6.045

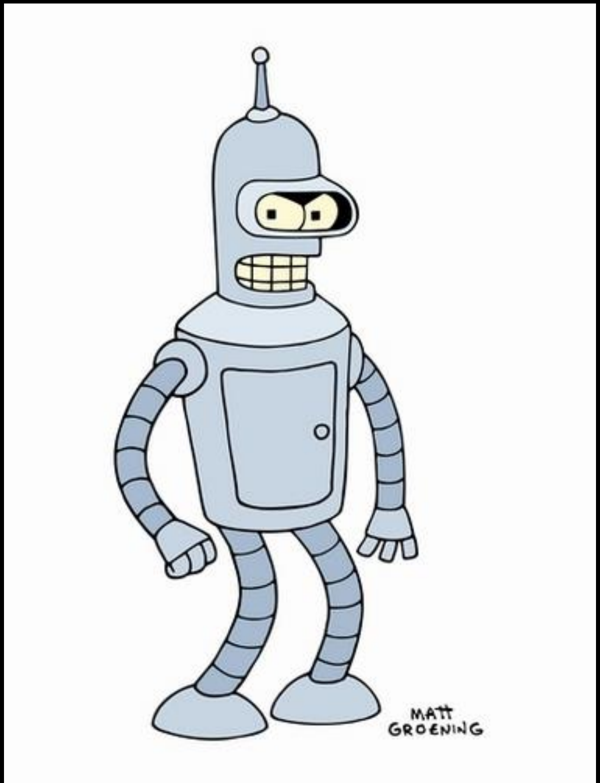
Lecture 4:
More on Regexps,
Non-Regular Languages

6.045

Announcements:

- Pset 1 is on piazza (as of last night)
- No class next Tuesday
- Come to office hours?

Deterministic Finite Automata



Computation with finite memory

Non-**D**eterministic **F**inite **A**utomata

Computation with finite memory

and magical guessing

Regular Languages are closed under all of the following operations:

Union: $A \cup B = \{ w \mid w \in A \text{ or } w \in B \}$

Intersection: $A \cap B = \{ w \mid w \in A \text{ and } w \in B \}$

Complement: $\neg A = \{ w \in \Sigma^* \mid w \notin A \}$

Reverse: $A^R = \{ w_1 \ldots w_k \mid w_k \ldots w_1 \in A, w_i \in \Sigma\}$

Concatenation: $A \cdot B = \{ vw \mid v \in A \text{ and } w \in B \}$

Star: $A^* = \{ s_1 \ldots s_k \mid k \geq 0 \text{ and each } s_i \in A \}$

Regular Expressions: Computation as Description

A different way of thinking about computation:

What is the complexity of describing the strings in the language?

DFAs find "patterns" in strings; how to describe them?

Syntax

Inductive Definition of Regexp

Let Σ be an alphabet. We define the regular expressions over Σ inductively:

For all $\sigma \in \Sigma$, σ is a regexp

ε is a regexp

$\varnothing$ is a regexp

If R_1 and R_2 are both regexps, then

(R_1R_2), $(R_1 + R_2)$, and $(R_1)^*$ are regexps

Examples: ε, 0, $(1)^*$, $(0+1)^*$, $((((0)^*1)^*1) + (10))$

Semantics

Definition: Regexps Represent Languages

The regexp $\sigma \in \Sigma$ *represents* the language $\{\sigma\}$

The regexp ε represents $\{\varepsilon\}$

The regexp $\varnothing$ represents $\varnothing$

If R_1 and R_2 are regular expressions representing L_1 and L_2 then:

(R_1R_2) represents $L_1 \cdot L_2$

$(R_1 + R_2)$ represents $L_1 \cup L_2$

$(R_1)^*$ represents L_1^*

Example: $(10 + 0^*1)$ represents $\{10\} \cup \{0^k1 \mid k \geq 0\}$

Regexps Represent Languages

For every regexp R,
define L(R) to be the language that R represents

A string $w \in \Sigma^*$ is *accepted by R*
(or, w matches R) if $w \in L(R)$

Examples: 0, 010, and 01010 match (01)*0

11010111010110 0 matches (0+1)*0

L((0+1)*0) = {w in {0,1}* | w ends in a 0}

DFAs $\equiv$ NFAs $\equiv$ Regular Expressions!

L can be represented by some regexp
$\Leftrightarrow$ L is regular

We saw: L can be represented by some regexp
$\Rightarrow$ L is regular

Every regexp can be converted into an NFA

Now we'll show: L is regular
$\Rightarrow$ L can be represented by some regexp

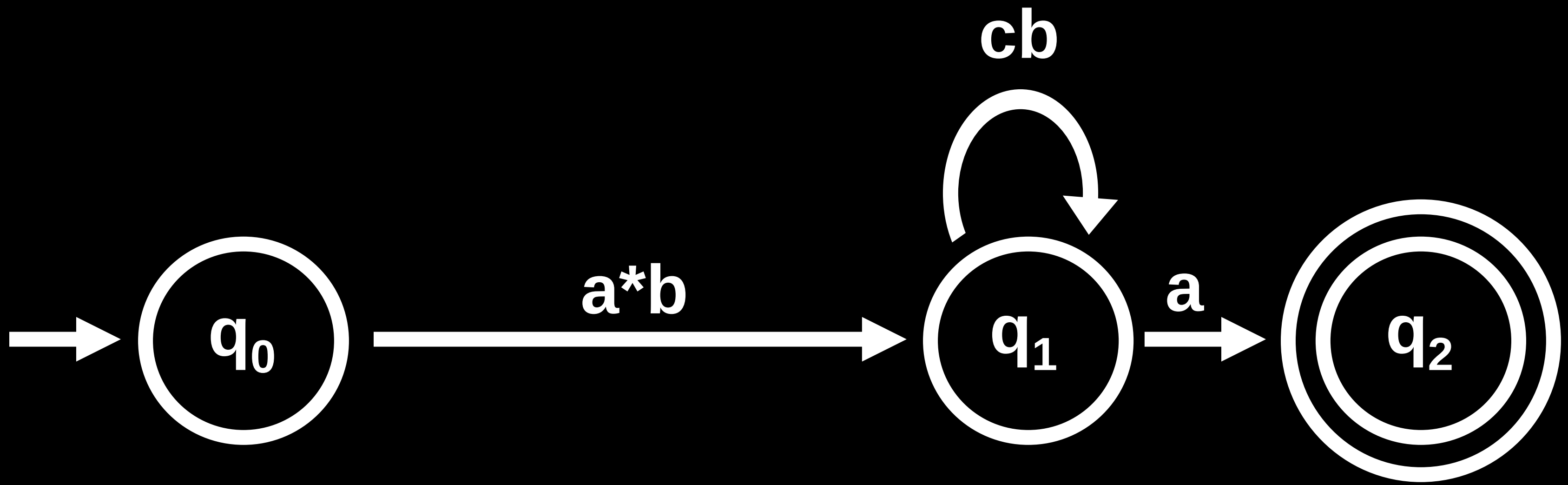
Every DFA can be converted into a regexp

Generalized NFAs (GNFA)

Idea: Transform an DFA for L into a regular expression by ***removing states*** and re-labeling the arcs connected to those states with ***regular expressions***

Rather than reading in just 0 or 1 letters from the string on an arc, we can read in *entire substrings*

Generalized NFA (GNFA)



Accept string x ⇔ there is *some path* of regexps $R_1, \ldots, R_k$ from start state to final such that x matches $R_1 \cdots R_k$

