

Lecture 32

NC and AC: Subclasses of $P_{/poly}$

Depth of a Circuit

Depth of a Circuit

Definition: The **depth** of a circuit is the **length of the longest directed path** from an input node

Depth of a Circuit

Definition: The **depth** of a circuit is the **length of the longest directed path** from an input node to the output node.

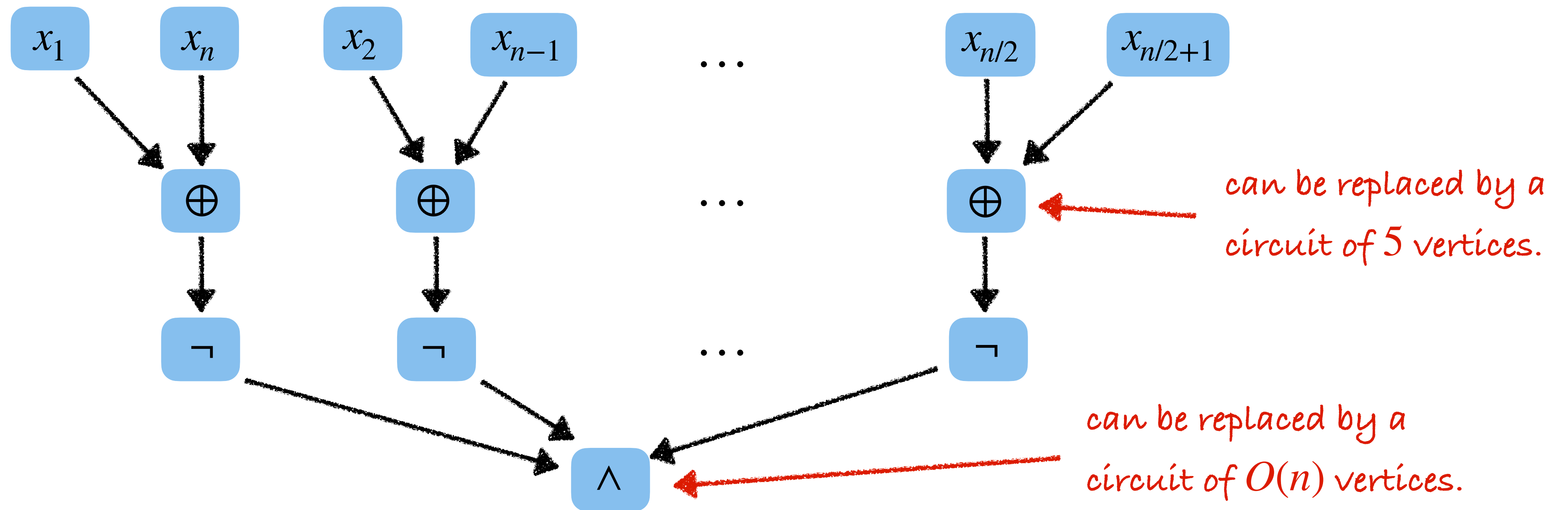
Depth of a Circuit

Definition: The **depth** of a circuit is the **length of the longest directed path** from an input node to the output node.

