BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

Number of States for DFAs and NFAs

DFA and NFA

Recall the theorem:

Thm If L is accepted by an NFA on n states then L is accepted by a DFA on $\leq 2^n$ states.

DFA and NFA

Recall the theorem:
Thm If L is accepted by an NFA on n states then L is accepted by a DFA on $\leq 2^n$ states.

We look at languages and see if the NFA is much smaller than the DFA.

a is n From the End

$L_n = \Sigma^* a \Sigma^n$.
Thm Any DFA for L_n **requires** 2^{n+1} states.

a is n From the End

$L_n = \Sigma^* a \Sigma^n$.
Thm Any DFA for L_n **requires** 2^{n+1} states.

Let $M = (Q, \Sigma, \delta, s, F)$ be a DFA for L_n.

a is n From the End

$L_n = \Sigma^* a \Sigma^n$.
Thm Any DFA for L_n **requires** 2^{n+1} states.

Let $M = (Q, \Sigma, \delta, s, F)$ be a DFA for L_n.

Let $\delta(s, w)$ be the state M ends up with if w is input.

a is n From the End

$L_n = \Sigma^* a \Sigma^n$.

Thm Any DFA for L_n **requires** 2^{n+1} states.

Let $M = (Q, \Sigma, \delta, s, F)$ be a DFA for L_n.

Let $\delta(s, w)$ be the state M ends up with if w is input.

We show that $\delta(s, -)$ restricted to $\{0, 1\}^{n+1}$ is an injection, so there must be 2^{n+1} states.

a is n From the End

$L_n = \Sigma^* a \Sigma^n$.

Thm Any DFA for L_n **requires** 2^{n+1} states.

Let $M = (Q, \Sigma, \delta, s, F)$ be a DFA for L_n.

Let $\delta(s, w)$ be the state M ends up with if w is input.

We show that $\delta(s, -)$ restricted to $\{0, 1\}^{n+1}$ is an injection, so there must be 2^{n+1} states.

Assume $w \neq w'$. We show that $\delta(s, w) \neq \delta(s, w')$.

a is n From the End

$L_n = \Sigma^* a \Sigma^n$.
Thm Any DFA for L_n **requires** 2^{n+1} states.

Let $M = (Q, \Sigma, \delta, s, F)$ be a DFA for L_n.

Let $\delta(s, w)$ be the state M ends up with if w is input.

We show that $\delta(s, -)$ restricted to $\{0, 1\}^{n+1}$ is an injection, so there must be 2^{n+1} states.

Assume $w \neq w'$. We show that $\delta(s, w) \neq \delta(s, w')$.

Since $w \neq w'$, $(\exists x, y, y')$ $w = xay$ $sw' = xby'$.
Key Since $|w| = n + 1$, $|y| = |y'| \geq n$. So $a^{n-|y|}$ makes sense.

a is n From the End

$L_n = \Sigma^* a \Sigma^n$.

Thm Any DFA for L_n **requires** 2^{n+1} states.

Let $M = (Q, \Sigma, \delta, s, F)$ be a DFA for L_n.

Let $\delta(s, w)$ be the state M ends up with if w is input.

We show that $\delta(s, -)$ restricted to $\{0, 1\}^{n+1}$ is an injection, so there must be 2^{n+1} states.

Assume $w \neq w'$. We show that $\delta(s, w) \neq \delta(s, w')$.

Since $w \neq w'$, $(\exists x, y, y')$ $w = xay$ $sw' = xby'$.

Key Since $|w| = n + 1$, $|y| = |y'| \geq n$. So $a^{n-|y|}$ makes sense.

Assume, BWOC, $\delta(s, xay) = \delta(s, xby')$. Then

$$\delta(s, xaya^{n-|y|}) = \delta(s, xby'a^{n-|y'|})$$

a is n From the End

$L_n = \Sigma^* a \Sigma^n$.

Thm Any DFA for L_n **requires** 2^{n+1} states.

Let $M = (Q, \Sigma, \delta, s, F)$ be a DFA for L_n.

Let $\delta(s, w)$ be the state M ends up with if w is input.

We show that $\delta(s, -)$ restricted to $\{0, 1\}^{n+1}$ is an injection, so there must be 2^{n+1} states.

Assume $w \neq w'$. We show that $\delta(s, w) \neq \delta(s, w')$.