This GNFA recognizes L(a*b(cb)*a), the set of strings matched by a*b(cb)*a

Add unique start and accept states

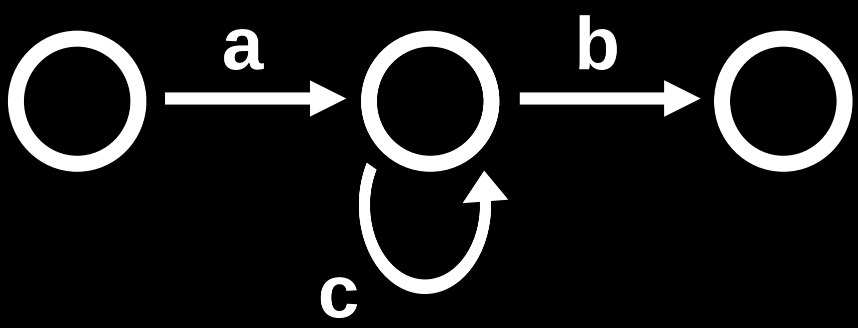
Goal: Replace 

with a single regexp R

Then, L(R) = L(DFA)

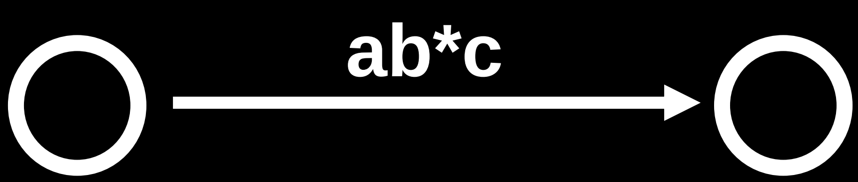
While the machine has more than 2 states:

Pick an internal state, rip it out and
re-label the arrows with regexps,
to account for paths through the missing state



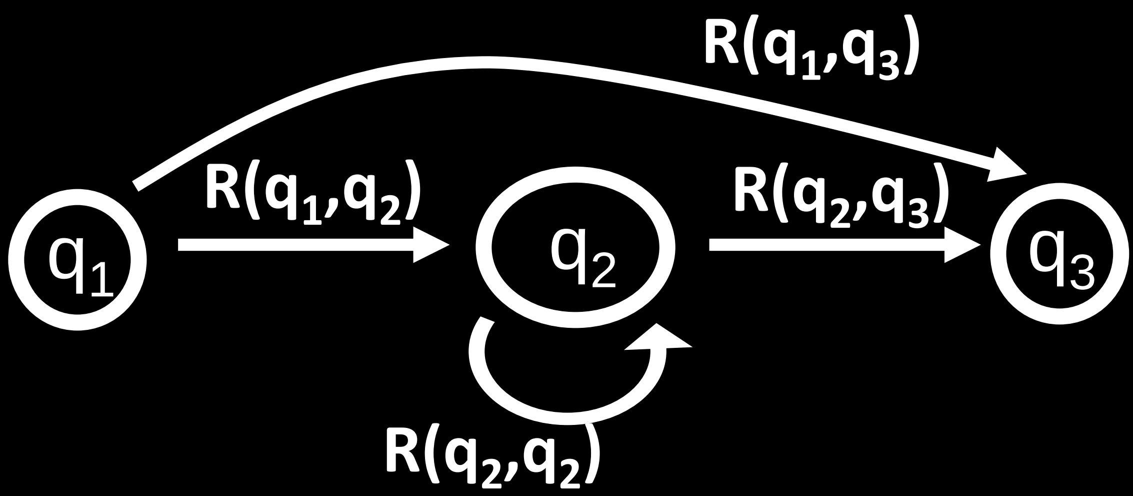
While the machine has more than 2 states:

Pick an internal state, rip it out and
re-label the arrows with regexps,
to account for paths through the missing state



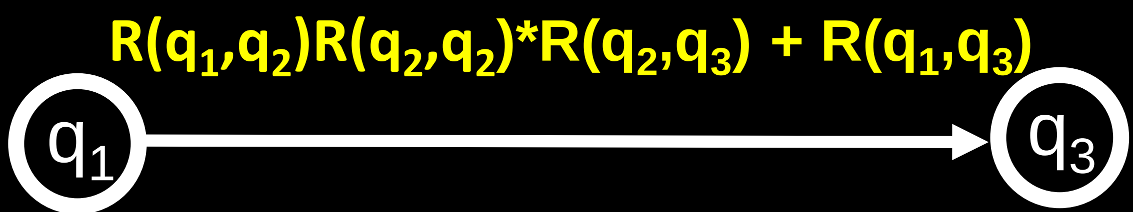
While the machine has more than 2 states:

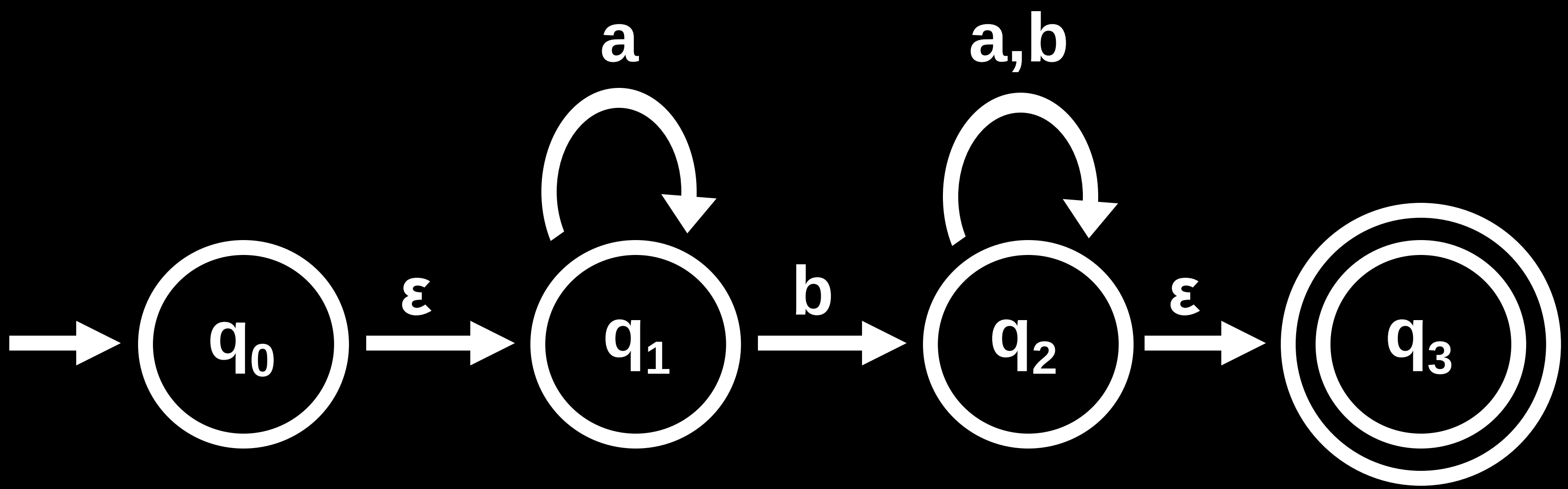
In general:



While the machine has more than 2 states:

In general:





$R(q_0,q_3) = (a^*b)(a+b)^*$

represents L(N)

Formally: Given a DFA M, add q_{start} and q_{acc} to create G

For all q, q', define $R(q,q') = \sigma_1 + \cdots + \sigma_k$ s.t. $\delta(q,\sigma_i) = q'$