Example: Depth of *PALIN*'s circuit was

Depth of a Circuit

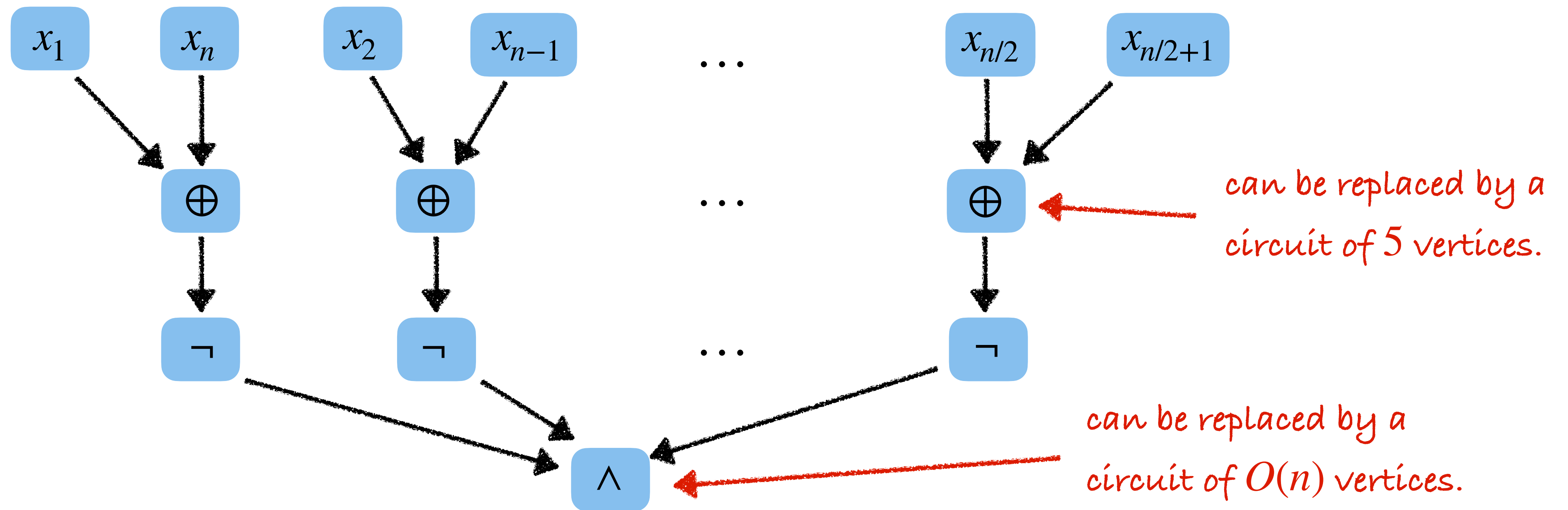
Definition: The **depth** of a circuit is the **length of the longest directed path** from an input node to the output node.



Example: Depth of *PALIN*'s circuit was

Depth of a Circuit

Definition: The **depth** of a circuit is the **length of the longest directed path** from an input node to the output node.



Example: Depth of *PALIN*'s circuit was $O(\log n)$.

NC and AC

NC and AC

Definition: For every $d \geq 0$, a language L is in NC^d

NC and AC

Definition: For every $d \geq 0$, a language L is in NC^d if L can be decided by a family of circuits

NC and AC

Definition: For every $d \geq 0$, a language L is in NC^d if L can be decided by a family of circuits $\{C_n\}_{n \in \mathbb{N}}$, where C_n has *poly*(n)-size and $O(\log^d n)$ depth.

NC and AC

Definition: For every $d \geq 0$, a language L is in NC^d if L can be decided by a family of circuits $\{C_n\}_{n \in \mathbb{N}}$, where C_n has *poly(n)-size* and $O(\log^d n)$ depth.

Definition: $\text{NC} = \bigcup_{i \geq 0} \text{NC}^i$ (NC stands for Nick's Class)

NC and AC

Definition: For every $d \geq 0$, a language L is in NC^d if L can be decided by a family of circuits $\{C_n\}_{n \in \mathbb{N}}$, where C_n has *poly*(n)-size and $O(\log^d n)$ depth.

Definition: $\text{NC} = \bigcup_{i \geq 0} \text{NC}^i$ (NC stands for Nick's Class)

Definition: For every $d \geq 0$, a language L is in AC^d

NC and AC

Definition: For every $d \geq 0$, a language L is in NC^d if L can be decided by a family of circuits $\{C_n\}_{n \in \mathbb{N}}$, where C_n has *poly(n)-size* and $O(\log^d n)$ depth.

Definition: $\text{NC} = \bigcup_{i \geq 0} \text{NC}^i$ (NC stands for Nick's Class)

Definition: For every $d \geq 0$, a language L is in AC^d if L can be decided by a family of circuits

NC and AC

Definition: For every $d \geq 0$, a language L is in \mathbf{NC}^d if L can be decided by a family of circuits $\{C_n\}_{n \in \mathbb{N}}$, where C_n has *poly(n)-size* and $O(\log^d n)$ depth.

Definition: $\mathbf{NC} = \bigcup_{i \geq 0} \mathbf{NC}^i$ (NC stands for Nick's Class)

Definition: For every $d \geq 0$, a language L is in \mathbf{AC}^d if L can be decided by a family of circuits $\{C_n\}_{n \in \mathbb{N}}$, where C_n has unbounded fan-in, *poly(n)-size* and $O(\log^d n)$ depth.