Since $w \neq w'$, $(\exists x, y, y')$ $w = xay$ $sw' = xby'$.
Key Since $|w| = n + 1$, $|y| = |y'| \geq n$. So $a^{n-|y|}$ makes sense.

Assume, BWOC, $\delta(s, xay) = \delta(s, xby')$. Then

$$\delta(s, xaya^{n-|y|}) = \delta(s, xby'a^{n-|y'|})$$

But $xaya^{n-|y|} \in L_n$ and $xby'a^{n-|y'} \notin L_n$.

a is n From the End

$L_n = \Sigma^* a \Sigma^n$.
Thm Any DFA for L_n **requires** 2^{n+1} states.

Let $M = (Q, \Sigma, \delta, s, F)$ be a DFA for L_n.

Let $\delta(s, w)$ be the state M ends up with if w is input.

We show that $\delta(s, -)$ restricted to $\{0, 1\}^{n+1}$ is an injection, so there must be 2^{n+1} states.

Assume $w \neq w'$. We show that $\delta(s, w) \neq \delta(s, w')$.

Since $w \neq w'$, $(\exists x, y, y')$ $w = xay$ $sw' = xby'$.
Key Since $|w| = n + 1$, $|y| = |y'| \geq n$. So $a^{n-|y|}$ makes sense.

Assume, BWOC, $\delta(s, xay) = \delta(s, xby')$. Then

$$\delta(s, xaya^{n-|y|}) = \delta(s, xby'a^{n-|y'|})$$

But $xaya^{n-|y|} \in L_n$ and $xby'a^{n-|y'} \notin L_n$.
That is a contradiction.

Size of NFA is $\ll$ Size of DFA

a is n From the End

$$L_n = \Sigma^* a \Sigma^n.$$

a is n From the End

$$L_n = \Sigma^* a \Sigma^n.$$

1. Every DFA for L **requires** $\geq 2^{n+1}$ states.

a is n From the End

$$L_n = \Sigma^* a \Sigma^n.$$

1. Every DFA for L **requires** $\geq 2^{n+1}$ states.
2. **There is** an NFA for L with $n+2$ states.

a is n From the End

$$L_n = \Sigma^* a \Sigma^n.$$

1. Every DFA for L **requires** $\geq 2^{n+1}$ states.
2. **There is** an NFA for L with $n+2$ states.
3. **There is a CFG** for L with $O(\log n)$ states (this will be later in the course).

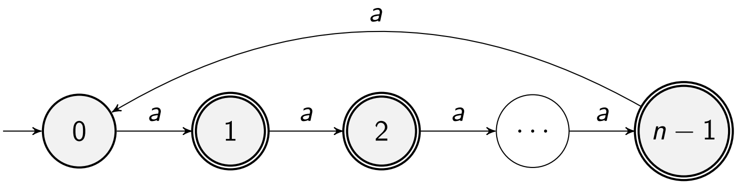
a is n From the End

$$L_n = \Sigma^* a \Sigma^n.$$

1. Every DFA for L **requires** $\geq 2^{n+1}$ states.
2. **There is** an NFA for L with $n+2$ states.
3. **There is a CFG** for L with $O(\log n)$ states (this will be later in the course).

There are examples where the NFA has n states and any DFA requires 2^n states but they are messy so we omit.

$L = \{a^i : i \not\equiv 0 \pmod{n}\}$



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

Note

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

Note

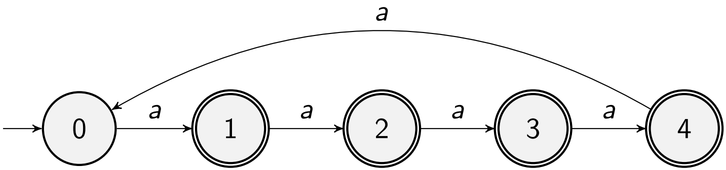
1. If $i \not\equiv 0 \pmod{5}$ then $a^i \in L$ (Since $35 \equiv 0 \pmod{5}$.)