CONVERT(G): *(Takes a GNFA, outputs a regexp)*

If #states = 2 return $R(q_{start}, q_{acc})$

If #states > 2

pick $q_{rip} \in Q$ different from q_{start} and q_{acc}

define $Q' = Q - \{q_{rip}\}$

define R' on $Q'-\{q_{acc}\} \times Q'-\{q_{start}\}$ as:

$$R'(q_i,q_j) = R(q_i,q_{rip})R(q_{rip},q_{rip})^*R(q_{rip},q_j) + R(q_i,q_j)$$

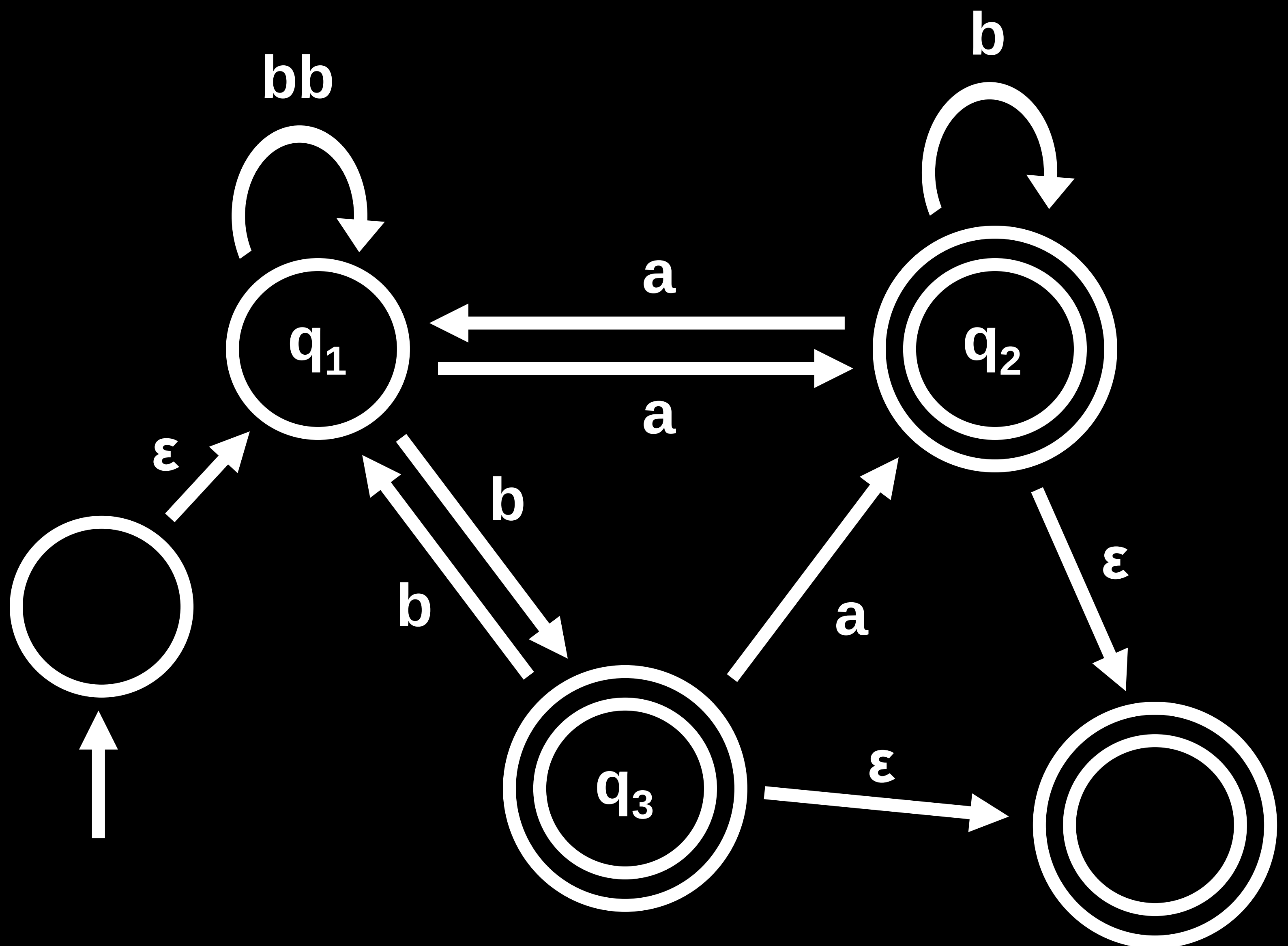
return CONVERT(G')

defines a new GNFA G'

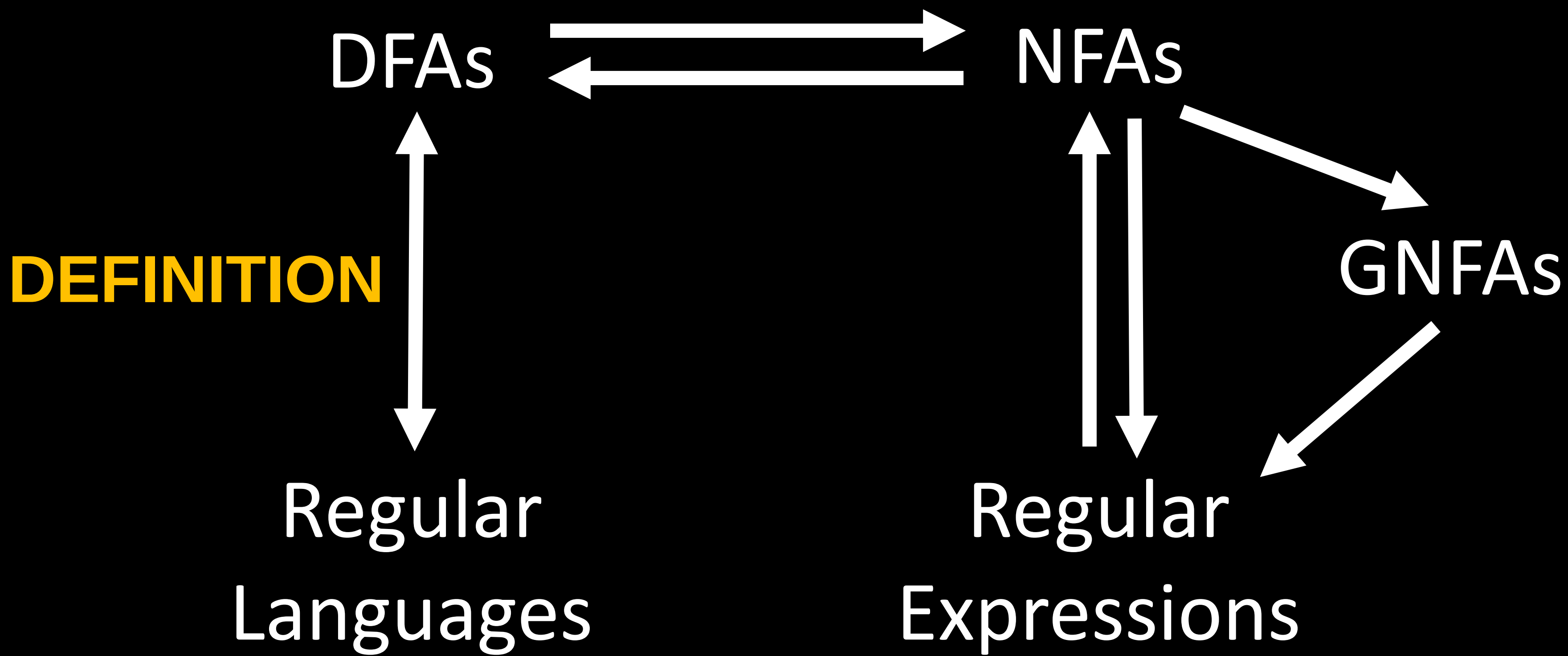
Theorem: Let R = CONVERT(G). Then L(R) = L(M).

Claim: L(G') = L(G)

[Sipser, p.73-74]



Convert to a regular expression


DFAs
NFAs
GNFAs
DEFINITION
Regular Languages
Regular Expressions

Many Languages Are Not Regular:

Limitations on DFAs/NFAs
a.k.a.
“Lower Bounds” on DFAs/NFAs

$\Sigma = \{0,1\}$

Regular or Not?

C = { w | w has equal number of 1s and 0s}

D = { w | w has equal number of occurrences of 01 and 10}

A Language With No DFA

Theorem: $A = \{0^n1^n \mid n \geq 0\}$ is not regular

Big Idea:

No DFA can "remember" the number of 0's, if it reads more 0's than its number of states.

In that case, the DFA can't accurately compare the number of 0's to the number of 1s!

A Language With No DFA

Theorem: A = $\{0^n1^n \mid n \geq 0\}$ is not regular

Proof: By contradiction. Assume A *is* regular.
Then A has a DFA M with Q states, for some Q > 0.