NC and AC

Definition: For every $d \geq 0$, a language L is in \mathbf{NC}^d if L can be decided by a family of circuits $\{C_n\}_{n \in \mathbb{N}}$, where C_n has *poly(n)-size* and $O(\log^d n)$ depth.

Definition: $\mathbf{NC} = \bigcup_{i \geq 0} \mathbf{NC}^i$ (NC stands for Nick's Class)

Definition: For every $d \geq 0$, a language L is in \mathbf{AC}^d if L can be decided by a family of circuits $\{C_n\}_{n \in \mathbb{N}}$, where C_n has unbounded fan-in, *poly(n)-size* and $O(\log^d n)$ depth.

Definition: $\mathbf{AC} = \bigcup_{i \geq 0} \mathbf{AC}^i$ (AC stands for Alternating's Class)

NC and AC

Definition: For every $d \geq 0$, a language L is in \mathbf{NC}^d if L can be decided by a family of circuits $\{C_n\}_{n \in \mathbb{N}}$, where C_n has *poly(n)-size* and $O(\log^d n)$ depth.

Definition: $\mathbf{NC} = \bigcup_{i \geq 0} \mathbf{NC}^i$ (NC stands for Nick's Class)

Definition: For every $d \geq 0$, a language L is in \mathbf{AC}^d if L can be decided by a family of circuits $\{C_n\}_{n \in \mathbb{N}}$, where C_n has unbounded fan-in, *poly(n)-size* and $O(\log^d n)$ depth.

Definition: $\mathbf{AC} = \bigcup_{i \geq 0} \mathbf{AC}^i$ (AC stands for Alternating's Class)

Definition: *uniform-NC* and *uniform-AC* require circuits to be logspace uniform.

Motivation for NC and AC

Motivation for NC and AC

Why should we study **NC** and **AC**:

Motivation for NC and AC

Why should we study **NC** and **AC**:

- Showing **NP** $\not\subseteq$ **NC** might be easier than **NP** $\not\subseteq$ **P**/_{poly} and may give insight to prove **NP** $\not\subseteq$ **P**/_{poly}.

Motivation for NC and AC

Why should we study **NC** and **AC**:

- Showing $\mathbf{NP} \not\subseteq \mathbf{NC}$ might be easier than $\mathbf{NP} \not\subseteq \mathbf{P}/\text{poly}$ and may give insight to prove $\mathbf{NP} \not\subseteq \mathbf{P}/\text{poly}$.
- **NC** and **AC** correspond to efficient parallel computation.

Observation on NC and AC

Observation on NC and AC

- Output of an \mathbf{NC}^0 circuit depends on the constant number of input bits.

Observation on NC and AC

- Output of an \mathbf{NC}^0 circuit depends on the constant number of input bits.

Example: $L = \{1^n \mid n \geq 1\}$ is not in \mathbf{NC}^0 .

Observation on NC and AC

- Output of an \mathbf{NC}^0 circuit depends on the constant number of input bits.

Example: $L = \{1^n \mid n \geq 1\}$ is not in \mathbf{NC}^0 .

- $\mathbf{NC}^i \subseteq \mathbf{AC}^i \subseteq \mathbf{NC}^{i+1}$.

Observation on NC and AC

- Output of an \mathbf{NC}^0 circuit depends on the constant number of input bits.

Example: $L = \{1^n \mid n \geq 1\}$ is not in \mathbf{NC}^0 .

- $\mathbf{NC}^i \subseteq \mathbf{AC}^i \subseteq \mathbf{NC}^{i+1}$.


trivial

Observation on NC and AC

- Output of an \mathbf{NC}^0 circuit depends on the constant number of input bits.

Example: $L = \{1^n \mid n \geq 1\}$ is not in \mathbf{NC}^0 .

- $\mathbf{NC}^i \subseteq \mathbf{AC}^i \subseteq \mathbf{NC}^{i+1}$.


trivial

 a vertex with unbounded fan-in can be replaced by an $O(\log n)$ depth circuit.

Observation on NC and AC

- Output of an \mathbf{NC}^0 circuit depends on the constant number of input bits.

Example: $L = \{1^n \mid n \geq 1\}$ is not in \mathbf{NC}^0 .

- $\mathbf{NC}^i \subseteq \mathbf{AC}^i \subseteq \mathbf{NC}^{i+1}$. Thus, $\mathbf{NC} = \mathbf{AC}$.


trivial

 a vertex with unbounded fan-in can be replaced by an $O(\log n)$ depth circuit.

