Number of States for DFAs and NFAs

Goal

Goal

Compare the sizes of smallest DFA and NFA for some language. (Size is number of states.)

First Language We Consider

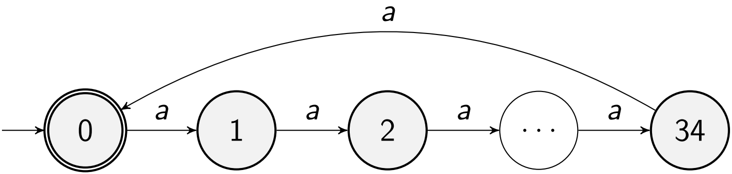
$$L_1 = \{a^i : i \equiv 0 \pmod{35}\}$$

First Language We Consider

$$L_1 = \{a^i : i \equiv 0 \pmod{35}\}$$

Next slide has DFA for it.

$L_1 = \{a^i : i \equiv 0 \pmod{35}\}$



DFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

DFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Is there a smaller DFA for L_1?

DFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Is there a smaller DFA for L_1?

VOTE

DFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Is there a smaller DFA for L_1?

VOTE

1. Bill knows a DFA for L_1 with ≤ 34 states.

DFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Is there a smaller DFA for L_1?

VOTE

1. Bill knows a DFA for L_1 with ≤ 34 states.
2. Bill can prove all DFA's for L_1 have ≥ 35 states.

DFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Is there a smaller DFA for L_1?

VOTE

1. Bill knows a DFA for L_1 with ≤ 34 states.
2. Bill can prove all DFA's for L_1 have ≥ 35 states.
3. The answer is UNKNOWN TO BILL!

DFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Is there a smaller DFA for L_1?

VOTE

1. Bill knows a DFA for L_1 with ≤ 34 states.
2. Bill can prove all DFA's for L_1 have ≥ 35 states.
3. The answer is UNKNOWN TO BILL!

Bill can prove all DFA's for L_1 have ≥ 35 states.

DFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem Any DFA for L_1 has at least 35 states.

DFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem Any DFA for L_1 has at least 35 states.
Proof: Assume BWOC ($\exists$DFA M), $\le$ 34 states, for L_1.

DFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem Any DFA for L_1 has at least 35 states.
Proof: Assume BWOC ($\exists \mathrm{DFA}\ M$), ≤ 34 states, for L_1.

Feed in the string a^{35}.

DFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem Any DFA for L_1 has at least 35 states.
Proof: Assume BWOC ($\exists$DFA M), ≤ 34 states, for L_1.

Feed in the string a^{35}.

States visited: $s = q_0, q_1, \ldots, q_{35} \in F$
(Note that a word of length L visits $L + 1$ states.)

DFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem Any DFA for L_1 has at least 35 states.
Proof: Assume BWOC ($\exists$DFA M), ≤ 34 states, for L_1.

Feed in the string a^{35}.

States visited: $s = q_0, q_1, \ldots, q_{35} \in F$
(Note that a word of length L visits $L+1$ states.)

We just look at $q_0, \ldots, q_{34}$ which is 35 (not necc different) states.
Since the DFA has ≤ 34 states
$(\exists 0 \le i < j \le 34)$ such that $q_i = q_j$. Say $i = 3$ and $j = 5$.

DFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem Any DFA for L_1 has at least 35 states.
Proof: Assume BWOC ($\exists \mathrm{DFA}\ M$), ≤ 34 states, for L_1.

Feed in the string a^{35}.

States visited: $s = q_0, q_1, \ldots, q_{35} \in F$
(Note that a word of length L visits $L + 1$ states.)

We just look at $q_0, \ldots, q_{34}$ which is 35 (not necc different) states.
Since the DFA has ≤ 34 states
$(\exists 0 \leq i < j \leq 34)$ such that $q_i = q_j$. Say $i = 3$ and $j = 5$.

Feed in the string a^{33}.

DFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem Any DFA for L_1 has at least 35 states.
Proof: Assume BWOC $(\exists \mathrm{DFA}\ M)$, ≤ 34 states, for L_1.

Feed in the string a^{35}.

States visited: $s = q_0, q_1, \ldots, q_{35} \in F$
(Note that a word of length L visits $L+1$ states.)

We just look at $q_0, \ldots, q_{34}$ which is 35 (not necc different) states.
Since the DFA has ≤ 34 states
$(\exists 0 \le i < j \le 34)$ such that $q_i = q_j$. Say $i = 3$ and $j = 5$.

Feed in the string a^{33}.

States visited: $s = q_0, q_1, q_2, q_3 = q_5, q_6, q_7, \ldots, q_{35} \in F$.

DFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem Any DFA for L_1 has at least 35 states.
Proof: Assume BWOC ($\exists$DFA M), ≤ 34 states, for L_1.

Feed in the string a^{35}.

States visited: $s = q_0, q_1, \ldots, q_{35} \in F$
(Note that a word of length L visits $L+1$ states.)

We just look at $q_0, \ldots, q_{34}$ which is 35 (not necc different) states.
Since the DFA has ≤ 34 states
$(\exists 0 \le i < j \le 34)$ such that $q_i = q_j$. Say $i = 3$ and $j = 5$.

Feed in the string a^{33}.

States visited: $s = q_0, q_1, q_2, q_3 = q_5, q_6, q_7, \ldots, q_{35} \in F$.

Hence a^{33} is accepted. This is the contradiction.

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

$\exists$ DFA for L_1: 35 states, hence $\exists$ NFA for L_1: 35 states.

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

$\exists$ DFA for L_1: 35 states, hence $\exists$ NFA for L_1: 35 states.

Is there a smaller NFA for L_1?

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

$\exists$ DFA for L_1: 35 states, hence $\exists$ NFA for L_1: 35 states.

Is there a smaller NFA for L_1?

VOTE

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

$\exists$ DFA for L_1: 35 states, hence $\exists$ NFA for L_1: 35 states.

Is there a smaller NFA for L_1?

VOTE

1. Bill knows an NFA for L_1 with ≤ 34 states.

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

$\exists$ DFA for L_1: 35 states, hence $\exists$ NFA for L_1: 35 states.

Is there a smaller NFA for L_1?

VOTE

1. Bill knows an NFA for L_1 with ≤ 34 states.
2. Bill can prove all NFA's for L_1 have ≥ 35 states.

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

$\exists$ DFA for L_1: 35 states, hence $\exists$ NFA for L_1: 35 states.

Is there a smaller NFA for L_1?

VOTE

1. Bill knows an NFA for L_1 with ≤ 34 states.
2. Bill can prove all NFA's for L_1 have ≥ 35 states.
3. The answer is UNKNOWN TO BILL!

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

$\exists$ DFA for L_1: 35 states, hence $\exists$ NFA for L_1: 35 states.

Is there a smaller NFA for L_1?

VOTE

1. Bill knows an NFA for L_1 with ≤ 34 states.
2. Bill can prove all NFA's for L_1 have ≥ 35 states.
3. The answer is UNKNOWN TO BILL!

Bill can prove all NFA's for L_1 have ≥ 35 states.

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

$\exists$ DFA for L_1: 35 states, hence $\exists$ NFA for L_1: 35 states.

Is there a smaller NFA for L_1?

VOTE

1. Bill knows an NFA for L_1 with ≤ 34 states.
2. Bill can prove all NFA's for L_1 have ≥ 35 states.
3. The answer is UNKNOWN TO BILL!

Bill can prove all NFA's for L_1 have ≥ 35 states.
Its on the next slide.

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

$\exists$ DFA for L_1: 35 states, hence $\exists$ NFA for L_1: 35 states.

Is there a smaller NFA for L_1?

VOTE

1. Bill knows an NFA for L_1 with ≤ 34 states.
2. Bill can prove all NFA's for L_1 have ≥ 35 states.
3. The answer is UNKNOWN TO BILL!

Bill can prove all NFA's for L_1 have ≥ 35 states.
Its on the next slide. Its similar to the DFA proof.

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem any NFA for L_1 has at least 35 states.

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem any NFA for L_1 has at least 35 states.
Proof: Assume BWOC ($\exists$NFA M), $\leq$ 34 states, for L_1.

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem any NFA for L_1 has at least 35 states.
Proof: Assume BWOC ($\exists$NFA M), ≤ 34 states, for L_1.
Feed in the string a^{35}. **Some Path Accepts.**

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem any NFA for L_1 has at least 35 states.
Proof: Assume BWOC ($\exists$NFA M), ≤ 34 states, for L_1.
Feed in the string a^{35}. **Some Path Accepts.**

Let the states visited on that path be: $s = q_0, q_1, \ldots, q_{35} \in F$

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem any NFA for L_1 has at least 35 states.
Proof: Assume BWOC ($\exists$NFA M), ≤ 34 states, for L_1.
Feed in the string a^{35}. **Some Path Accepts.**

Let the states visited on that path be: $s = q_0, q_1, \ldots, q_{35} \in F$
We look at $q_0, \ldots, q_{34}$.

$\exists 0 \leq i < j \leq 34$ such that $q_i = q_j$. Say $i = 3$ and $j = 5$.