Suppose we run M on the input $w = 0^{Q+1}$.

By the pigeonhole principle, *some state q of M is visited more than once while reading in w.*

Therefore, M is in state q after reading 0^S,
and M is in state q after reading 0^R, for some $R < S \leq Q+1$.

What happens when M reads 1^S starting from state q?

M must accept, because $0^S\,1^S$ in A.

AND M must reject, because $0^R\,1^S$ is not in A.

Contradiction!

Counting: Hard With Finite Brain

Thm: EQ = {w | w has an equal number of 0s and 1s}
is not regular

Proof: By contradiction. Assume EQ *is* regular.

Observation: $EQ \cap L(0^*1^*) = \{0^n1^n \mid n \geq 0\}$

If EQ is regular and $L(0^*1^*)$ is regular
then $EQ \cap L(0^*1^*)$ is regular.
(Regular Languages are closed under intersection!)

But $\{0^n1^n \mid n \geq 0\}$ is not regular!

Contradiction!

Palindromes: Hard With Finite Brain

Theorem: PAL = $\{w \mid w = w^R\}$ is not regular

Proof: By contradiction. Assume PAL *is* regular.
Then PAL has a DFA M with Q states, for some $Q > 0$.

Run M on the input $w = 10^{Q+1}$

By the pigeonhole principle, *some state q of M is visited more than once, while reading in the 0's of w.*

Therefore, M is in state q after reading 10^S,
and is also in q after reading 10^R, for some $R < S \leq Q+1$.

What happens when M reads 10^S1 starting from state q?

M must accept, because 10^S10^S1 is in PAL.

Contradiction!

AND M must reject, because 10^R10^S1 is not…

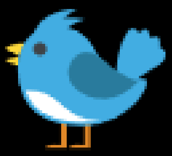
How to Make a DFA Lose Its Mind

Want to show: Language L is not regular

Proof: By contradiction. Assume L *is* regular.
So L has a DFA M with Q states, for some Q > 0.

YOU: Cleverly pick strings x, y where |y| > Q

Run M on xy. *Pigeons tell us: Some state q of M is visited more than once, while reading in y.*

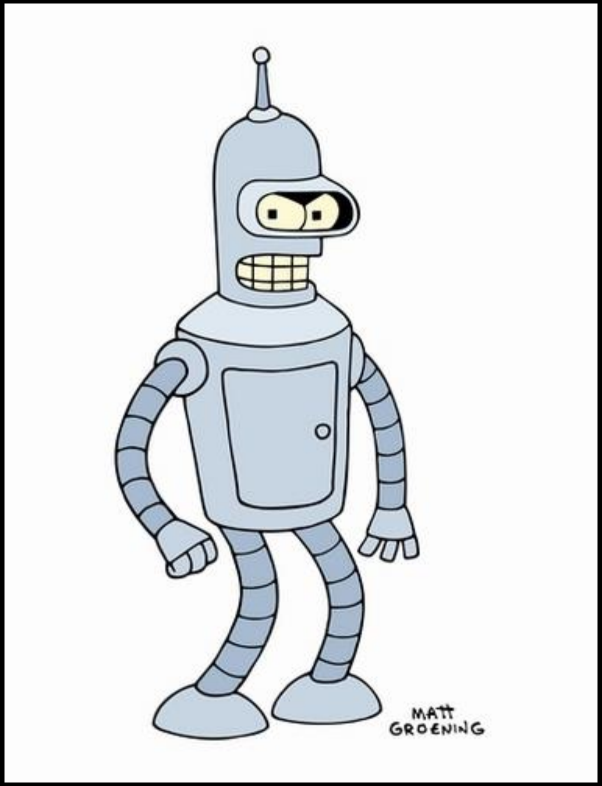


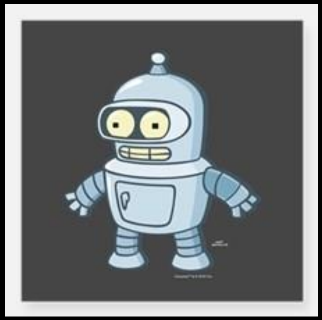
Therefore, M is in state q after reading xy’, and is in q after reading xy’’, for distinct prefixes y’ and y’’ of y

YOU: Cleverly pick string z so that *exactly one* of xy’z and xy’’z is in L

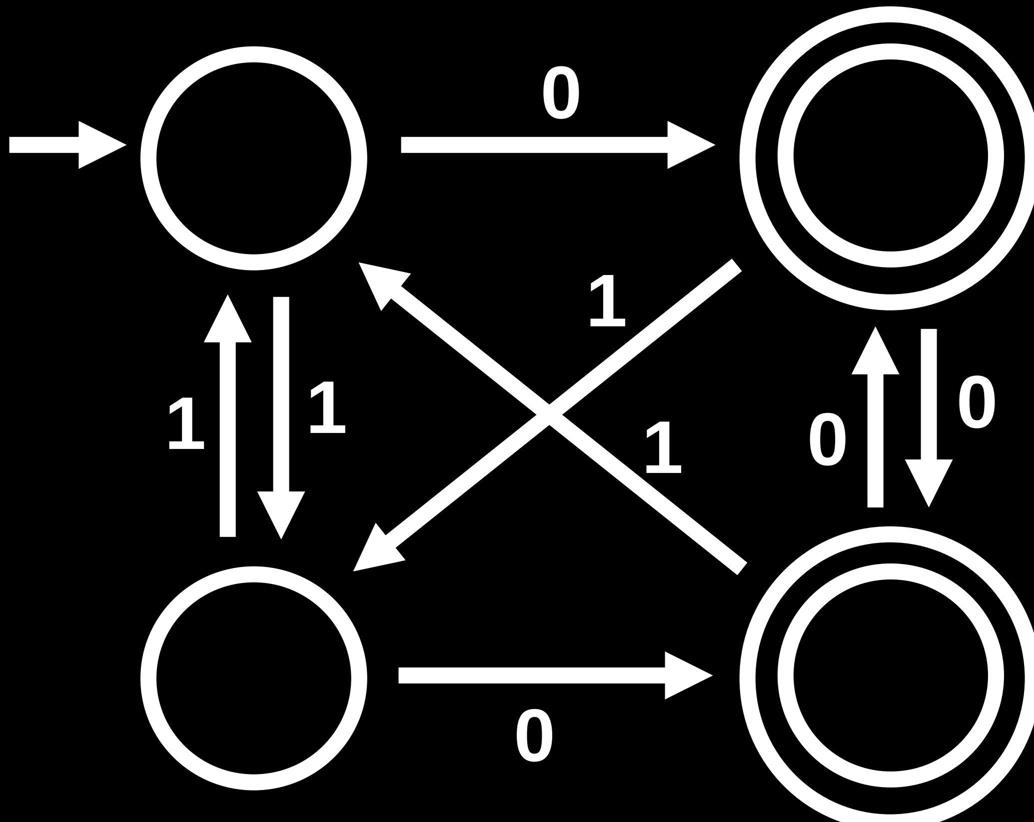
But M will give the same output on both! ***Contradiction!***