Observation on NC and AC

- Output of an \mathbf{NC}^0 circuit depends on the constant number of input bits.

Example: $L = \{1^n \mid n \geq 1\}$ is not in \mathbf{NC}^0 .

- $\mathbf{NC}^i \subseteq \mathbf{AC}^i \subseteq \mathbf{NC}^{i+1}$. Thus, $\mathbf{NC} = \mathbf{AC}$.


trivial


a vertex with unbounded fan-in can be replaced by an $O(\log n)$ depth circuit.

- $\mathbf{NC}^0 \subset \mathbf{AC}^0 \subset \mathbf{NC}^1$.

Observation on NC and AC

- Output of an \mathbf{NC}^0 circuit depends on the constant number of input bits.


Example: $L = \{1^n \mid n \geq 1\}$ is not in \mathbf{NC}^0 .

- $\mathbf{NC}^i \subseteq \mathbf{AC}^i \subseteq \mathbf{NC}^{i+1}$. Thus, $\mathbf{NC} = \mathbf{AC}$.


trivial


a vertex with unbounded fan-in can be replaced by an $O(\log n)$ depth circuit.

- $\mathbf{NC}^0 \subset \mathbf{AC}^0 \subset \mathbf{NC}^1$.


L of above example

Observation on NC and AC

- Output of an \mathbf{NC}^0 circuit depends on the constant number of input bits.

Example: $L = \{1^n \mid n \geq 1\}$ is not in \mathbf{NC}^0 .

- $\mathbf{NC}^i \subseteq \mathbf{AC}^i \subseteq \mathbf{NC}^{i+1}$. Thus, $\mathbf{NC} = \mathbf{AC}$.

trivial

a vertex with unbounded fan-in can be replaced by an $O(\log n)$ depth circuit.

- $\mathbf{NC}^0 \subset \mathbf{AC}^0 \subset \mathbf{NC}^1$.

L of above example

PARITY is in \mathbf{NC}^1 but not in \mathbf{AC}^0 .

uniform-NC¹ vs L

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof:

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

We will construct a logspace algorithm A for L .

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

We will construct a logspace algorithm A for L .

$A(x)$:

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

We will construct a logspace algorithm A for L .

$A(x)$:

let C = circuit for $|x|$ length input.

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

We will construct a logspace algorithm A for L .

$A(x)$:

let C = circuit for $|x|$ length input.

V = output vertex of C

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

We will construct a logspace algorithm A for L .

$A(x)$:

let C = circuit for $|x|$ length input.

V = output vertex of C

output $B(V, x)$

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

We will construct a logspace algorithm A for L .

$B(V, x)$:

$A(x)$:

let C = circuit for $|x|$ length input.

V = output vertex of C

output $B(V, x)$

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

We will construct a logspace algorithm A for L .

$A(x)$:

let C = circuit for $|x|$ length input.

V = output vertex of C

output $B(V, x)$

$B(V, x)$:

if V is an input vertex

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

We will construct a logspace algorithm A for L .

$A(x)$:

let C = circuit for $|x|$ length input.

V = output vertex of C

output $B(V, x)$

$B(V, x)$:

if V is an input vertex

return appropriate x_i

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

We will construct a logspace algorithm A for L .

$A(x)$:

let C = circuit for $|x|$ length input.

V = output vertex of C

output $B(V, x)$

$B(V, x)$:

if V is an input vertex

return appropriate x_i

let V_1, V_2 = vertices with an edge to V

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

We will construct a logspace algorithm A for L .

$A(x)$:

let C = circuit for $|x|$ length input.

V = output vertex of C

output $B(V, x)$

$B(V, x)$:

if V is an input vertex

return appropriate x_i

let V_1, V_2 = vertices with an edge to V

op = boolean operator of V

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

We will construct a logspace algorithm A for L .

$A(x)$:

let C = circuit for $|x|$ length input.

V = output vertex of C

output $B(V, x)$

$B(V, x)$:

if V is an input vertex

return appropriate x_i

let V_1, V_2 = vertices with an edge to V

op = boolean operator of V

return $B(V_1, x) op B(V_2, x)$

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

We will construct a logspace algorithm A for L .

$A(x)$:

let C = circuit for $|x|$ length input.