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem any NFA for L_1 has at least 35 states.
Proof: Assume BWOC ($\exists$NFA M), ≤ 34 states, for L_1.
Feed in the string a^{35}. **Some Path Accepts.**

Let the states visited on that path be: $s = q_0, q_1, \ldots, q_{35} \in F$
We look at $q_0, \ldots, q_{34}$.

$\exists 0 \leq i < j \leq 34$ such that $q_i = q_j$. Say $i = 3$ and $j = 5$.

Feed in the string a^{33}. **There is a Path:**

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem any NFA for L_1 has at least 35 states.
Proof: Assume BWOC ($\exists$NFA M), ≤ 34 states, for L_1.
Feed in the string a^{35}. **Some Path Accepts.**

Let the states visited on that path be: $s = q_0, q_1, \ldots, q_{35} \in F$
We look at $q_0, \ldots, q_{34}$.

$\exists 0 \le i < j \le 34$ such that $q_i = q_j$. Say $i = 3$ and $j = 5$.

Feed in the string a^{33}. **There is a Path:**

$s = q_0, q_1, q_2, q_3 = q_5, q_6, q_7, q_8 \ldots, q_{35} \in F$.

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem any NFA for L_1 has at least 35 states.
Proof: Assume BWOC ($\exists$NFA M), ≤ 34 states, for L_1.
Feed in the string a^{35}. **Some Path Accepts.**

Let the states visited on that path be: $s = q_0, q_1, \ldots, q_{35} \in F$
We look at $q_0, \ldots, q_{34}$.

$\exists 0 \leq i < j \leq 34$ such that $q_i = q_j$. Say $i = 3$ and $j = 5$.

Feed in the string a^{33}. **There is a Path:**

$s = q_0, q_1, q_2, q_3 = q_5, q_6, q_7, q_8 \ldots, q_{35} \in F$.

There is a path that accepts a^{33}. That is the contradiction.

NFA for $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$

Theorem any NFA for L_1 has at least 35 states.
Proof: Assume BWOC ($\exists$NFA M), ≤ 34 states, for L_1.
Feed in the string a^{35}. **Some Path Accepts.**

Let the states visited on that path be: $s = q_0, q_1, \ldots, q_{35} \in F$
We look at $q_0, \ldots, q_{34}$.

$\exists 0 \le i < j \le 34$ such that $q_i = q_j$. Say $i = 3$ and $j = 5$.

Feed in the string a^{33}. **There is a Path:**

$s = q_0, q_1, q_2, q_3 = q_5, q_6, q_7, q_8 \ldots, q_{35} \in F$.

There is a path that accepts a^{33}. That is the contradiction.

General Proof may be on a $2^{\{HW,MID,FINAL\}}$

$$L = \{a^i : i \equiv 0 \pmod{m}\}$$

$L = \{a^i : i \equiv 0 \pmod{m}\}$

1. There is a DFA for L with m states.

$L = \{a^i : i \equiv 0 \pmod{m}\}$

1. There is a DFA for L with m states.
2. If M is a DFA for L then M has $\geq m$ states.

$L = \{a^i : i \equiv 0 \pmod{m}\}$

1. There is a DFA for L with m states.
2. If M is a DFA for L then M has $\geq m$ states.
3. There is an NFA for L with m states.

$L = \{a^i : i \equiv 0 \pmod{m}\}$

1. There is a DFA for L with m states.
2. If M is a DFA for L then M has $\geq m$ states.
3. There is an NFA for L with m states.
4. If M is an NFA for L then M has $\geq m$ states.

Second Language We Consider

$$L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$$

DFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

DFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states: swap final-$\overline{\text{final}}$ states in DFA for L_1.

DFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states: swap final-$\overline{\text{final}}$ states in DFA for L_1.

Is there a smaller DFA for L_2?

DFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states: swap final-$\overline{\text{final}}$ states in DFA for L_1.

Is there a smaller DFA for L_2?

VOTE

DFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states: swap final-$\overline{\text{final}}$ states in DFA for L_1.

Is there a smaller DFA for L_2?

VOTE

1. Bill knows a DFA for L_2 with ≤ 34 states.

DFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states: swap final-$\overline{\text{final}}$ states in DFA for L_1.

Is there a smaller DFA for L_2?

VOTE

1. Bill knows a DFA for L_2 with ≤ 34 states.
2. Bill can prove all DFA's for L_2 have ≥ 35 states.

DFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states: swap final-$\overline{\text{final}}$ states in DFA for L_1.

Is there a smaller DFA for L_2?

VOTE

1. Bill knows a DFA for L_2 with ≤ 34 states.
2. Bill can prove all DFA's for L_2 have ≥ 35 states.
3. The answer is UNKNOWN TO BILL!

DFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states: swap final-$\overline{\text{final}}$ states in DFA for L_1.

Is there a smaller DFA for L_2?

VOTE

1. Bill knows a DFA for L_2 with ≤ 34 states.
2. Bill can prove all DFA's for L_2 have ≥ 35 states.
3. The answer is UNKNOWN TO BILL!

Bill can prove all DFA's for L_2 have ≥ 35 states:

DFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states: swap final-$\overline{\text{final}}$ states in DFA for L_1.

Is there a smaller DFA for L_2?

VOTE

1. Bill knows a DFA for L_2 with ≤ 34 states.
2. Bill can prove all DFA's for L_2 have ≥ 35 states.
3. The answer is UNKNOWN TO BILL!

Bill can prove all DFA's for L_2 have ≥ 35 states:
Assume $\exists$DFA M for L_2 with ≤ 34 states.

DFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states: swap final-$\overline{\text{final}}$ states in DFA for L_1.

Is there a smaller DFA for L_2?

VOTE

1. Bill knows a DFA for L_2 with ≤ 34 states.
2. Bill can prove all DFA's for L_2 have ≥ 35 states.
3. The answer is UNKNOWN TO BILL!

Bill can prove all DFA's for L_2 have ≥ 35 states:
Assume $\exists$DFA M for L_2 with ≤ 34 states.
Swap final-$\overline{\text{final}}$ states of M to get DFA for L_1: ≤ 34 states.

DFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states: swap final-$\overline{\text{final}}$ states in DFA for L_1.

Is there a smaller DFA for L_2?

VOTE

1. Bill knows a DFA for L_2 with ≤ 34 states.
2. Bill can prove all DFA's for L_2 have ≥ 35 states.
3. The answer is UNKNOWN TO BILL!

Bill can prove all DFA's for L_2 have ≥ 35 states:
Assume $\exists$DFA M for L_2 with ≤ 34 states.
Swap final-$\overline{\text{final}}$ states of M to get DFA for L_1: ≤ 34 states.
Contradiction.

NFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states, hence $\exists$ NFA for L_2: 35 states.

NFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states, hence $\exists$ NFA for L_2: 35 states.

Is there a smaller NFA for L_2?

NFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states, hence $\exists$ NFA for L_2: 35 states.

Is there a smaller NFA for L_2?

VOTE

NFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states, hence $\exists$ NFA for L_2: 35 states.

Is there a smaller NFA for L_2?

VOTE

1. Bill knows a NFA for L_2 with ≤ 34 states.

NFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states, hence $\exists$ NFA for L_2: 35 states.

Is there a smaller NFA for L_2?

VOTE

1. Bill knows a NFA for L_2 with ≤ 34 states.
2. Bill can prove all NFA's for L_2 have ≥ 35 states.

NFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states, hence $\exists$ NFA for L_2: 35 states.

Is there a smaller NFA for L_2?

VOTE

1. Bill knows a NFA for L_2 with ≤ 34 states.
2. Bill can prove all NFA's for L_2 have ≥ 35 states.
3. The answer is UNKNOWN TO BILL!

NFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$\exists$ DFA for L_2: 35 states, hence $\exists$ NFA for L_2: 35 states.

Is there a smaller NFA for L_2?

VOTE

1. Bill knows a NFA for L_2 with ≤ 34 states.
2. Bill can prove all NFA's for L_2 have ≥ 35 states.
3. The answer is UNKNOWN TO BILL!

Bill knows a NFA for L_2 with ≤ 34 states. Next slides.

NFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

Note

NFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

Note

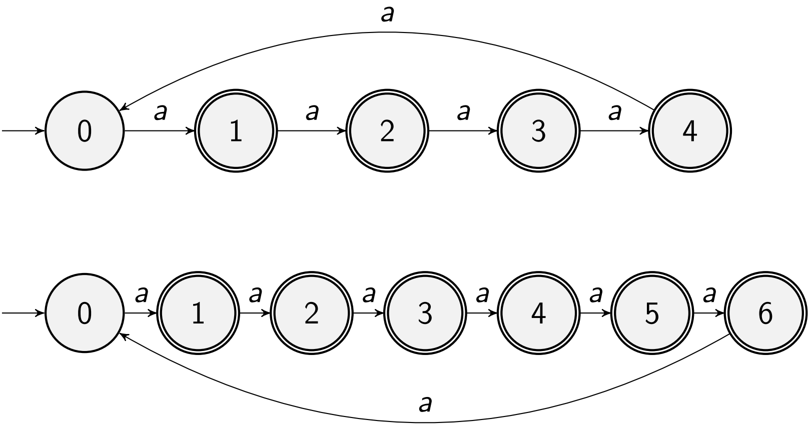
1. If $i \not\equiv 0 \pmod 5$ then $a^i \in L_2$ (Since $35 \equiv 0 \pmod 5$.)

NFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

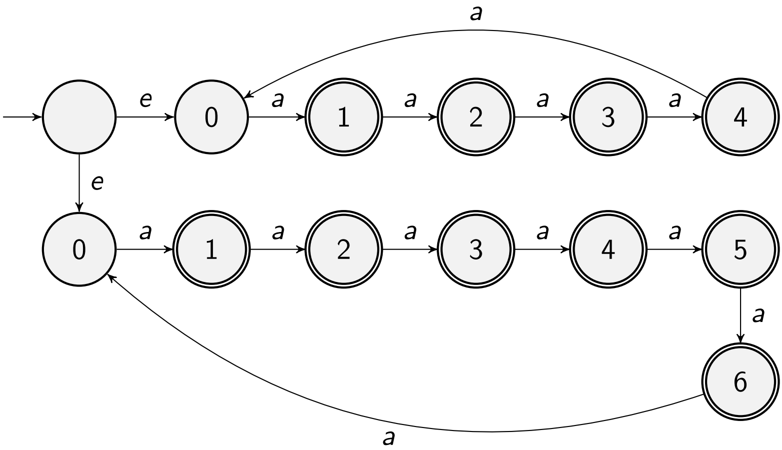
Note

1. If $i \not\equiv 0 \pmod 5$ then $a^i \in L_2$ (Since $35 \equiv 0 \pmod 5$.)
2. If $i \not\equiv 0 \pmod 7$ then $a^i \in L_2$ (Since $35 \equiv 0 \pmod 7$.)

Two Helpful DFAs



NFA for $L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$



$L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

We need the following claim:

$L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

We need the following claim:

Claim $i \not\equiv 0 \pmod{35} \rightarrow i \not\equiv 0 \pmod{5} \vee i \not\equiv 0 \pmod{7}$.

$L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

We need the following claim:

Claim $i \not\equiv 0 \pmod{35} \rightarrow i \not\equiv 0 \pmod{5} \vee i \not\equiv 0 \pmod{7}$.
Pf We prove contrapositive.

$L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

We need the following claim:

Claim $i \not\equiv 0 \pmod{35} \rightarrow i \not\equiv 0 \pmod{5} \vee i \not\equiv 0 \pmod{7}$.
Pf We prove contrapositive.
Assume $i \equiv 0 \pmod{5}$ AND $i \equiv 0 \pmod{7}$.

$L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

We need the following claim:

Claim $i \not\equiv 0 \pmod{35} \rightarrow i \not\equiv 0 \pmod{5} \vee i \not\equiv 0 \pmod{7}$.
Pf We prove contrapositive.
Assume $i \equiv 0 \pmod{5}$ AND $i \equiv 0 \pmod{7}$.

There exists x such that $i = 5x$

$L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

We need the following claim:

Claim $i \not\equiv 0 \pmod{35} \rightarrow i \not\equiv 0 \pmod{5} \vee i \not\equiv 0 \pmod{7}$.
Pf We prove contrapositive.
Assume $i \equiv 0 \pmod{5}$ AND $i \equiv 0 \pmod{7}$.

There exists x such that $i = 5x$

There exists y such that $i = 7y$

$L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

We need the following claim:

Claim $i \not\equiv 0 \pmod{35} \rightarrow i \not\equiv 0 \pmod{5} \vee i \not\equiv 0 \pmod{7}$.
Pf We prove contrapositive.
Assume $i \equiv 0 \pmod{5}$ AND $i \equiv 0 \pmod{7}$.

There exists x such that $i = 5x$

There exists y such that $i = 7y$

$5x = 7y$. So 5 divides $7y$.

$L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

We need the following claim:

Claim $i \not\equiv 0 \pmod{35} \rightarrow i \not\equiv 0 \pmod{5} \vee i \not\equiv 0 \pmod{7}$.
Pf We prove contrapositive.
Assume $i \equiv 0 \pmod{5}$ AND $i \equiv 0 \pmod{7}$.

There exists x such that $i = 5x$

There exists y such that $i = 7y$

$5x = 7y$. So 5 divides $7y$.

Since 5,7 have no common factors 5 divides y.

$L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

We need the following claim:

Claim $i \not\equiv 0 \pmod{35} \rightarrow i \not\equiv 0 \pmod{5} \vee i \not\equiv 0 \pmod{7}$.
Pf We prove contrapositive.
Assume $i \equiv 0 \pmod{5}$ AND $i \equiv 0 \pmod{7}$.

There exists x such that $i = 5x$

There exists y such that $i = 7y$

$5x = 7y$. So 5 divides $7y$.

Since 5,7 have no common factors 5 divides y.

There exists z, $y = 5z$, so $i = 7y = 35z$.

$L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

$L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

DFA for L_2 requires 35 states.

$L_2 = \{a^i : i \not\equiv 0 \pmod{35}\}$

DFA for L_2 requires 35 states.

NFA for L_2 can be done with $1 + 5 + 7 = 13$ states.

NFA for $L_2 = \{a^i : i \equiv 0 \pmod{35}\}$

L_2 can be done by an NFA with 13 states.

NFA for $L_2 = \{a^i : i \equiv 0 \pmod{35}\}$

L_2 can be done by an NFA with 13 states.

$\exists$ NFA for L_2 with ≤ 12 states?

NFA for $L_2 = \{a^i : i \equiv 0 \pmod{35}\}$

L_2 can be done by an NFA with 13 states.

$\exists$ NFA for L_2 with ≤ 12 states?

VOTE

NFA for $L_2 = \{a^i : i \equiv 0 \pmod{35}\}$

L_2 can be done by an NFA with 13 states.

$\exists$ NFA for L_2 with ≤ 12 states?

VOTE

1. Bill knows an NFA for L_2 with ≤ 12 states.

NFA for $L_2 = \{a^i : i \equiv 0 \pmod{35}\}$

L_2 can be done by an NFA with 13 states.

$\exists$ NFA for L_2 with ≤ 12 states?

VOTE

1. Bill knows an NFA for L_2 with ≤ 12 states.
2. Bill can prove all NFA's for L_2 have ≥ 13 states.

NFA for $L_2 = \{a^i : i \equiv 0 \pmod{35}\}$

L_2 can be done by an NFA with 13 states.

$\exists$ NFA for L_2 with ≤ 12 states?

VOTE

1. Bill knows an NFA for L_2 with ≤ 12 states.
2. Bill can prove all NFA's for L_2 have ≥ 13 states.
3. The answer is UNKNOWN TO BILL!

NFA for $L_2 = \{a^i : i \equiv 0 \pmod{35}\}$

L_2 can be done by an NFA with 13 states.

$\exists$ NFA for L_2 with ≤ 12 states?

VOTE

1. Bill knows an NFA for L_2 with ≤ 12 states.
2. Bill can prove all NFA's for L_2 have ≥ 13 states.
3. The answer is UNKNOWN TO BILL!

The answer is UNKNOWN TO BILL!

Third Language We Consider

$$L_3 = \{a^{1000}\}$$

$L_3 = \{a^{1000}\}$

This is similar to $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$.

1. There is a DFA for L_3 that has 1000 states.
2. Any DFA for L_3 has ≥ 1000 states.
3. There is an NFA for L_3 that has 1000 states.
4. Any NFA for L_3 has ≥ 1000 states.

$L_3 = \{a^{1000}\}$

This is similar to $L_1 = \{a^i : i \equiv 0 \pmod{35}\}$.

1. There is a DFA for L_3 that has 1000 states.
2. Any DFA for L_3 has ≥ 1000 states.
3. There is an NFA for L_3 that has 1000 states.
4. Any NFA for L_3 has ≥ 1000 states.

Might be on a $2^{\{HW,MID,FINAL\}}$.

Fourth Language We Consider

$$L_4 = \{a^i : i \neq 1000\}$$

DFA for $L_4 = \{a^i : i \neq 1000\}$

DFA for $L_4 = \{a^i : i \neq 1000\}$

1. There is a DFA for L_4 that has 1000 states.
2. Any DFA for L_3 has ≥ 1000 states.

NFA for $L_4 = \{a^i : i \neq 1000\}$

NFA for $L_4 = \{a^i : i \neq 1000\}$

There is an NFA for L_4 that has 1000 states.

NFA for $L_4 = \{a^i : i \neq 1000\}$

There is an NFA for L_4 that has 1000 states.

Work in groups to see if you can do better.

Is there an NFA for L_4 with ≤ 999 states?

NFA for $L_4 = \{a^i : i \neq 1000\}$

There is an NFA for L_4 that has 1000 states.
Work in groups to see if you can do better.
Is there an NFA for L_4 with ≤ 999 states?
VOTE

NFA for $L_4 = \{a^i : i \ne 1000\}$

There is an NFA for L_4 that has 1000 states.
Work in groups to see if you can do better.

Is there an NFA for L_4 with ≤ 999 states?