Minimizing DFAs

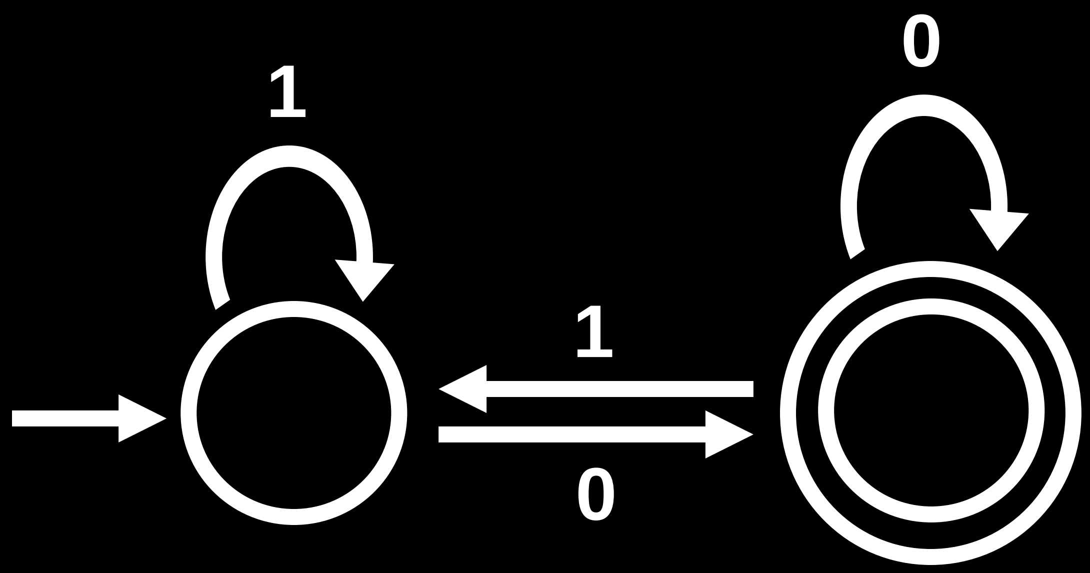




Does this DFA have a minimal number of states?



Is this minimal?



How can we tell in general?

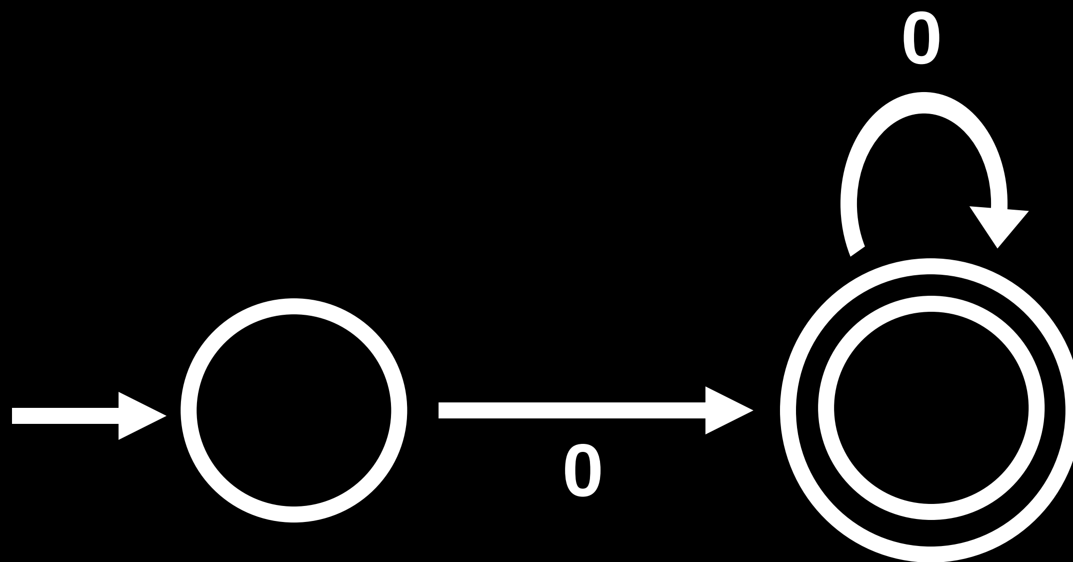
DFA Minimization Theorem:

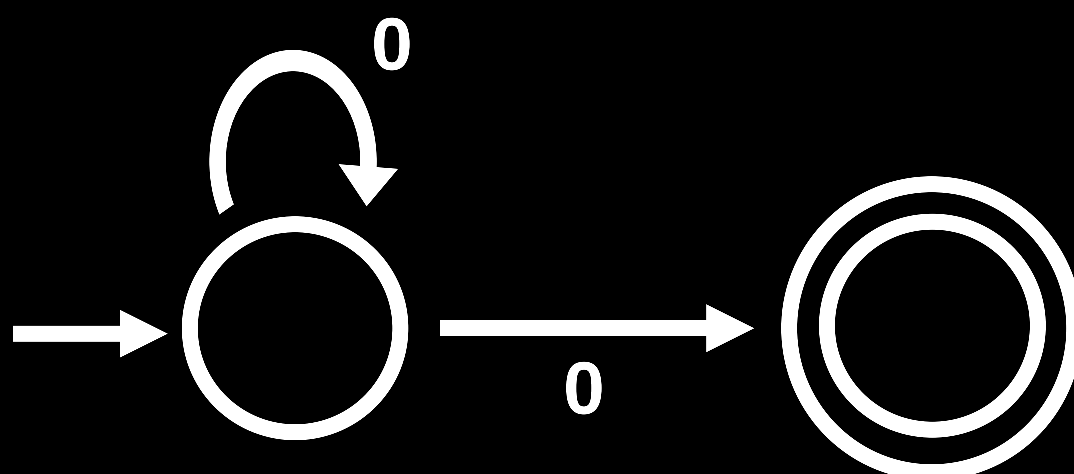
For every regular language A, there is a unique (up to re-labeling of the states) minimal-state DFA M* such that A = L(M*).

Furthermore, there is an *efficient algorithm* which, given any DFA M, will output this unique M*.

If such algorithms existed for more general models of computation, that would be an engineering breakthrough!!

In general, there isn't a uniquely minimal NFA

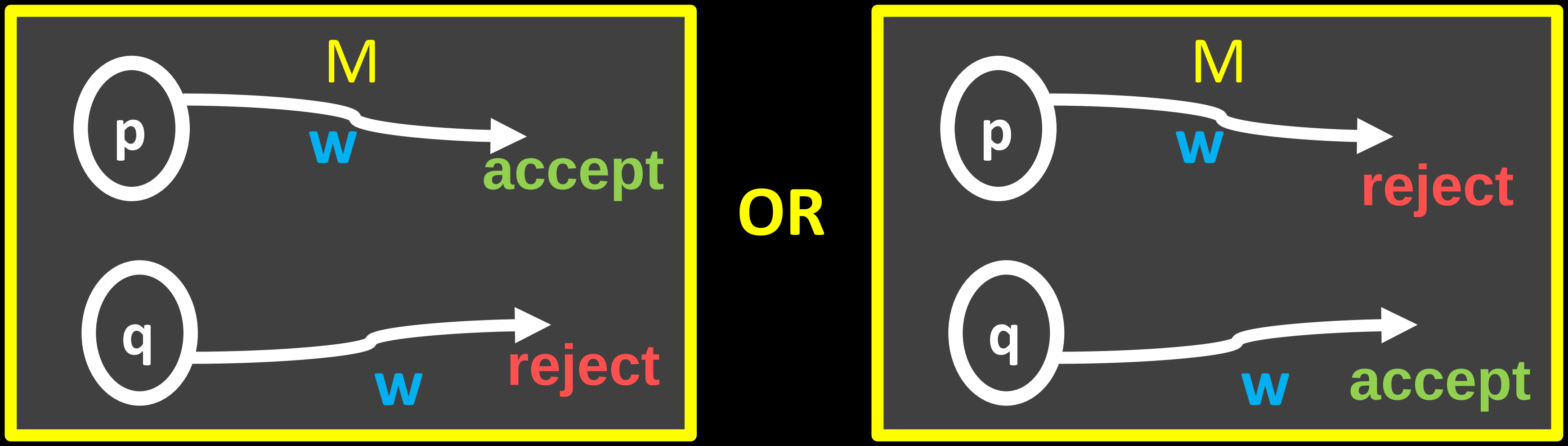




Distinguishing states with strings

For a DFA $M = (Q, \Sigma, \delta, q_0, F)$, and $q \in Q$,
let M_q be the DFA equal to $(Q, \Sigma, \delta, q, F)$