V = output vertex of C

output $B(V, x)$

$B(V, x)$:

if V is an input vertex

return appropriate x_i

let V_1, V_2 = vertices with an edge to V

op = boolean operator of V

return $B(V_1, x) op B(V_2, x)$

Space Complexity of B :

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

We will construct a logspace algorithm A for L .

$A(x)$:

let C = circuit for $|x|$ length input.

V = output vertex of C

output $B(V, x)$

$B(V, x)$:

if V is an input vertex

return appropriate x_i

let V_1, V_2 = vertices with an edge to V

op = boolean operator of V

return $B(V_1, x) op B(V_2, x)$

Space Complexity of B : Total $O(\log n)$ recursion levels and at every level it is storing

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

We will construct a logspace algorithm A for L .

$A(x)$:

let C = circuit for $|x|$ length input.

V = output vertex of C

output $B(V, x)$

$B(V, x)$:

if V is an input vertex

return appropriate x_i

let V_1, V_2 = vertices with an edge to V

op = boolean operator of V

return $B(V_1, x) op B(V_2, x)$

Space Complexity of B : Total $O(\log n)$ recursion levels and at every level it is storing **constant information**.

uniform-NC¹ vs L

Theorem: uniform-NC¹ \subseteq L.

Proof: Let L be in uniform-NC¹.

We will construct a logspace algorithm A for L .

$A(x)$:

let C = circuit for $|x|$ length input.

V = output vertex of C

output $B(V, x)$

$B(V, x)$:

if V is an input vertex

return appropriate x_i

let V_1, V_2 = vertices with an edge to V

op = boolean operator of V

return $B(V_1, x) op B(V_2, x)$

Space Complexity of B : Total $O(\log n)$ recursion levels and at every level it is storing **constant information.**



uniform-AC¹ vs NL

uniform-AC¹ vs NL

Theorem: $NL \subseteq \text{uniform-AC}^1$.

uniform-AC¹ vs NL

Theorem: $NL \subseteq \text{uniform-AC}^1$.

Proof:

uniform-AC¹ vs NL

Theorem: $NL \subseteq \text{uniform-AC}^1$.

Proof: Let L be in NL and M be a logspace NTM that decides it.

uniform-AC¹ vs NL

Theorem: $NL \subseteq \text{uniform-AC}^1$.

Proof: Let L be in NL and M be a logspace NTM that decides it.

Let A_i denote the $N \times N$ matrix, where $N = \#$ of configurations of M on an input x , s.t.

uniform-AC¹ vs NL

Theorem: $NL \subseteq \text{uniform-AC}^1$.

Proof: Let L be in NL and M be a logspace NTM that decides it.

Let A_l denote the $N \times N$ matrix, where $N = \#$ of configurations of M on an input x , s.t.

$A_l[i, j] = 1$ iff \exists a path of length at most 2^l from i to j in $G_{M,x}$.

uniform-AC¹ vs NL

Theorem: $NL \subseteq \text{uniform-AC}^1$.

Proof: Let L be in NL and M be a logspace NTM that decides it.

Let A_l denote the $N \times N$ matrix, where $N = \#$ of configurations of M on an input x , s.t.

$A_l[i, j] = 1$ iff \exists a path of length at most 2^l from i to j in $G_{M,x}$.

How can we compute A_{l+1} from A_l ?

uniform-AC¹ vs NL

Theorem: $NL \subseteq \text{uniform-AC}^1$.

Proof: Let L be in NL and M be a logspace NTM that decides it.

Let A_l denote the $N \times N$ matrix, where $N = \#$ of configurations of M on an input x , s.t.

$A_l[i, j] = 1$ iff \exists a path of length at most 2^l from i to j in $G_{M,x}$.

How can we compute A_{l+1} from A_l ?

$$A_{l+1}[i, j] =$$

uniform-AC¹ vs NL

Theorem: NL \subseteq uniform-AC¹.

Proof: Let L be in NL and M be a logspace NTM that decides it.

Let A_l denote the $N \times N$ matrix, where $N = \#$ of configurations of M on an input x , s.t.

$A_l[i, j] = 1$ iff \exists a path of length at most 2^l from i to j in $G_{M,x}$.