VOTE

1. Bill knows an NFA for L_4 with ≤ 999 states.

NFA for $L_4 = \{a^i : i \neq 1000\}$

There is an NFA for L_4 that has 1000 states.
Work in groups to see if you can do better.

Is there an NFA for L_4 with ≤ 999 states?

VOTE

1. Bill knows an NFA for L_4 with ≤ 999 states.
2. Bill can prove all NFA's for L_4 have ≥ 1000 states.

NFA for $L_4 = \{a^i : i \neq 1000\}$

There is an NFA for L_4 that has 1000 states.
Work in groups to see if you can do better.

Is there an NFA for L_4 with ≤ 999 states?

VOTE

1. Bill knows an NFA for L_4 with ≤ 999 states.
2. Bill can prove all NFA's for L_4 have ≥ 1000 states.
3. The answer is UNKNOWN TO BILL!

NFA for $L_4 = \{a^i : i \neq 1000\}$

There is an NFA for L_4 that has 1000 states.
Work in groups to see if you can do better.

Is there an NFA for L_4 with ≤ 999 states?

VOTE

1. Bill knows an NFA for L_4 with ≤ 999 states.
2. Bill can prove all NFA's for L_4 have ≥ 1000 states.
3. The answer is UNKNOWN TO BILL!

Bill knows an NFA for L_4 with ≤ 999 states.

How Small?

How Small is the NFA for L_4

How Small is the NFA for L_4

VOTE. Let s be numb states in smallest NFA for L_4 that Bill knows.

How Small is the NFA for L_4

VOTE. Let s be numb states in smallest NFA for L_4 that Bill knows.

1. $700 \le s \le 999$

How Small is the NFA for L_4

VOTE. Let s be numb states in smallest NFA for L_4 that Bill knows.

1. $700 \le s \le 999$
2. $400 \le s \le 699$

How Small is the NFA for L_4

VOTE. Let s be numb states in smallest NFA for L_4 that Bill knows.

1. $700 \le s \le 999$
2. $400 \le s \le 699$
3. $100 \le s \le 399$

How Small is the NFA for L_4

VOTE. Let s be numb states in smallest NFA for L_4 that Bill knows.

1. $700 \le s \le 999$
2. $400 \le s \le 699$
3. $100 \le s \le 399$
4. $s \le 99$

Bill knows an NFA for L_4 with ≤ 99 states.

$L_4 = \{a^n : n \neq 1000\}$

Answer This can be done with 70 states.
This will take a few slides.

$L_4 = \{a^n : n \ne 1000\}$

Answer This can be done with 70 states.
This will take a few slides.
And there will be an **important moral to the story**.

Overall Method

Overall Method

Two NFA's:

Overall Method

Two NFA's:

NFA A:

Overall Method

Two NFA's:

NFA A:

- Does NOT accept a^{1000}.

Overall Method

Two NFA's:

NFA A:

- Does NOT accept a^{1000}.
- Accepts all words longer than 1000.

Overall Method

Two NFA's:

NFA A:

- Does NOT accept a^{1000}.
- Accepts all words longer than 1000.
- Do not care about words shorter than 1000.

Overall Method

Two NFA's:

NFA A:

- Does NOT accept a^{1000}.
- Accepts all words longer than 1000.
- Do not care about words shorter than 1000.

NFA B:

Overall Method

Two NFA's:

NFA A:

- Does NOT accept a^{1000}.
- Accepts all words longer than 1000.
- Do not care about words shorter than 1000.

NFA B:

- Does NOT accept a^{1000}.

Overall Method

Two NFA's:

NFA A:

- Does NOT accept a^{1000}.
- Accepts all words longer than 1000.
- Do not care about words shorter than 1000.

NFA B:

- Does NOT accept a^{1000}.
- Accepts all words shorter than 1000.

Overall Method

Two NFA's:

NFA A:

- Does NOT accept a^{1000}.
- Accepts all words longer than 1000.
- Do not care about words shorter than 1000.

NFA B:

- Does NOT accept a^{1000}.
- Accepts all words shorter than 1000.
- Do not care about words longer than 1000.

Overall Method

Two NFA's:

NFA A:

- Does NOT accept a^{1000}.
- Accepts all words longer than 1000.
- Do not care about words shorter than 1000.

NFA B:

- Does NOT accept a^{1000}.
- Accepts all words shorter than 1000.
- Do not care about words longer than 1000.

Create the union of NFA's A and B.

NFA A

Sums of 32's and 33's

Thm

Sums of 32's and 33's

Thm

1. For all $n \geq 992$ there exists $x, y \in \mathbb{N}$ such that $n = 32x + 33y$.

Sums of 32's and 33's

Thm

1. For all $n \geq 992$ there exists $x, y \in \mathbb{N}$ such that $n = 32x + 33y$.
2. There does not exist $x, y \in \mathbb{N}$ such that $991 = 32x + 33y$.

Sums of 32's and 33's

Thm

1. For all $n \geq 992$ there exists $x, y \in \mathbb{N}$ such that $n = 32x + 33y$.
2. There does not exist $x, y \in \mathbb{N}$ such that $991 = 32x + 33y$.

Write down this theorem! Will prove on next few slides and you need to know what I am proving.

Sums of 32's and 33's

Thm

1. For all $n \geq 992$ there exists $x, y \in \mathbb{N}$ such that $n = 32x + 33y$.
2. There does not exist $x, y \in \mathbb{N}$ such that $991 = 32x + 33y$.

Write down this theorem! Will prove on next few slides and you need to know what I am proving.

We will prove this by induction.

Base Case $992 = 32 \times 31 + 33 \times 0$.

$(\forall n \geq 992)(\exists x, y \in N)[n = 32x + 33y]$

Inductive Hypothesis $n \geq 993$ and $(\exists x', y')[n - 1 = 32x' + 33y']$.

$(\forall n \geq 992)(\exists x, y \in N)[n = 32x + 33y]$

Inductive Hypothesis $n \geq 993$ and $(\exists x', y')[n - 1 = 32x' + 33y']$.
Intuition Want to swap coins in and out to increase by 1. Can swap out a 32-coin and put in a 33-coin

$(\forall n \ge 992)(\exists x, y \in N)[n = 32x + 33y]$

Inductive Hypothesis $n \ge 993$ and $(\exists x', y')[n-1 = 32x' + 33y']$.
Intuition Want to swap coins in and out to increase by 1. Can swap out a 32-coin and put in a 33-coin if I HAVE a 32-coin.

$(\forall n \geq 992)(\exists x, y \in N)[n = 32x + 33y]$

Inductive Hypothesis $n \geq 993$ and $(\exists x', y')[n-1 = 32x' + 33y']$.
Intuition Want to swap coins in and out to increase by 1. Can swap out a 32-coin and put in a 33-coin if I HAVE a 32-coin.
Case 1 $x' \geq 1$. Then $n = 32(x'-1) + 33(y'+1)$.

$(\forall n \geq 992)(\exists x, y \in N)[n = 32x + 33y]$

Inductive Hypothesis $n \geq 993$ and $(\exists x', y')[n-1 = 32x' + 33y']$.

Intuition Want to swap coins in and out to increase by 1. Can swap out a 32-coin and put in a 33-coin if I HAVE a 32-coin.

Case 1 $x' \geq 1$. Then $n = 32(x'-1) + 33(y'+1)$.

Intuition What to do if $x' = 0$. Need to remove some 33's and add some 32's. Use that $32 \times 32 - 31 \times 33 = 1024 - 1023 = 1$. Can swap out 31 33-coins and put in 32 32-coins

$(\forall n \geq 992)(\exists x, y \in N)[n = 32x + 33y]$

Inductive Hypothesis $n \geq 993$ and $(\exists x', y')[n - 1 = 32x' + 33y']$.

Intuition Want to swap coins in and out to increase by 1. Can swap out a 32-coin and put in a 33-coin if I HAVE a 32-coin.

Case 1 $x' \geq 1$. Then $n = 32(x' - 1) + 33(y' + 1)$.

Intuition What to do if $x' = 0$. Need to remove some 33's and add some 32's. Use that $32 \times 32 - 31 \times 33 = 1024 - 1023 = 1$. Can swap out 31 33-coins and put in 32 32-coinsif I HAVE 31 33-coins.

$(\forall n \geq 992)(\exists x, y \in N)[n = 32x + 33y]$

Inductive Hypothesis $n \geq 993$ and $(\exists x', y')[n-1 = 32x' + 33y']$.
Intuition Want to swap coins in and out to increase by 1. Can swap out a 32-coin and put in a 33-coin if I HAVE a 32-coin.
Case 1 $x' \geq 1$. Then $n = 32(x'-1) + 33(y'+1)$.
Intuition What to do if $x' = 0$. Need to remove some 33's and add some 32's. Use that $32 \times 32 - 31 \times 33 = 1024 - 1023 = 1$. Can swap out 31 33-coins and put in 32 32-coinsif I HAVE 31 33-coins.
Case 2 $y' \geq 31$. Then $n = 32(x'+32) + 33(y'-31)$.