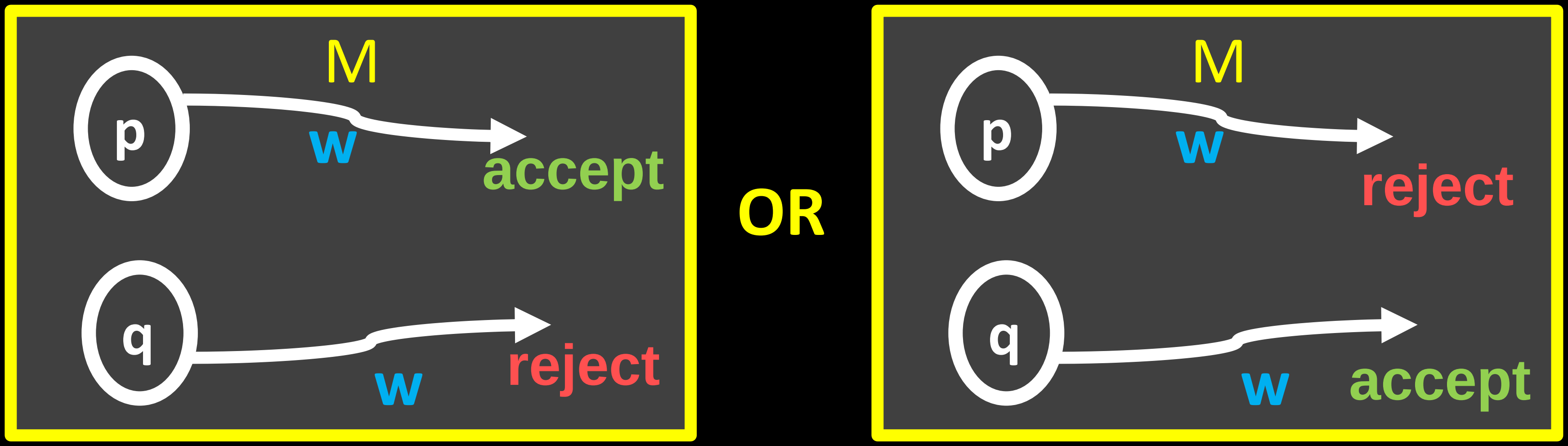
Def. $w \in \Sigma^*$ *distinguishes* states p and q if:
M_p accepts $w \Leftrightarrow M_q$ rejects w



Distinguishing states with strings

For a DFA $M = (Q, \Sigma, \delta, q_0, F)$, and $q \in Q$,
let M_q be the DFA equal to $(Q, \Sigma, \delta, q, F)$

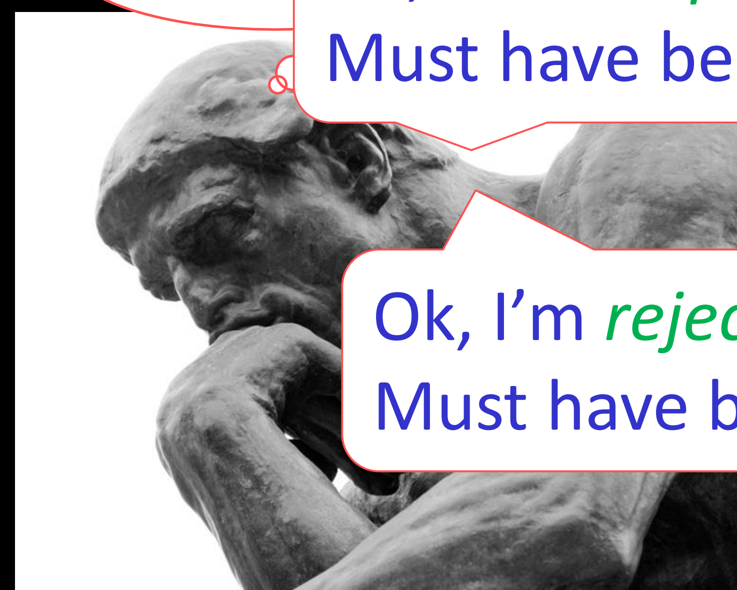
Def. $w \in \Sigma^*$ ***distinguishes*** states p and q if:
M_p and M_q have *different outputs* on input w



Distinguishing two states

Def. w ∈ Σ* *distinguishes* states p and q iff

M_p and M_q have *different outputs* on w



Fix $M = (Q, \Sigma, \delta, q_0, F)$ and let $p, q \in Q$

Let $M_p = (Q, \Sigma, \delta, p, F)$ and $M_q = (Q, \Sigma, \delta, q, F)$

Definition(s):