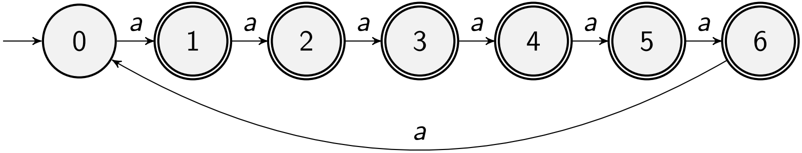
$L = \{a^i : i \not\equiv 0 \pmod{35}\}$

Note

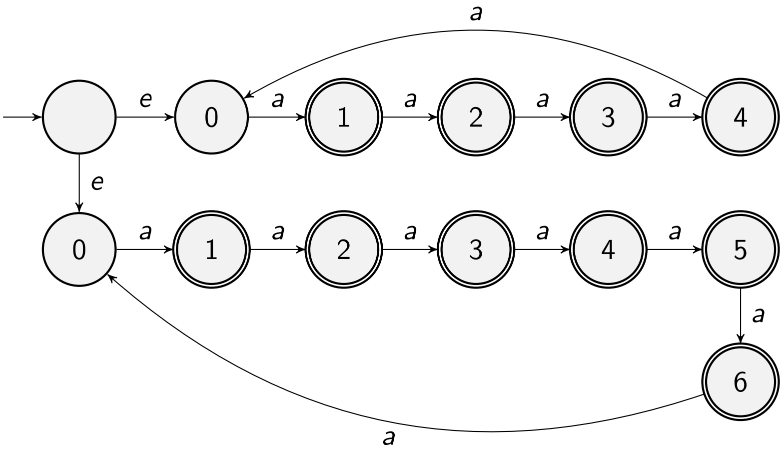
1. If $i \not\equiv 0 \pmod 5$ then $a^i \in L$ (Since $35 \equiv 0 \pmod 5$.)
2. If $i \not\equiv 0 \pmod 7$ then $a^i \in L$ (Since $35 \equiv 0 \pmod 7$.)

Two Helpful DFAs





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



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

To prove that the NFA in the last slide works we need the following claim:

Claim If $i \not\equiv 0 \pmod{35}$ then either

$i \not\equiv 0 \pmod{5}$ OR $i \not\equiv 0 \pmod{7}$.

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

To prove that the NFA in the last slide works we need the following claim:

Claim If $i \not\equiv 0 \pmod{35}$ then either

$i \not\equiv 0 \pmod{5}$ OR $i \not\equiv 0 \pmod{7}$.

We will restate it and prove it on the next slide.

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

Claim If $i \not\equiv 0 \pmod{35}$ then either

$i \not\equiv 0 \pmod{5}$ OR $i \not\equiv 0 \pmod{7}$.

Pf We prove contrapositive.

Assume $i \equiv 0 \pmod{5}$ AND $i \equiv 0 \pmod{7}$.

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

Claim If $i \not\equiv 0 \pmod{35}$ then either

$i \not\equiv 0 \pmod{5}$ OR $i \not\equiv 0 \pmod{7}$.
Pf We prove contrapositive.
Assume $i \equiv 0 \pmod{5}$ AND $i \equiv 0 \pmod{7}$.
There exists x such that $i = 5x$

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

Claim If $i \not\equiv 0 \pmod{35}$ then either

$i \not\equiv 0 \pmod{5}$ OR $i \not\equiv 0 \pmod{7}$.

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 $i = 7y$

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

Claim If $i \not\equiv 0 \pmod{35}$ then either

$i \not\equiv 0 \pmod{5}$ OR $i \not\equiv 0 \pmod{7}$.

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 $7y$.

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

Claim If $i \not\equiv 0 \pmod{35}$ then either
$i \not\equiv 0 \pmod{5}$ OR $i \not\equiv 0 \pmod{7}$.
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.

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

Claim If $i \not\equiv 0 \pmod{35}$ then either

$i \not\equiv 0 \pmod{5}$ OR $i \not\equiv 0 \pmod{7}$.

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 $i = 7y = 35z$.

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

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

DFA for L requires 35 states.

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

DFA for L requires 35 states.

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

Does this Lang have a Small NFA?

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

Any DFA for L requires 1001 states.

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

Any DFA for L requires 1001 states.
Is there an NFA with fewer states?

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

Any DFA for L requires 1001 states.
Is there an NFA with fewer states?

Vote

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

Any DFA for L requires 1001 states.
Is there an NFA with fewer states?

Vote

1. Any NFA for L **requires** 1001 states.

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

Any DFA for L requires 1001 states.
Is there an NFA with fewer states?

Vote

1. Any NFA for L **requires** 1001 states.
2. There is an NFA For L with slightly less than 1001 and this is roughly optimal (For example there is an NFA with 995 states.)