$(\forall n \ge 992)(\exists x, y \in N)[n = 32x + 33y]$

Inductive Hypothesis $n \ge 993$ and $(\exists x', y')[n - 1 = 32x' + 33y']$.
Intuition Want to swap coins in and out to increase by 1. Can swap out a 32-coin and put in a 33-coin if I HAVE a 32-coin.
Case 1 $x' \ge 1$. Then $n = 32(x' - 1) + 33(y' + 1)$.
Intuition What to do if $x' = 0$. Need to remove some 33's and add some 32's. Use that $32 \times 32 - 31 \times 33 = 1024 - 1023 = 1$. Can swap out 31 33-coins and put in 32 32-coinsif I HAVE 31 33-coins.
Case 2 $y' \ge 31$. Then $n = 32(x' + 32) + 33(y' - 31)$.
Case 3 $x' \le 0$ and $y' \le 30$. Then $n = 32x' + 33y' \le 33 \times 30 = 990 < 993$, so cannot occur.

There is no $x, y \in N$ with $991 = 32x + 33y$

Pf by contradiction.

There is no $x, y \in N$ with $991 = 32x + 33y$

Pf by contradiction.

Assume there exists $x, y \in \mathbb{N}$ such that

$$991 = 32x + 33y$$

There is no $x, y \in N$ with $991 = 32x + 33y$

Pf by contradiction.

Assume there exists $x, y \in \mathbb{N}$ such that

$$991 = 32x + 33y$$

Then

$$991 \equiv 32x + 33y \pmod{32}$$

There is no $x, y \in N$ with $991 = 32x + 33y$

Pf by contradiction.
Assume there exists $x, y \in \mathbb{N}$ such that

$$991 = 32x + 33y$$

Then

$$991 \equiv 32x + 33y \pmod{32}$$

$$31 \equiv 0x + 1y \pmod{32}$$

There is no $x, y \in N$ with $991 = 32x + 33y$

Pf by contradiction.

Assume there exists $x, y \in \mathbb{N}$ such that

$$991 = 32x + 33y$$

Then

$$991 \equiv 32x + 33y \pmod{32}$$

$$31 \equiv 0x + 1y \pmod{32}$$

$$31 \equiv y \pmod{32} \text{ So } y \geq 31$$

There is no $x, y \in N$ with $991 = 32x + 33y$

Pf by contradiction.

Assume there exists $x, y \in \mathbb{N}$ such that

$$991 = 32x + 33y$$

Then

$$991 \equiv 32x + 33y \pmod{32}$$

$$31 \equiv 0x + 1y \pmod{32}$$

$$31 \equiv y \pmod{32} \text{ So } y \geq 31$$

$991 = 32x + 33y \geq 32x + 33 \times 31 \geq 1023$ **Contradiction!**

Sums of 32's and 33's and ONE 9

Thm

1) For all $n \geq 1001$ there exists $x, y \in \mathbb{N}$ such that $n = 32x + 33y + 9$.

Sums of 32's and 33's and ONE 9

Thm

1) For all $n \geq 1001$ there exists $x, y \in \mathbb{N}$ such that $n = 32x + 33y + 9$.

2) There does not exist $x, y \in \mathbb{N}$ such that $1000 = 32x + 33y + 9$.

Sums of 32's and 33's and ONE 9

Thm

1) For all $n \geq 1001$ there exists $x, y \in \mathbb{N}$ such that $n = 32x + 33y + 9$.

2) There does not exist $x, y \in \mathbb{N}$ such that $1000 = 32x + 33y + 9$.

Pf

Sums of 32's and 33's and ONE 9

Thm

1) For all $n \geq 1001$ there exists $x, y \in \mathbb{N}$ such that $n = 32x + 33y + 9$.

2) There does not exist $x, y \in \mathbb{N}$ such that $1000 = 32x + 33y + 9$.

Pf

1) If $n \geq 1001$ then $n - 9 \geq 992$ so by prior Thm

$$(\exists x, y \in \mathbb{N})[n - 9 = 32x + 33y]$$

Sums of 32's and 33's and ONE 9

Thm

1) For all $n \geq 1001$ there exists $x, y \in \mathbb{N}$ such that $n = 32x + 33y + 9$.

2) There does not exist $x, y \in \mathbb{N}$ such that $1000 = 32x + 33y + 9$.

Pf

1) If $n \geq 1001$ then $n - 9 \geq 992$ so by prior Thm

$$(\exists x, y \in \mathbb{N})[n - 9 = 32x + 33y]$$

$$(\exists x, y \in \mathbb{N})[n = 32x + 33y + 9]$$

Sums of 32's and 33's and ONE 9

Thm

1) For all $n \geq 1001$ there exists $x, y \in \mathbb{N}$ such that $n = 32x + 33y + 9$.

2) There does not exist $x, y \in \mathbb{N}$ such that $1000 = 32x + 33y + 9$.

Pf

1) If $n \geq 1001$ then $n - 9 \geq 992$ so by prior Thm

$$(\exists x, y \in \mathbb{N})[n - 9 = 32x + 33y]$$

$$(\exists x, y \in \mathbb{N})[n = 32x + 33y + 9]$$

2) Assume, by way of contradiction,

$$(\exists x, y)[1000 = 32x + 33y + 9]$$

Sums of 32's and 33's and ONE 9

Thm

1) For all $n \geq 1001$ there exists $x, y \in \mathbb{N}$ such that $n = 32x + 33y + 9$.

2) There does not exist $x, y \in \mathbb{N}$ such that $1000 = 32x + 33y + 9$.

Pf

1) If $n \geq 1001$ then $n - 9 \geq 992$ so by prior Thm

$$(\exists x, y \in \mathbb{N})[n - 9 = 32x + 33y]$$

$$(\exists x, y \in \mathbb{N})[n = 32x + 33y + 9]$$

2) Assume, by way of contradiction,

$$(\exists x, y)[1000 = 32x + 33y + 9]$$

$$(\exists x, y)[992 = 32x + 33y]$$

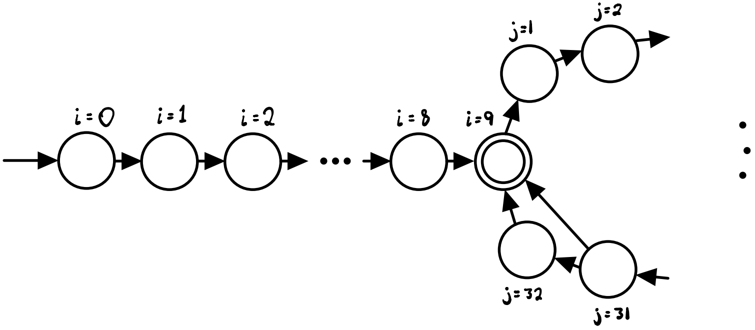
This contradicts prior Thm.

NFA A

Idea Start state, then 8 states, then a loop of size 33 with a shortcut at 32.

NFA A

Idea Start state, then 8 states, then a loop of size 33 with a shortcut at 32.



Number of States for $\{a^i : i \geq 1001\}$

Number of States for $\{a^i : i \geq 1001\}$

1. Start state

Number of States for $\{a^i : i \geq 1001\}$

1. Start state
2. A chain of 9 states including the start state.

Number of States for $\{a^i : i \geq 1001\}$

1. Start state
2. A chain of 9 states including the start state.
3. A loop of 33 states. The shortcut on 32 does not affect the number of states.

Number of States for $\{a^i : i \geq 1001\}$

1. Start state
2. A chain of 9 states including the start state.
3. A loop of 33 states. The shortcut on 32 does not affect the number of states.

Total number of states: $9 + 33 = 42$.

NFA B

Still Need NFA B

Still Need NFA B

Idea

Still Need NFA B

Idea

$1000 \equiv 0 \pmod 2$ SO want to accept $\{a^i : i \not\equiv 0 \pmod 2\}$.
2-state DFA.

Still Need NFA B

Idea

$1000 \equiv 0 \pmod 2$ SO want to accept $\{a^i : i \not\equiv 0 \pmod 2\}$.
2-state DFA.

$1000 \equiv 1 \pmod 3$ SO want to accept $\{a^i : i \not\equiv 1 \pmod 3\}$.
3-state DFA.

Still Need NFA B

Idea

$1000 \equiv 0 \pmod 2$ SO want to accept $\{a^i : i \not\equiv 0 \pmod 2\}$.
2-state DFA.

$1000 \equiv 1 \pmod 3$ SO want to accept $\{a^i : i \not\equiv 1 \pmod 3\}$.
3-state DFA.

$1000 \equiv 0 \pmod 5$ SO want to accept $\{a^i : i \not\equiv 0 \pmod 5\}$.
5-state DFA.

Still Need NFA B

Idea

$1000 \equiv 0 \pmod 2$ SO want to accept $\{a^i : i \not\equiv 0 \pmod 2\}$.
2-state DFA.

$1000 \equiv 1 \pmod 3$ SO want to accept $\{a^i : i \not\equiv 1 \pmod 3\}$.
3-state DFA.

$1000 \equiv 0 \pmod 5$ SO want to accept $\{a^i : i \not\equiv 0 \pmod 5\}$.
5-state DFA.