State p is *distinguishable* from state q

iff there is a $w \in \Sigma^*$ that distinguishes p and q

iff there is a $w \in \Sigma^*$ so that

M_p accepts w $\Leftrightarrow$ M_q rejects w

State p is *indistinguishable* from state q

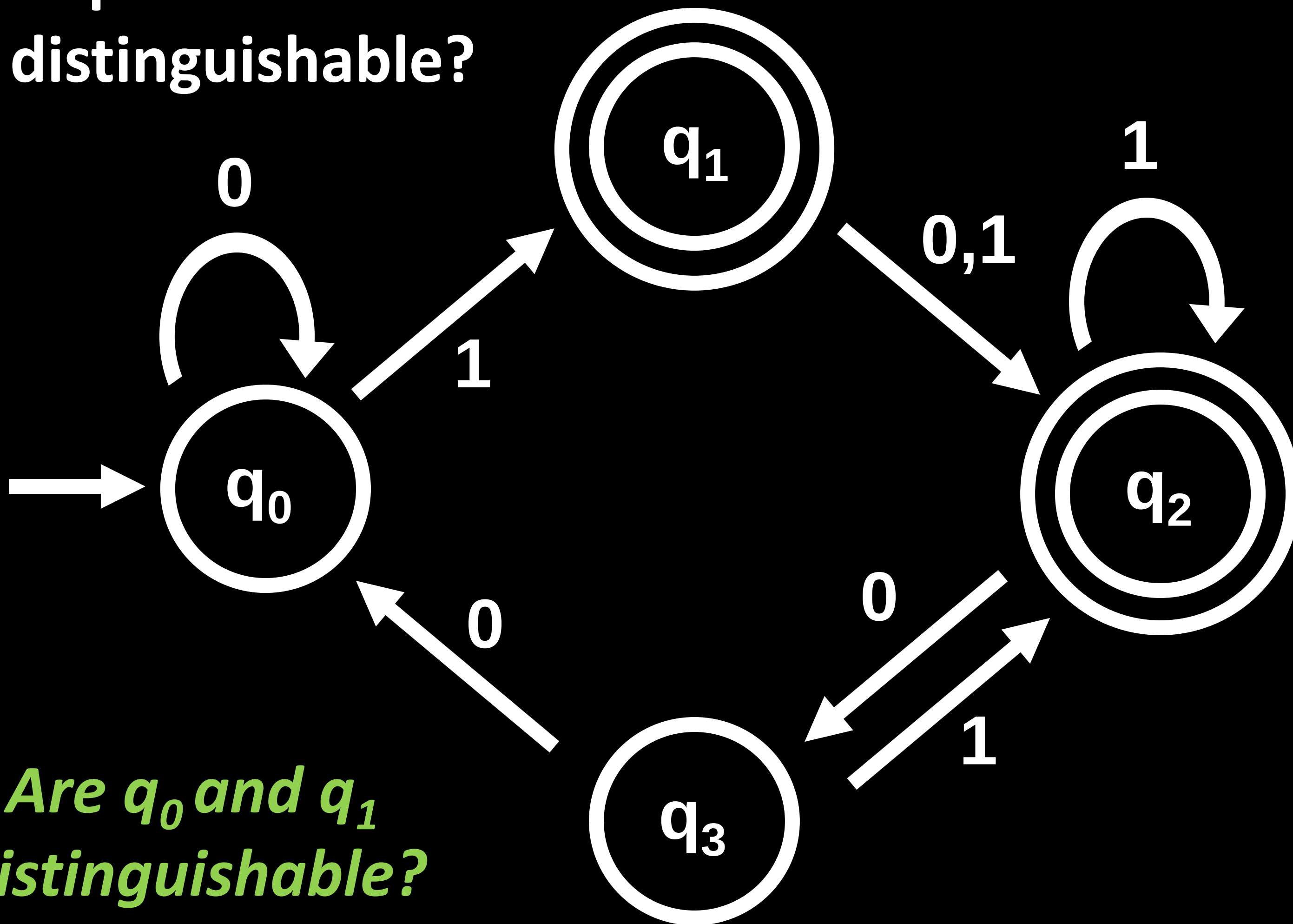
iff p is not distinguishable from q

iff for all $w \in \Sigma^*$, M_p accepts w $\Leftrightarrow$ M_q accepts w

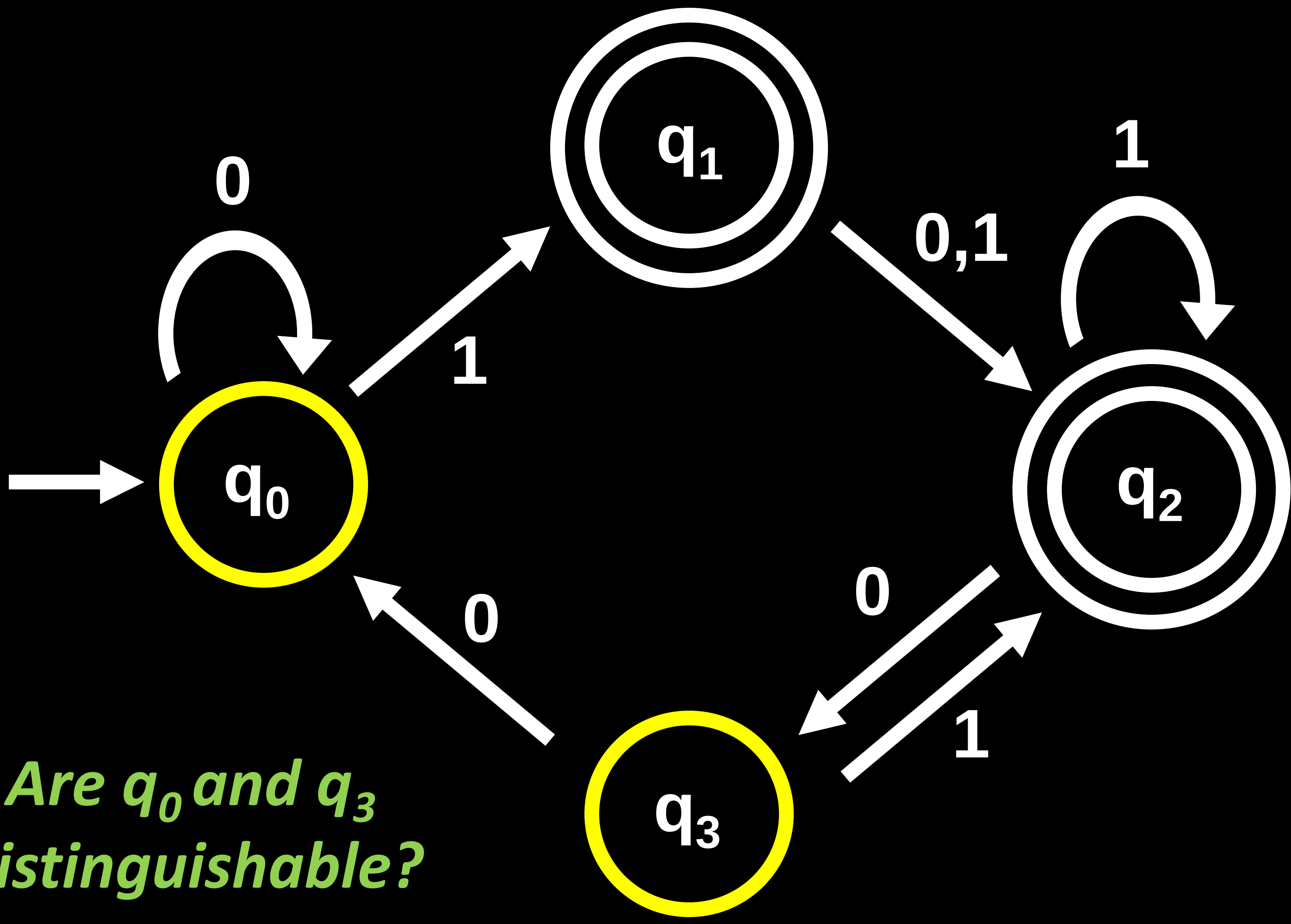
Big Idea: Pairs of indistinguishable states are redundant!

From p or q, M has exactly the same output behavior

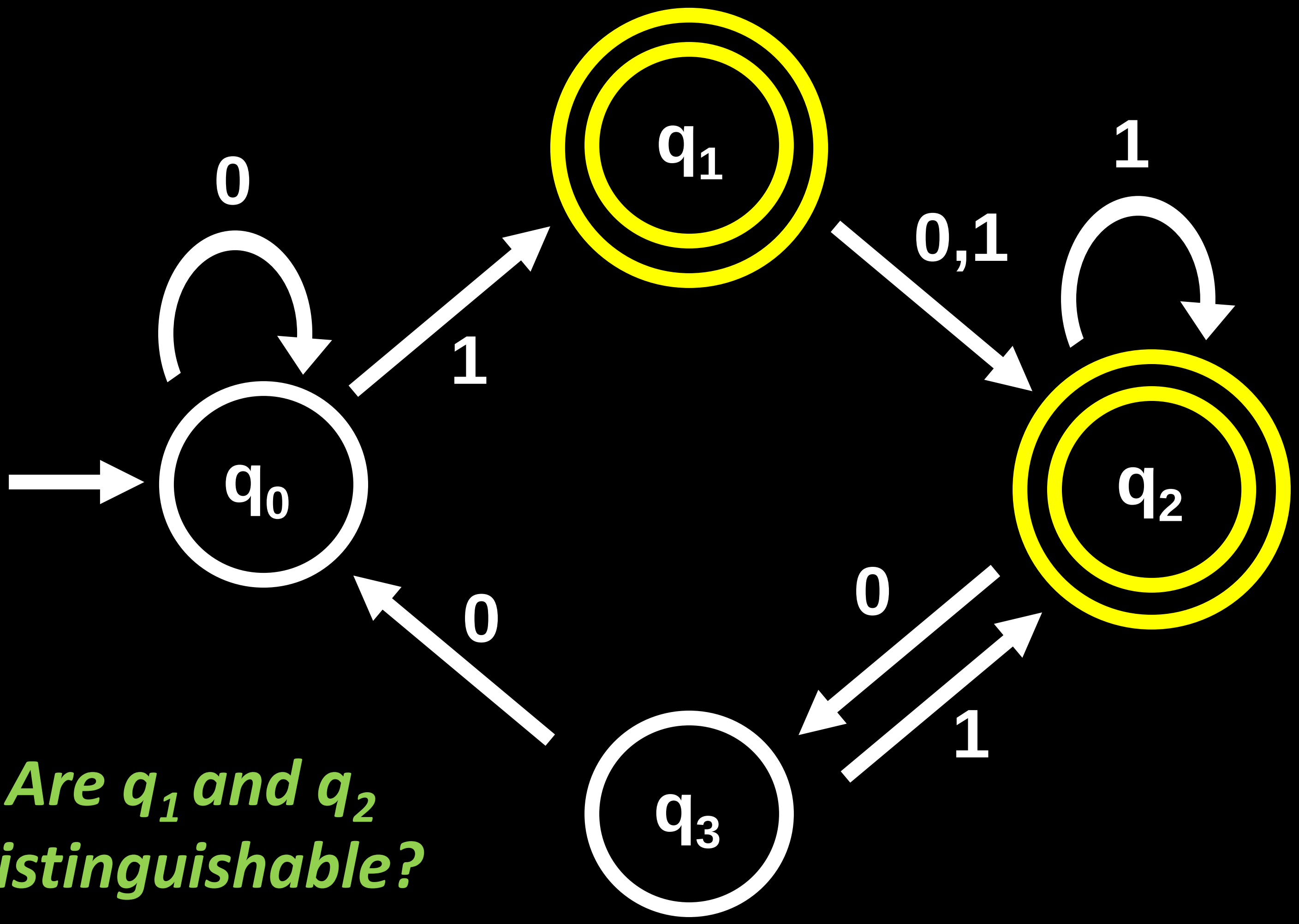
Which pairs of states are distinguishable?



