6.3
Fooling sets: Proving non-regularity

Fooling Sets

Definition

For a language L over Σ a set of strings F (could be infinite) is a fooling set or distinguishing set for L if every two distinct strings $x, y \in F$ are distinguishable.

Example: $F = \{0^i \mid i \geq 0\}$ is a fooling set for the language $L = \{0^k 1^k \mid k \geq 0\}$.

Theorem

Suppose F is a fooling set for L. If F is finite then there is no DFA M that accepts L with less than $|F|$ states.

Fooling Sets

Definition

For a language L over Σ a set of strings F (could be infinite) is a fooling set or distinguishing set for L if every two distinct strings $x, y \in F$ are distinguishable.

Example: $F = \{0^i \mid i \geq 0\}$ is a fooling set for the language $L = \{0^k 1^k \mid k \geq 0\}$.

Theorem

Suppose F is a fooling set for L. If F is finite then there is no DFA *M that accepts L with less than $|F|$ states.*

Fooling Sets

Definition

For a language L over Σ a set of strings F (could be infinite) is a fooling set or distinguishing set for L if every two distinct strings $x, y \in F$ are distinguishable.

Example: $F = \{0^i \mid i \geq 0\}$ is a fooling set for the language $L = \{0^k 1^k \mid k \geq 0\}$.

Theorem

Suppose F is a fooling set for L. If F is finite then there is no DFA *M that accepts L with less than $|F|$ states.*

Recall

Already proved the following lemma:

Lemma

L: regular language.
$M = (Q, \Sigma, \delta, s, A)$: DFA for L.
If $x, y \in \Sigma^*$ are distinguishable, then $\nabla x \neq \nabla y$.

Reminder: $\nabla x = \delta^*(s, x)$.

Proof of theorem

Theorem (Reworded.)

L: A language
F: a fooling set for L.
If F is finite then any DFA M that accepts L has at least $|F|$ states.

Proof.

Let $F = \{w_1, w_2, \ldots, w_m)$ be the fooling set.
Let $M = (Q, \Sigma, \delta, s, A)$ be any DFA that accepts L.
Let $q_i = \nabla w_i = \delta^*(s, x_i)$.
By lemma $q_i \neq q_j$ for all $i \neq j$.
As such, $|Q| \geq |\{q_1, \ldots, q_m\}| = |\{w_1, \ldots, w_m\}| = |F|$. □

Proof of theorem

Theorem (Reworded.)

L: A language
F: a fooling set for L.
If F is finite then any DFA M that accepts L has at least $|F|$ states.

Proof.

Let $F = \{w_1, w_2, \ldots, w_m)$ be the fooling set.
Let $M = (Q, \Sigma, \delta, s, A)$ be any DFA that accepts L.
Let $q_i = \nabla w_i = \delta^*(s, x_i)$.
By lemma $q_i \neq q_j$ for all $i \neq j$.
As such, $|Q| \geq |\{q_1, \ldots, q_m\}| = |\{w_1, \ldots, w_m\}| = |F|$. □

Proof of theorem

Theorem (Reworded.)

L: A language
F: a fooling set for L.
If F is finite then any DFA M that accepts L has at least $|F|$ states.

Proof.

Let $F = \{w_1, w_2, \ldots, w_m)$ be the fooling set.
Let $M = (Q, \Sigma, \delta, s, A)$ be any DFA that accepts L.
Let $q_i = \nabla w_i = \delta^*(s, x_i)$.
By lemma $q_i \neq q_j$ for all $i \neq j$.
As such, $|Q| \geq |\{q_1, \ldots, q_m\}| = |\{w_1, \ldots, w_m\}| = |F|$. $\square$

Infinite Fooling Sets

Corollary

If L has an infinite fooling set F then L is not regular.

Proof.

Let $w_1, w_2, \ldots \subseteq F$ be an infinite sequence of strings such that every pair of them are distinguishable.
Assume for contradiction that $\exists$ M a DFA for L.
Let $F_i = \{w_1, \ldots, w_i\}$.
By theorem, $\#$ states of $M \geq |F_i| = i$, for all i.
As such, number of states in M is infinite.
Contradiction: DFA = deterministic finite automata. But M not finite. $\square$

Infinite Fooling Sets

Corollary

If L has an infinite fooling set F then L is not regular.

Proof.

Let $w_1, w_2, \ldots \subseteq F$ be an infinite sequence of strings such that every pair of them are distinguishable.
Assume for contradiction that $\exists$ M a DFA for L.
Let $F_i = \{w_1, \ldots, w_i\}$.
By theorem, $\#$ states of $M \geq |F_i| = i$, for all i.
As such, number of states in M is infinite.
Contradiction: DFA = deterministic finite automata. But M not finite. □

Infinite Fooling Sets

Corollary

If L has an infinite fooling set F then L is not regular.

Proof.

Let $w_1, w_2, \ldots \subseteq F$ be an infinite sequence of strings such that every pair of them are distinguishable.
Assume for contradiction that $\exists$ M a DFA for L.
Let $F_i = \{w_1, \ldots, w_i\}$.
By theorem, $\#$ states of $M \geq |F_i| = i$, for all i.
As such, number of states in M is infinite.
Contradiction: DFA = deterministic finite automata. But M not finite. $\square$

Examples

- $\{0^k 1^k \mid k \geq 0\}$
- {bitstrings with equal number of 0s and 1s}
- $\{0^k 1^\ell \mid k \neq \ell\}$

Examples

- $\{0^k 1^k \mid k \geq 0\}$
- $\{$bitstrings with equal number of 0s and 1s$\}$
- $\{0^k 1^\ell \mid k \neq \ell\}$

Examples

- $\{0^k 1^k \mid k \geq 0\}$
- $\{$bitstrings with equal number of 0s and 1s$\}$
- $\{0^k 1^\ell \mid k \neq \ell\}$

Harder example: The language of squares is not regular

$\{0^{k^2} \mid k \geq 0\}$

Really hard: Primes are not regular

An exercise left for your enjoyment

$\{0^k \mid k \text{ is a prime number}\}$

Hints:

1. Probably easier to prove directly on the automata.
2. There are infinite number of prime numbers.
3. For every $n > 0$, observe that $n!, n! + 1, \ldots, n! + n$ are all composite – there are arbitrarily big gaps between prime numbers.

THE END

...

(for now)