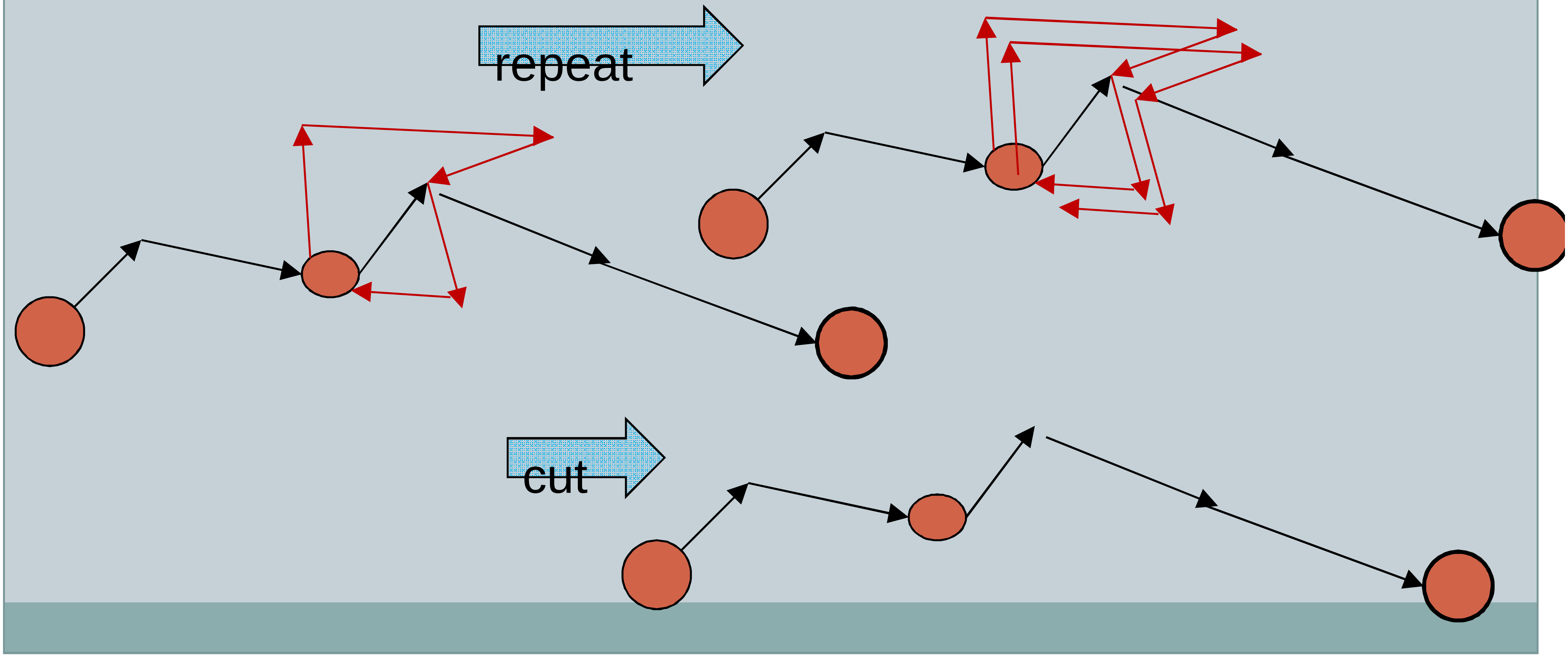
But since $2^n + d < 2^n + n < 2^n+2^n = 2^{n+1}$, which is the next power of 2 $> 2^n$, Hence $a^{2^n+d} \notin C$

=> the DFA also accepts a string $\notin C$, a contradiction!

Hence C is not regular.

Intuition behind the Pumping Lemma for FA

- For an FA to accept a long string s (≥ its number of states), the visited path for s must contains a cycle and hence can be cut or repeated to accept also many new strings.



The pumping lemma

Theorem 11.1: If A is a regular set, then

(P): $\$ k > 0$ s.t. for any string $xyz \in A$ with $|y| \geq k$,

there exists a decomposition $y = uvw$ s.t.

$v \neq e$ and for all $i \geq 0$, the string $xuv^iwz \in A$.

pf: Similar to the previous examples. Let $k = |Q|$ where Q is the set of states in a DFA accepting A. Also let s and F be the initial and set of final states of the FA, respectively. Now if there is a string $xyz \in A$ with $|y| \geq k$, consider the sequence of states:

$$D(s,xy_0), D(s, xy_1), D(s,xy_2), \ldots D(s, xy_k),$$

where y_j ($j = 0..k$) denote the prefix of y of the first j symbols. Since there are k+1 items in the sequence, each a state in Q, by pigeonhole principle, there must exist two items $D(s, xy_m)$, $D(s, xy_n)$ corresponding to the same state. Without loss of generality, assume $m < n$. Now let $u = y_m$, $y_n = u\, v$ and $y= uvw$.