Are q_0 and q_1 distinguishable?



Are q_0 and q_3 distinguishable?



Are q_1 and q_2 distinguishable?

Fix $M = (Q, \Sigma, \delta, q_0, F)$ and let $p, q, r \in Q$

Define a binary relation $\sim$ on the states of M:

$p \sim q$ iff p is indistinguishable from q

$p \nsim q$ iff p is distinguishable from q

Proposition: $\sim$ is an equivalence relation

$p \sim p$ (reflexive)

$p \sim q \Rightarrow q \sim p$ (symmetric)

$p \sim q$ and $q \sim r \Rightarrow p \sim r$ (transitive)

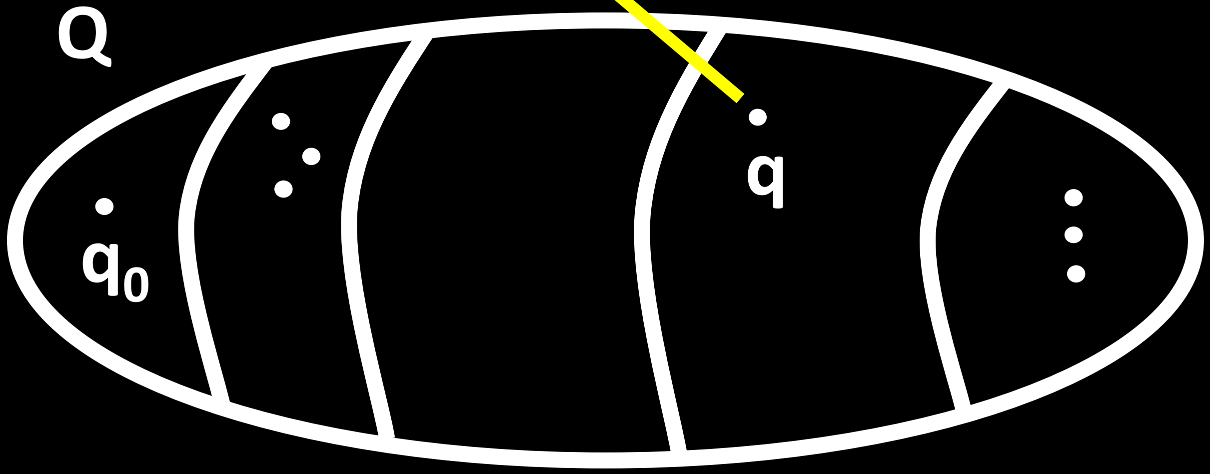
Proof? Just look at the definition! $p \sim q$ means for all w, M_p accepts w $\Leftrightarrow$ M_q accepts w

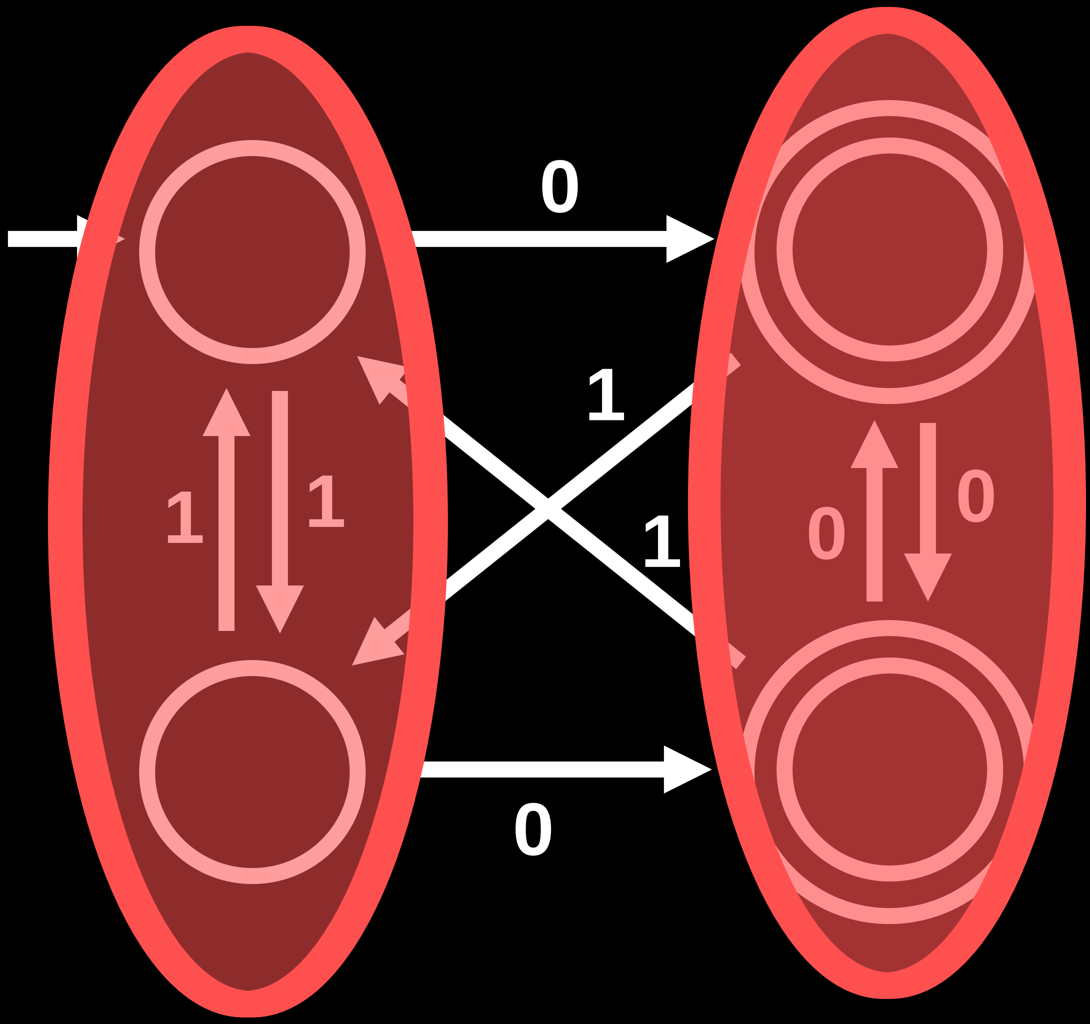
Fix $M = (Q, \Sigma, \delta, q_0, F)$ and let $p, q, r \in Q$

Therefore, the relation $\sim$ partitions Q into disjoint equivalence classes

Proposition: $\sim$ is an equivalence relation

$[q] := \{ p \mid p \sim q \}$




0
1
1
1
1
0
0
0

Algorithm: MINIMIZE-DFA

Input: DFA M

Output: DFA M_{MIN} such that:

1. $L(M) = L(M_{MIN})$

not reachable from start

=

2. M_{MIN} has no *inaccessible* states

3. M_{MIN} is *irreducible*

=

for all states $p \neq q$ of M_{MIN}, p and q are distinguishable

Theorem: Every M_{MIN} satisfying 1,2,3 is the unique minimal DFA equivalent to M

Intuition:

States of M_{MIN} = *Equivalence classes* of states of M

We'll uncover these equivalent states with a *dynamic programming* algorithm