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

Any DFA for L requires 1001 states.
Is there an NFA with fewer states?

Vote

1. Any NFA for L **requires** 1001 states.
2. There is an NFA For L with slightly less than 1001 and this is roughly optimal (For example there is an NFA with 995 states.)
3. There is an NFA for L with substantially less. (For example there is an NFA with 500 states.)

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

Any DFA for L requires 1001 states.
Is there an NFA with fewer states?

Vote

1. Any NFA for L **requires** 1001 states.
2. There is an NFA For L with slightly less than 1001 and this is roughly optimal (For example there is an NFA with 995 states.)
3. There is an NFA for L with substantially less. (For example there is an NFA with 500 states.)

I will put you into breakout rooms for this.

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

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

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

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

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

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

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.

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

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 $n = 32(x' + 32) + 33(y' - 31)$.

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

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 $n = 32(x' + 32) + 33(y' - 31)$.
Case 3 $x' \leq 0$ and $y' \leq 30$. Then
$n = 32x' + 33y' \leq 33 \times 30 = 990 < 993$, 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

$$991 = 32x + 33y$$

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

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

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

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

$$991 = 32x + 33y \geq 32x + 33 \times 31 = 1023$$ **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 $n = 32x + 33y + 9$.

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,

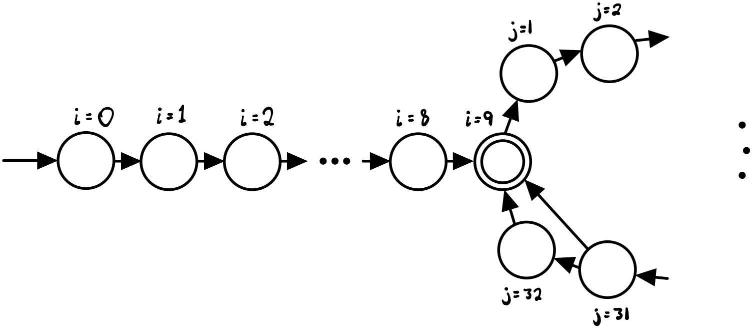
$$(\exists x, y)[1000 = 32x + 33y + 9]$$

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

This contradicts prior Thm.

There Exists an NFA for $\{a^i : i \geq 1001\}$

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: $9 + 33 = 42$.

Still Need $\{a^i : i \leq 999\}$

Idea

Still Need $\{a^i : i \le 999\}$

Idea

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

Still Need $\{a^i : i \le 999\}$

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 $\{a^i : i \le 999\}$

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 $\{a^i : i \le 999\}$

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 $\{a^i : i \le 999\}$

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 $\{a^i : i \le 999\}$

Idea

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

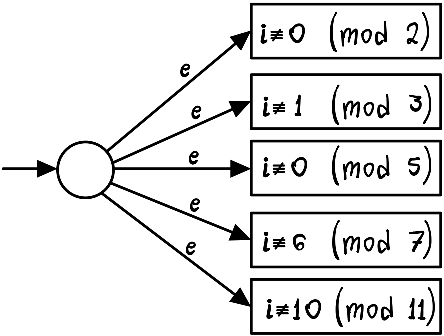
$1000 \equiv 1 \pmod 3$ SO want to accept $\{a^i : i \not\equiv 1 \pmod 3\}$.
3-state DFA.

$1000 \equiv 0 \pmod 5$ 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.

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}

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

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

NFA for $\{a^i : i \leq 999\}$ 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 $i \equiv 20 \pmod{35}$.

$i \equiv 1 \pmod{11}$

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

$i \equiv 1 \pmod{11}$

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 Spring of 2015, 2016, 2017, 2018, 2019, 2020, and now 2021 I have given this problem to the students in CMSC 452.

Interesting Problem, Profound Moral

1. In the Spring of 2015, 2016, 2017, 2018, 2019, 2020, and now 2021 I have given this problem to the students in CMSC 452.
2. Every year almost everyone thinks **The NFA requires $\sim n$ states**. Yaelle and Saadiq thought it!

Interesting Problem, Profound Moral

1. In the Spring of 2015, 2016, 2017, 2018, 2019, 2020, and now 2021 I have given this problem to the students in CMSC 452.
2. Every year almost everyone thinks **The NFA requires $\sim n$ states**. Yaelle and Saadiq thought it!
3. Why is this? They did not know the trick.