We thus have $D(s, xuwz) = D(s, xy_m wz) = D(s, xy_nwz) = D(s, xuvwz) \in F$

Likewise, for all $j > 1$, $D(s, xuv^jwz) = D(xuv\, v^{j-1}\, wz) = D(xuv^{j-1}\, wz) = \ldots = D(xuv^{j-2}\, wz) = \ldots$ $=D(s,xuvwz) \in F$. QED

The pumping lemma

Theorem 11.1: Let A be any language. If A is a regular, then

(P): \$ k > 0 s.t. for any string xyz ∈ A with |y| ≥ k,

there exist a decomposition y = uvw s.t.

v ≠ e and for all i ≥ 0, the string xuv^iwz ∈ A.

Theorem 11.2 (pumping lemma, the contropositive form)

If A is any language satisfying the property (~P):

∀k> 0 \$ xyz ∈ A s.t. |y| ≥ k and ∀u,v,w with uvw = y and v ≠ e, there exists an i ≥ 0 s.t. xuv^ivw ∉ A,

then A is not regular. [~P means

for any k > 0, there is a substring of length ≥ k [of a member] of A, a cut or a certain duplicates of the middle of any 3-segment decomposition of which will produce a string □ ∉ A.]

Game semantics for quantification

1. Two players:
   - You (want to show a theorem T holds)
   - Demon (the opponent want to show T does not hold)

- rules: If the game (or proposition) G is
  - ∀x:U, F ==> D pick a member a of U and continue the game F(a).
  - ∃x:U, F ==> Y choose a nmember b of U and continue the game F(b).
  - if G has no quantification then end.
- Result:
  - Y win if the resulting proposition holds
  - D wins o/w
- T holds if Y has a winning strategy (always wins).

Examples

- Show that (∀x:nat, ∃ y:nat, x < y).

pf:

D: choose any number k for x.

Y: let y be k + 1

Result: k < k+1 , so Y wins.

Since Y always wins in this game. The result is proved.

The winning strategy is the function : k |-> k+1.

- Show that (∀x:nat, ∃ y:nat, y < x).

pf: D: pick number 0 for x

Y: either fail or

pick a number m for y.

D wins since ~(0 < m).

Hence the statement is not proved.

Game-theoretical proof of non regularity of a set

1. Two players:

   - You (want to show that ~P holds and A is not regular)
   - Demon (the opponent want to show that P holds)

2 The game proceeds as follows:

   1. D picks a $k > 0$ (if A is regular, D's best strategy is to pick k = #states of a FA accepting A)
   2. Y picks x,y,x with $xyz \in A$ and $|y| \geq k$.
   3. D picks u,v,w s.t. $y = uvw$ and $v \neq e$.
   4. Y picks $i \geq 0$

3. Finally Y wins if $xuv^iwz \notin A$ and D wins if $xuv^iwz \in A$.

4. By Theorem 11.2, A is not regular if there is a winning strategy according to which Y always win.

Note: P is a necessary but not a sufficient condition for the regularity of A (i.e., there is nonregular set A satisfying P).

Using the pumping lemma

- Ex1: Show the set $A = \{a^n b^m \mid n \geq m \}$ is not regular.

the proof:

  - 1. D gives k [for any $k > 0$]
  - 2. Y pick $x = a^k$, $y = b^k$, $z = e$ [\$ xyz in A with $|y| \geq k$]
  - ==> $xyz = a^k b^k \in A$
  - 3. D decompose y = uvw with [for all uvw with uvw=y and
  - $|u|=j$, $|v|=m > 0$ and $|w|= n$ $v \neq e$]
  - 4. Y take i = 2. [\$ $i \geq 0$ s.t. $xuv^iwz \notin A$]
  - => $xuv^2wz = a^k b^j b^{2m} b^n = a^k b^{k+m} \notin A$
  - => Y wins. Hence A is not regular.

- Ex2: $C = \{a^{n!} \mid n \geq 0 \}$ is not regular.

pf: similar to Ex1. Left as an exercise.

hint: for any $k > 0$ D chooses, let $xyz = a^{k \times k!} a^{k!} e$ and let i = 0.

Other techniques:

- Using closure property of regular sets.

Ex3: $D = \{ x \in \{a,b\}^* \mid \#a(x) = \#b(x) \}$

$= \{e, ab, ba, aabb, abab. baba, bbaa, abba, baab, \dots \}$

is not regular. (Why ?)

if regular => $D \cap a^*b^* = \{a^nb^n \mid n \geq 0 \} = B$ is regular.

But B is not regular, D thus is not regular.

- [H2E2:] A: any language; if A is regular, then

  $rev(A) =_{def} \{x_nx_{n-1}\dots x_1 \mid x_1x_2\dots x_n \in A\}$ is regular.

- Ex4: $A = \{a^nb^m \mid m \geq n \}$ is not regular.

pf: If A is regular => rev(A) and $h((rev(A)) = \{a^nb^m \mid n \geq m\}$ is regular, where $h(a) = b$ and $h(b) = a$.

=> $A \cap h(rev(A)) = \{a^nb^n \mid n \geq 0\}$ is regular, a contradiction!