How can we compute A_{l+1} from A_l ?

$$A_{l+1}[i, j] = \bigvee_{1 \leq k \leq N} (A_l[i, k] \wedge A_l[k, j])$$

uniform-AC¹ vs NL

Theorem: NL \subseteq uniform-AC¹.

Proof: Let L be in NL and M be a logspace NTM that decides it.

Let A_l denote the $N \times N$ matrix, where $N = \#$ of configurations of M on an input x , s.t.

$A_l[i, j] = 1$ iff \exists a path of length at most 2^l from i to j in $G_{M,x}$.

How can we compute A_{l+1} from A_l ?

$$A_{l+1}[i, j] = \bigvee_{1 \leq k \leq N} (A_l[i, k] \wedge A_l[k, j])$$

Building the circuit for L :

uniform-AC¹ vs NL

Theorem: NL \subseteq uniform-AC¹.

Proof: Let L be in NL and M be a logspace NTM that decides it.

Let A_l denote the $N \times N$ matrix, where $N = \#$ of configurations of M on an input x , s.t.

$A_l[i, j] = 1$ iff \exists a path of length at most 2^l from i to j in $G_{M,x}$.

How can we compute A_{l+1} from A_l ?

$$A_{l+1}[i, j] = \bigvee_{1 \leq k \leq N} (A_l[i, k] \wedge A_l[k, j])$$

Building the circuit for L :

- Have one layer for every $l \in [0, \log N]$.

uniform-AC¹ vs NL

Theorem: NL \subseteq uniform-AC¹.

Proof: Let L be in NL and M be a logspace NTM that decides it.

Let A_l denote the $N \times N$ matrix, where $N = \#$ of configurations of M on an input x , s.t.

$A_l[i, j] = 1$ iff \exists a path of length at most 2^l from i to j in $G_{M,x}$.

How can we compute A_{l+1} from A_l ?

$$A_{l+1}[i, j] = \bigvee_{1 \leq k \leq N} (A_l[i, k] \wedge A_l[k, j])$$

Building the circuit for L :

- Have one layer for every $l \in [0, \log N]$.
- In the l th layer, keep one vertex for every (i, j) th entry of A_l .

uniform-AC¹ vs NL

Theorem: NL \subseteq uniform-AC¹.

Proof: Let L be in NL and M be a logspace NTM that decides it.

Let A_l denote the $N \times N$ matrix, where $N = \#$ of configurations of M on an input x , s.t.

$$A_l[i, j] = 1 \text{ iff } \exists \text{ a path of length at most } 2^l \text{ from } i \text{ to } j \text{ in } G_{M,x}.$$

How can we compute A_{l+1} from A_l ?

$$A_{l+1}[i, j] = \bigvee_{1 \leq k \leq N} (A_l[i, k] \wedge A_l[k, j])$$

Building the circuit for L :

- Have one layer for every $l \in [0, \log N]$.
- In the l th layer, keep one vertex for every (i, j) th entry of A_l .
- Arrange wires/edges from l th layer to $(l + 1)$ th layer according to this formula.

uniform-AC¹ vs NL

Theorem: NL \subseteq uniform-AC¹.

Proof: Let L be in NL and M be a logspace NTM that decides it.

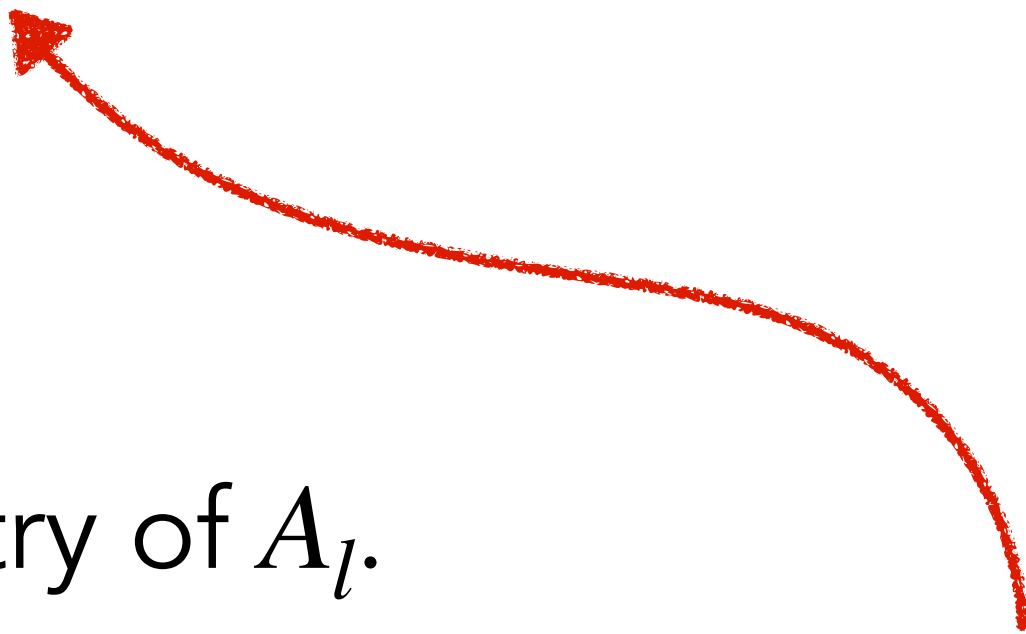
Let A_l denote the $N \times N$ matrix, where $N = \#$ of configurations of M on an input x , s.t.