$1000 \equiv 6 \pmod 7$ SO want to accept $\{a^i : i \not\equiv 6 \pmod 7\}$.
7-state DFA.

Still Need NFA B

Idea

$1000 \equiv 0 \pmod 2$ SO want to accept $\{a^i : i \not\equiv 0 \pmod 2\}$.
2-state DFA.

$1000 \equiv 1 \pmod 3$ SO want to accept $\{a^i : i \not\equiv 1 \pmod 3\}$.
3-state DFA.

$1000 \equiv 0 \pmod 5$ SO want to accept $\{a^i : i \not\equiv 0 \pmod 5\}$.
5-state DFA.

$1000 \equiv 6 \pmod 7$ SO want to accept $\{a^i : i \not\equiv 6 \pmod 7\}$.
7-state DFA.

$1000 \equiv 10 \pmod{11}$ SO want to accept $\{a^i : i \not\equiv 10 \pmod{11}\}$.
11-state DFA.

Still Need NFA B

Idea

$1000 \equiv 0 \pmod 2$ SO want to accept $\{a^i : i \not\equiv 0 \pmod 2\}$.
2-state DFA.

$1000 \equiv 1 \pmod 3$ SO want to accept $\{a^i : i \not\equiv 1 \pmod 3\}$.
3-state DFA.

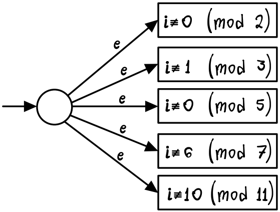
$1000 \equiv 0 \pmod 5$ SO want to accept $\{a^i : i \not\equiv 0 \pmod 5\}$.
5-state DFA.

$1000 \equiv 6 \pmod 7$ SO want to accept $\{a^i : i \not\equiv 6 \pmod 7\}$.
7-state DFA.

$1000 \equiv 10 \pmod{11}$ SO want to accept $\{a^i : i \not\equiv 10 \pmod{11}\}$.
11-state DFA.
Could go on to 13,17, etc. But we will see we can stop here.

Machine B

Machine B



NFA for $\{a^i : i \le 999\}$ AND More, but NOT a^{1000}

Thm Let M be the NFA from the last slide.
$M(a^{1000})$ is rejected. This is obvious.
For all $0 \le i \le 999$, $M(a^i)$ is accepted.
Pf We show that if $M(a^i)$ is rejected then $i \ge 1000$. Assume $M(a^i)$ rejected. Then

NFA for $\{a^i : i \le 999\}$ AND More, but NOT a^{1000}

Thm Let M be the NFA from the last slide.
$M(a^{1000})$ is rejected. This is obvious.
For all $0 \le i \le 999$, $M(a^i)$ is accepted.
Pf We show that if $M(a^i)$ is rejected then $i \ge 1000$. Assume $M(a^i)$ rejected. Then
$i \equiv 0 \pmod{2}$
$i \equiv 1 \pmod{3}$
$i \equiv 0 \pmod{5}$
$i \equiv 6 \pmod{7}$
$i \equiv 10 \pmod{11}$

NFA for $\{a^i : i \le 999\}$ AND More, but NOT a^{1000}

Thm Let M be the NFA from the last slide.
$M(a^{1000})$ is rejected. This is obvious.
For all $0 \le i \le 999$, $M(a^i)$ is accepted.
Pf We show that if $M(a^i)$ is rejected then $i \ge 1000$. Assume $M(a^i)$ rejected. Then
$i \equiv 0 \pmod 2$
$i \equiv 1 \pmod 3$
$i \equiv 0 \pmod 5$
$i \equiv 6 \pmod 7$
$i \equiv 10 \pmod{11}$
Continued on next slide

NFA for $\{a^i : i \leq 999\}$ AND More, but NOT a^{1000}

NFA for $\{a^i : i \le 999\}$ AND More, but NOT a^{1000}

$i \equiv 0 \pmod 2$
$i \equiv 1 \pmod 3$

NFA for $\{a^i : i \leq 999\}$ AND More, but NOT a^{1000}

$i \equiv 0 \pmod{2}$
$i \equiv 1 \pmod{3}$
Hence $i \equiv 4 \pmod{6}$.

NFA for $\{a^i : i \le 999\}$ AND More, but NOT a^{1000}

$i \equiv 0 \pmod{2}$
$i \equiv 1 \pmod{3}$
Hence $i \equiv 4 \pmod{6}$.

$i \equiv 0 \pmod{5}$
$i \equiv 6 \pmod{7}$

NFA for $\{a^i : i \le 999\}$ AND More, but NOT a^{1000}

$i \equiv 0 \pmod 2$
$i \equiv 1 \pmod 3$
Hence $i \equiv 4 \pmod 6$.

$i \equiv 0 \pmod 5$
$i \equiv 6 \pmod 7$

Hence $i \equiv 20 \pmod{35}$.

NFA for $\{a^i : i \le 999\}$ AND More, but NOT a^{1000}

$i \equiv 0 \pmod 2$
$i \equiv 1 \pmod 3$
Hence $i \equiv 4 \pmod 6$.

$i \equiv 0 \pmod 5$
$i \equiv 6 \pmod 7$

Hence $i \equiv 20 \pmod{35}$.

$i \equiv 10 \pmod{11}$

NFA for $\{a^i : i \le 999\}$ AND More, but NOT a^{1000}

$i \equiv 0 \pmod 2$
$i \equiv 1 \pmod 3$
Hence $i \equiv 4 \pmod 6$.

$i \equiv 0 \pmod 5$
$i \equiv 6 \pmod 7$

Hence $i \equiv 20 \pmod{35}$.

$i \equiv 10 \pmod{11}$

So we have
$i \equiv 4 \pmod 6$
$i \equiv 20 \pmod{35}$
$i \equiv 10 \pmod{11}$.
Continued on next slide

NFA for $\{a^i : i \le 999\}$ AND More, but NOT a^{1000}?

From:
$i \equiv 4 \pmod{6}$
$i \equiv 20 \pmod{35}$
$i \equiv 10 \pmod{11}$.
One can show
$i \equiv 1000 \pmod{6 \times 35 \times 11}$

NFA for $\{a^i : i \le 999\}$ AND More, but NOT a^{1000}?

From:
$i \equiv 4 \pmod 6$
$i \equiv 20 \pmod{35}$
$i \equiv 10 \pmod{11}$.
One can show
$i \equiv 1000 \pmod{6 \times 35 \times 11}$
So
$i \equiv 1000 \pmod{2310}$
Hence $i \ge 1000$.

NFA for $\{a^i : i \le 999\}$ AND More, but NOT a^{1000}?

From:
$i \equiv 4 \pmod 6)$
$i \equiv 20 \pmod{35}$
$i \equiv 10 \pmod{11}$.
One can show
$i \equiv 1000 \pmod{6 \times 35 \times 11}$
So
$i \equiv 1000 \pmod{2310}$
Hence $i \ge 1000$.
Recap If a^i is rejected then $i \ge 1000$.
Hence If $i \le 999$ then a^i is accepted.

How Many States for $\{a^i : i \le 999\}$ AND More, but NOT a^{1000}?

$2 + 3 + 5 + 7 + 11 = 28$ states.
Plus the start state, so 29.

NFA for $\{a^i : i \neq 1000\}$

NFA for $\{a^i : i \neq 1000\}$

1. We have an NFA on 42 states that accepts $\{a^i : i \geq 1001\}$ This includes the start state.

NFA for $\{a^i : i \neq 1000\}$

1. We have an NFA on 42 states that accepts $\{a^i : i \geq 1001\}$ This includes the start state.
2. We have an NFA on 29 states that accepts $\{a^i : i \leq 999\}$ and other stuff, but NOT a^{1000}. This includes the start state.

NFA for $\{a^i : i \neq 1000\}$

1. We have an NFA on 42 states that accepts $\{a^i : i \geq 1001\}$ This includes the start state.
2. We have an NFA on 29 states that accepts $\{a^i : i \leq 999\}$ and other stuff, but NOT a^{1000}. This includes the start state.

Take NFA of union using e-transitions for an NFA and do not count start state twice, so have

$$42 + 29 - 1 = 70 \text{ states.}$$

Interesting Problem, Profound Moral

Interesting Problem, Profound Moral

1. In the Springs of 2015, 2016, 2017, 2018, 2019, 2020, and 2021, Gasarch has given this problem to the students in CMSC 452.

Interesting Problem, Profound Moral

1. In the Springs of 2015, 2016, 2017, 2018, 2019, 2020, and 2021, Gasarch has given this problem to the students in CMSC 452.
2. Every year almost everyone thinks **The NFA requires $\sim n$ states**.

Interesting Problem, Profound Moral

1. In the Springs of 2015, 2016, 2017, 2018, 2019, 2020, and 2021, Gasarch has given this problem to the students in CMSC 452.
2. Every year almost everyone thinks **The NFA requires $\sim n$ states**.
3. Why is this? They did not know the trick.

Interesting Problem, Profound Moral

1. In the Springs of 2015, 2016, 2017, 2018, 2019, 2020, and 2021, Gasarch has given this problem to the students in CMSC 452.
2. Every year almost everyone thinks **The NFA requires $\sim n$ states**.
3. Why is this? They did not know the trick.
4. **Moral Lesson** Lower bounds are hard! You have to rule out that someone does not have a very clever trick that you just had not thought of.