Interesting Problem, Profound Moral

1. In the Spring of 2015, 2016, 2017, 2018, 2019, 2020, and now 2021 I have given this problem to the students in CMSC 452.
2. Every year almost everyone thinks **The NFA requires $\sim n$ states**. Yaelle and Saadiq thought it!
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.

1. This was the first 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.

1. This was the first lecture on NP-completeness.
2. 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.

1. This was the first lecture on NP-completeness.
2. Just because you cannot think of an algorithm for SAT in P does not mean that there is not one.
3. 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.

1. This was the first lecture on NP-completeness.
2. Just because you cannot think of an algorithm for SAT in P does not mean that there is not one.
3. It is possible that someone will come up with a technique you didn't think of, or some use math you did not know.
4. 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.

1. This was the first lecture on NP-completeness.
2. Just because you cannot think of an algorithm for SAT in P does not mean that there is not one.
3. It is possible that someone will come up with a technique you didn't think of, or some use math you did not know.
4. 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.

1. This was the first lecture on NP-completeness.
2. Just because you cannot think of an algorithm for SAT in P does not mean that there is not one.
3. It is possible that someone will come up with a technique you didn't think of, or some use math you did not know.
4. 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.

1. This was the first lecture on NP-completeness.
2. Just because you cannot think of an algorithm for SAT in P does not mean that there is not one.
3. It is possible that someone will come up with a technique you didn't think of, or some use math you did not know.
4. 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.

1. This was the first lecture on NP-completeness.
2. Just because you cannot think of an algorithm for SAT in P does not mean that there is not one.
3. It is possible that someone will come up with a technique you didn't think of, or some use math you did not know.
4. 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.
5. **Upshot** Lower bounds are hard to prove since they must rule out techniques you have not through of.

This was NOT a lecture on Size of NFAs

You thought this was a lecture on sizes of NFAs.

It was not.

1. This was the first lecture on NP-completeness.
2. Just because you cannot think of an algorithm for SAT in P does not mean that there is not one.
3. It is possible that someone will come up with a technique you didn't think of, or some use math you did not know.
4. 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.
5. **Upshot** Lower bounds are hard to prove since they must rule out techniques you have not through of.
6. Respect the difficulty of lower bounds!

Can We Do Better than 70 States?

For $\{a^i : i \neq 1000\}$, we had a 70 state NFA.

Can we do better?

Can We Do Better than 70 States?

For $\{a^i : i \neq 1000\}$, we had a 70 state NFA.

Can we do better?

Vote:

1. 70 is optimal
2. Can do between 60 and 69
3. Can do between 50 and 59
4. Unknown to science!

Can We Do Better than 70 States?

For $\{a^i : i \neq 1000\}$, we had a 70 state NFA.

Can we do better?

Vote:

1. 70 is optimal
2. Can do between 60 and 69
3. Can do between 50 and 59
4. Unknown to science!

Answer: This can be improved to only 59 states.

See next slide.

Two Tricks Used To Get it to 59 States

1. To get $\{a^i : i \le 999\}$, 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 $\{a^i : i \le 999\}$, 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 $\{a^i : i \le 999\}$, 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 $\{a^i : i \ne n\}$ 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 $xy - x - y = cx + dy$.

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 $x, y \sim \sqrt{n}$.

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 $x, y \sim \sqrt{n}$.
Want to get $xy - x - y \le n$ so can use the tail to get $xy - x - y + t = n$.

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 $x, y \sim \sqrt{n}$.
Want to get $xy - x - y \leq n$ so can use the tail to get
$xy - x - y + t = n$.
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

I have not filled in the 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

I have not filled in the details, but from the last two slides you can get that

$$\{a^i : i \neq n\}$$

has an NFA of size $\leq 2\sqrt{n} + (\log n)^2 \log\log n$.

One can get it down to $\leq \sqrt{n} + (\log n)^2 \log\log n$.

From the Last Two Slides

I have not filled in the details, but from the last two slides you can get that

$$\{a^i : i \neq n\}$$

has an NFA of size $\leq 2\sqrt{n} + (\log n)^2 \log\log n$.

One can get it down to $\leq \sqrt{n} + (\log n)^2 \log\log n$.
(Paper by Gasarch-Metz-Xu-Shen-Zbarsky.)