$A_l[i, j] = 1$ iff \exists a path of length at most 2^l from i to j in $G_{M,x}$.

How can we compute A_{l+1} from A_l ?

$$A_{l+1}[i, j] = \bigvee_{1 \leq k \leq N} (A_l[i, k] \wedge A_l[k, j])$$

Building the circuit for L :

- Have one layer for every $l \in [0, \log N]$.
 - In the l th layer, keep one vertex for every (i, j) th entry of A_l .
 - Arrange wires/edges from l th layer to $(l + 1)$ th layer according to this formula.
- 

uniform-AC¹ vs NL

Theorem: $NL \subseteq \text{uniform-AC}^1$.

Proof: Let L be in NL and M be a logspace NTM that decides it.

Let A_l denote the $N \times N$ matrix, where $N = \#$ of configurations of M on an input x , s.t.

$$A_l[i, j] = 1 \text{ iff } \exists \text{ a path of length at most } 2^l \text{ from } i \text{ to } j \text{ in } G_{M,x}.$$

How can we compute A_{l+1} from A_l ?

$$A_{l+1}[i, j] = \bigvee_{1 \leq k \leq N} (A_l[i, k] \wedge A_l[k, j])$$

Building the circuit for L :

- Have one layer for every $l \in [0, \log N]$.
- In the l th layer, keep one vertex for every (i, j) th entry of A_l .
- Arrange wires/edges from l th layer to $(l + 1)$ th layer according to this formula.

edges for 0th layer
require some work



uniform-AC¹ vs NL

Theorem: NL \subseteq uniform-AC¹.

Proof: Let L be in NL and M be a logspace NTM that decides it.

Let A_l denote the $N \times N$ matrix, where $N = \#$ of configurations of M on an input x , s.t.

$A_l[i, j] = 1$ iff \exists a path of length at most 2^l from i to j in $G_{M,x}$.


How can we compute A_{l+1} from A_l ?

$$A_{l+1}[i, j] = \bigvee_{1 \leq k \leq N} (A_l[i, k] \wedge A_l[k, j])$$

Building the circuit for L :

- Have one layer for every $l \in [0, \log N]$.
- In the l th layer, keep one vertex for every (i, j) th entry of A_l .
- Arrange wires/edges from l th layer to $(l + 1)$ th layer according to this formula.
- Keep the (start config, acc. config.) vertex in the last layer as output vertex.

edges for 0th layer
require some work



uniform-AC¹ vs NL

Theorem: NL \subseteq uniform-AC¹.

Proof: Let L be in NL and M be a logspace NTM that decides it.

Let A_l denote the $N \times N$ matrix, where $N = \#$ of configurations of M on an input x , s.t.

$A_l[i, j] = 1$ iff \exists a path of length at most 2^l from i to j in $G_{M,x}$.

How can we compute A_{l+1} from A_l ?

$$A_{l+1}[i, j] = \bigvee_{1 \leq k \leq N} (A_l[i, k] \wedge A_l[k, j])$$

Building the circuit for L :

- Have one layer for every $l \in [0, \log N]$.
- In the l th layer, keep one vertex for every (i, j) th entry of A_l .
- Arrange wires/edges from l th layer to $(l + 1)$ th layer according to this formula.
- Keep the (start config, acc. config.) vertex in the last layer as output vertex.

edges for 0th layer
require some work