This was NOT a lecture on Size of NFAs

You thought this was a lecture on sizes of NFAs.

This was NOT a lecture on Size of NFAs

You thought this was a lecture on sizes of NFAs.

It was not.

This was NOT a lecture on Size of NFAs

You thought this was a lecture on sizes of NFAs.

It was not.

- This is a lecture on NP-completeness.

This was NOT a lecture on Size of NFAs

You thought this was a lecture on sizes of NFAs.

It was not.

- This is a lecture on NP-completeness.
- Just because you cannot think of an algorithm for SAT in P does not mean that there is not one.

This was NOT a lecture on Size of NFAs

You thought this was a lecture on sizes of NFAs.

It was not.

- This is a lecture on NP-completeness.
- Just because you cannot think of an algorithm for SAT in P does not mean that there is not one.
- It is possible that someone will come up with a technique you didn't think of, or some use math you did not know.

This was NOT a lecture on Size of NFAs

You thought this was a lecture on sizes of NFAs.

It was not.

- This is a lecture on NP-completeness.
- Just because you cannot think of an algorithm for SAT in P does not mean that there is not one.
- It is possible that someone will come up with a technique you didn't think of, or some use math you did not know.
- Is this just a vague possibility?

This was NOT a lecture on Size of NFAs

You thought this was a lecture on sizes of NFAs.

It was not.

- This is a lecture on NP-completeness.
- Just because you cannot think of an algorithm for SAT in P does not mean that there is not one.
- It is possible that someone will come up with a technique you didn't think of, or some use math you did not know.
- Is this just a vague possibility?
  It just happened to you in a different context!

This was NOT a lecture on Size of NFAs

You thought this was a lecture on sizes of NFAs.

It was not.

- This is a lecture on NP-completeness.
- Just because you cannot think of an algorithm for SAT in P does not mean that there is not one.
- It is possible that someone will come up with a technique you didn't think of, or some use math you did not know.
- Is this just a vague possibility?
  It just happened to you in a different context!
  You thought $\{a^i : i \neq 1000\}$ required a ~ 1000 state NFA.

This was NOT a lecture on Size of NFAs

You thought this was a lecture on sizes of NFAs.

It was not.

- This is a lecture on NP-completeness.
- Just because you cannot think of an algorithm for SAT in P does not mean that there is not one.
- It is possible that someone will come up with a technique you didn't think of, or some use math you did not know.
- Is this just a vague possibility?
  It just happened to you in a different context!
  You thought $\{a^i : i \neq 1000\}$ required a ~ 1000 state NFA.
  But a technique and some math got it to 70 states.

This was NOT a lecture on Size of NFAs

You thought this was a lecture on sizes of NFAs.

It was not.

- This is a lecture on NP-completeness.
- Just because you cannot think of an algorithm for SAT in P does not mean that there is not one.
- It is possible that someone will come up with a technique you didn't think of, or some use math you did not know.
- Is this just a vague possibility?
  It just happened to you in a different context!
  You thought $\{a^i : i \neq 1000\}$ required a ~ 1000 state NFA.
  But a technique and some math got it to 70 states.
- **Upshot** Lower bounds are hard to prove since they must rule out techniques you have not thought of.

This was NOT a lecture on Size of NFAs

You thought this was a lecture on sizes of NFAs.

It was not.

- This is a lecture on NP-completeness.
- Just because you cannot think of an algorithm for SAT in P does not mean that there is not one.
- It is possible that someone will come up with a technique you didn't think of, or some use math you did not know.
- Is this just a vague possibility?
  It just happened to you in a different context!
  You thought $\{a^i : i \neq 1000\}$ required a ~ 1000 state NFA.
  But a technique and some math got it to 70 states.
- **Upshot** Lower bounds are hard to prove since they must rule out techniques you have not thought of.
- Respect the difficulty of lower bounds!

Can We Do Better than 70 States?

There is a 70-state NFA for $\{a^i : i \neq 1000\}$.

Can We Do Better than 70 States?

There is a 70-state NFA for $\{a^i : i \neq 1000\}$.

Is there a smaller NFA?

Can We Do Better than 70 States?

There is a 70-state NFA for $\{a^i : i \neq 1000\}$.

Is there a smaller NFA?

Vote:

Can We Do Better than 70 States?

There is a 70-state NFA for $\{a^i : i \neq 1000\}$.

Is there a smaller NFA?

Vote:

1. Bill knows an NFA with ≤ 69 states.

Can We Do Better than 70 States?

There is a 70-state NFA for $\{a^i : i \neq 1000\}$.

Is there a smaller NFA?

Vote:

1. Bill knows an NFA with ≤ 69 states.
2. Bill can prove that any NFA for L_4 has ≥ 70 states.

Can We Do Better than 70 States?

There is a 70-state NFA for $\{a^i : i \neq 1000\}$.

Is there a smaller NFA?

Vote:

1. Bill knows an NFA with ≤ 69 states.
2. Bill can prove that any NFA for L_4 has ≥ 70 states.
3. The answer is UNKNOWN TO BILL!

Can We Do Better than 70 States?

There is a 70-state NFA for $\{a^i : i \neq 1000\}$.

Is there a smaller NFA?

Vote:

1. Bill knows an NFA with ≤ 69 states.
2. Bill can prove that any NFA for L_4 has ≥ 70 states.
3. The answer is UNKNOWN TO BILL!

Bill knows an NFA with ≤ 69 states.

Can We Do Better than 70 States?

There is a 70-state NFA for $\{a^i : i \neq 1000\}$.

Is there a smaller NFA?

Vote:

1. Bill knows an NFA with ≤ 69 states.
2. Bill can prove that any NFA for L_4 has ≥ 70 states.
3. The answer is UNKNOWN TO BILL!

Bill knows an NFA with ≤ 69 states.
There is an NFA for L_4 with 59 states.

Can We Do Better than 70 States?

There is a 70-state NFA for $\{a^i : i \neq 1000\}$.

Is there a smaller NFA?

Vote:

1. Bill knows an NFA with ≤ 69 states.
2. Bill can prove that any NFA for L_4 has ≥ 70 states.
3. The answer is UNKNOWN TO BILL!

Bill knows an NFA with ≤ 69 states.
There is an NFA for L_4 with 59 states.
See next slide.

The 59-state NFA for L_4

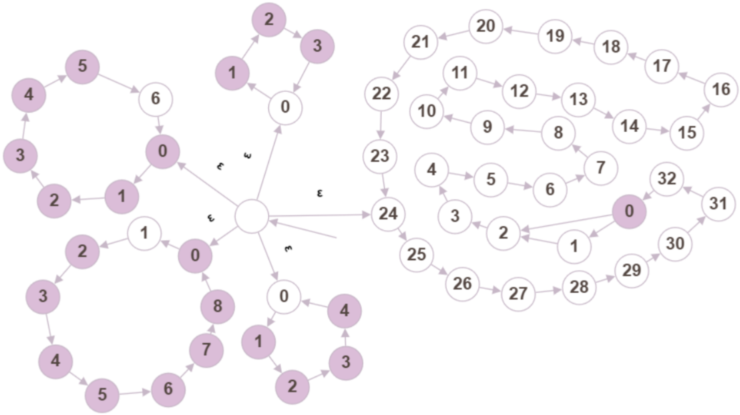


Figure: 59 State NFA for L_4

Two Tricks Used To Get it to 59 States

1. To get $\{a^i : i \leq 999\}$, we used DFAs that picked out specific values mod $\{2, 3, 5, 7, 11\}$.

Two Tricks Used To Get it to 59 States

1. To get $\{a^i : i \leq 999\}$, we used DFAs that picked out specific values mod $\{2, 3, 5, 7, 11\}$.

   The same proof works for any set of coprime numbers that multiply to ≥ 1000.

Two Tricks Used To Get it to 59 States

1. To get $\{a^i : i \leq 999\}$, we used DFAs that picked out specific values mod $\{2, 3, 5, 7, 11\}$.

   The same proof works for any set of coprime numbers that multiply to ≥ 1000.

   Optimally, we would use $\{4, 5, 7, 9\}$, saving 3 states.

Two Tricks Used To Get it to 59 States

1. To get $\{a^i : i \leq 999\}$, we used DFAs that picked out specific values mod $\{2, 3, 5, 7, 11\}$.

   The same proof works for any set of coprime numbers that multiply to ≥ 1000.

   Optimally, we would use $\{4, 5, 7, 9\}$, saving 3 states.
2. To get $\{a^i : i \geq 1001\}$, we calculated $32 \times 33 - 32 - 33 = 991$, and then added 9 additional states before the loop.

Two Tricks Used To Get it to 59 States

1. To get $\{a^i : i \leq 999\}$, we used DFAs that picked out specific values mod $\{2, 3, 5, 7, 11\}$.

   The same proof works for any set of coprime numbers that multiply to ≥ 1000.

   Optimally, we would use $\{4, 5, 7, 9\}$, saving 3 states.

2. To get $\{a^i : i \geq 1001\}$, we calculated $32 \times 33 - 32 - 33 = 991$, and then added 9 additional states before the loop.

   However, we could have instead made the 9th state of the loop accept, and have the shortcut go to the 9th state instead.

Two Tricks Used To Get it to 59 States

1. To get $\{a^i : i \leq 999\}$, we used DFAs that picked out specific values mod $\{2, 3, 5, 7, 11\}$.

   The same proof works for any set of coprime numbers that multiply to ≥ 1000.

   Optimally, we would use $\{4, 5, 7, 9\}$, saving 3 states.
2. To get $\{a^i : i \geq 1001\}$, we calculated $32 \times 33 - 32 - 33 = 991$, and then added 9 additional states before the loop.

   However, we could have instead made the 9th state of the loop accept, and have the shortcut go to the 9th state instead.

   This would save us 8 states, because we still need a distinct start state.

Can We Do Better than 59 States?

Vote:

1. No, 59 is optimal
2. Yes, but not by much
3. Yes, substantially!
4. Unknown to science!

Can We Do Better than 59 States?

Vote:

1. No, 59 is optimal
2. Yes, but not by much
3. Yes, substantially!
4. Unknown to science!

Answer: Unknown to science.

Math Needed for $\{a^i : i \neq n\}$ I

Frobenius Thm (aka The Chicken McNugget Thm)

Math Needed for $\{a^i : i \neq n\}$ I

Frobenius Thm (aka The Chicken McNugget Thm)

Thm If x, y are relatively prime then

- For all $z \geq xy - x - y + 1$ there exists $c, d \in \mathbb{N}$ such that $z = cx + dy$.
- There is no $c, d \in \mathbb{N}$ such that $xy - x - y = cx + dy$.

Math Needed for $\{a^i : i \neq n\}$ I

Frobenius Thm (aka The Chicken McNugget Thm)

Thm If x, y are relatively prime then

- For all $z \geq xy - x - y + 1$ there exists $c, d \in \mathbb{N}$ such that $z = cx + dy$.
- There is no $c, d \in \mathbb{N}$ such that $xy - x - y = cx + dy$.

We use this to get an NFA for $\{a^i : i \geq n + 1\}$ by using $x, y \approx \sqrt{n}$.

Math Needed for $\{a^i : i \ne n\}$ I

Frobenius Thm (aka The Chicken McNugget Thm)

Thm If x, y are relatively prime then

- For all $z \ge xy - x - y + 1$ there exists $c, d \in \mathbb{N}$ such that $z = cx + dy$.
- There is no $c, d \in \mathbb{N}$ such that $xy - x - y = cx + dy$.

We use this to get an NFA for $\{a^i : i \ge n + 1\}$ by using $x, y \approx \sqrt{n}$.
Want to get $xy - x - y \le n$ so can use the tail to get
$xy - x - y + t = n + 1$.

Math Needed for $\{a^i : i \neq n\}$ I

Frobenius Thm (aka The Chicken McNugget Thm)

Thm If x, y are relatively prime then

- For all $z \geq xy - x - y + 1$ there exists $c, d \in \mathbb{N}$ such that $z = cx + dy$.
- There is no $c, d \in \mathbb{N}$ such that $xy - x - y = cx + dy$.

We use this to get an NFA for $\{a^i : i \geq n + 1\}$ by using $x, y \approx \sqrt{n}$.
Want to get $xy - x - y \leq n$ so can use the tail to get
$xy - x - y + t = n + 1$.
This leads to loops and tail that are roughly $\leq 2\sqrt{n}$ states.

Math Needed for $\{a^i : i \ne n\}$ II

Thm Let $n \in \mathbb{N}$. Let $q_1, \ldots, q_k$ be rel prime such that $\prod_{i=1}^{k} q_i \ge n$. Then the set of all i such that

$i \not\equiv n \pmod{q_1}$.

$\vdots$

$i \not\equiv n \pmod{q_k}$.

Contains $\{1, \ldots, n-1\}$ and **does not contain n**

Math Needed for $\{a^i : i \neq n\}$ II

Thm Let $n \in \mathbb{N}$. Let $q_1, \ldots, q_k$ be rel prime such that $\prod_{i=1}^{k} q_i \geq n$. Then the set of all i such that
$i \not\equiv n \pmod{q_1}$.
$\vdots$
$i \not\equiv n \pmod{q_k}$.
Contains $\{1, \ldots, n-1\}$ and **does not contain n**

Number theory tells us that can find such a $q_1, \ldots, q_k$ with

$$\sum_{i=1}^{k} q_i \leq (\log n)^2 \log \log n.$$

Math Needed for $\{a^i : i \neq n\}$ II

Thm Let $n \in \mathbb{N}$. Let $q_1, \ldots, q_k$ be rel prime such that $\prod_{i=1}^{k} q_i \geq n$. Then the set of all i such that
$i \not\equiv n \pmod{q_1}$.
$\vdots$
$i \not\equiv n \pmod{q_k}$.
Contains $\{1, \ldots, n-1\}$ and **does not contain n**

Number theory tells us that can find such a $q_1, \ldots, q_k$ with

$$\sum_{i=1}^{k} q_i \leq (\log n)^2 \log \log n.$$

So can use this to get NFA for $\{a^i : i \leq n-1\}$ (and other stuff but not a^n) with $\leq (\log n)^2 \log \log n$ states.

From the Last Two Slides

No details, but from the last two slides you can get that $\{a^i : i \neq n\}$ has an NFA of size $\leq 2\sqrt{n} + (\log n)^2 \log\log n$.

From the Last Two Slides

No details, but from the last two slides you can get that $\{a^i : i \neq n\}$ has an NFA of size $\leq 2\sqrt{n} + (\log n)^2 \log\log n$.

Can be improved:

From the Last Two Slides

No details, but from the last two slides you can get that $\{a^i : i \neq n\}$ has an NFA of size $\leq 2\sqrt{n} + (\log n)^2 \log\log n$.

Can be improved:

Thm The language $\{a^i : i \neq n\}$ has an NFA of size $\sqrt{n} + O\left((\log n)^2 / \log\log n\right)$.

From the Last Two Slides

No details, but from the last two slides you can get that $\{a^i : i \neq n\}$ has an NFA of size $\leq 2\sqrt{n} + (\log n)^2 \log\log n$.

Can be improved:

Thm The language $\{a^i : i \neq n\}$ has an NFA of size $\sqrt{n} + O\left((\log n)^2 / \log\log n\right)$.

The bound is tight:

From the Last Two Slides

No details, but from the last two slides you can get that $\{a^i : i \neq n\}$ has an NFA of size $\leq 2\sqrt{n} + (\log n)^2 \log\log n$.

Can be improved:

Thm The language $\{a^i : i \neq n\}$ has an NFA of size $\sqrt{n} + O\left((\log n)^2 / \log\log n\right)$.

The bound is tight:

Thm Any NFA for $\{a^i : i \neq n\}$ requires at least $\sqrt{n}$ states.

From the Last Two Slides

No details, but from the last two slides you can get that $\{a^i : i \neq n\}$ has an NFA of size $\leq 2\sqrt{n} + (\log n)^2 \log\log n$.

Can be improved:

Thm The language $\{a^i : i \neq n\}$ has an NFA of size $\sqrt{n} + O\left((\log n)^2 / \log\log n\right)$.

The bound is tight:

Thm Any NFA for $\{a^i : i \neq n\}$ requires at least $\sqrt{n}$ states.

Paper by Gasarch-Metz-Xu-Shen-Zbarsky.

General size for DFA vs. NFA for one letter alphabet

General size for DFA vs. NFA for one letter alphabet

Thm If language over a one letter alphabet is accepted by an NFA of size n, then it is accepted by a DFA of size $O\left(e^{\sqrt{n \ln n}}\right)$.

General size for DFA vs. NFA for one letter alphabet

Thm If language over a one letter alphabet is accepted by an NFA of size n, then it is accepted by a DFA of size $O\left(e^{\sqrt{n \ln n}}\right)$.

The bound is tight:

General size for DFA vs. NFA for one letter alphabet

Thm If language over a one letter alphabet is accepted by an NFA of size n, then it is accepted by a DFA of size $O\left(e^{\sqrt{n \ln n}}\right)$.

The bound is tight:

Thm There exists a language over a one letter alphabet that is accepted on an NFA of size n, but any DFA for the language has size (at least) $\Omega\left(e^{\sqrt{n \ln n}}\right)$)on a DFA.

General size for DFA vs. NFA for one letter alphabet

Thm If language over a one letter alphabet is accepted by an NFA of size n, then it is accepted by a DFA of size $O\left(e^{\sqrt{n \ln n}}\right)$.

The bound is tight:

Thm There exists a language over a one letter alphabet that is accepted on an NFA of size n, but any DFA for the language has size (at least) $\Omega\left(e^{\sqrt{n \ln n}}\right)$)on a DFA.

Is this interesting and/or important?

NP-Completeness

NP-Completeness

Another reason this lecture is about NP-Completeness

NP-Completeness

Another reason this lecture is about NP-Completeness

Determinism versus Nondeterminism.