Non-Uniform Computation & Circuits

Lecture 10

Wherein every language can be decided

Non-Uniform Computation

Non-Uniform Computation

- Uniform: Same program for all (the infinitely many) inputs

Non-Uniform Computation

- Uniform: Same program for all (the infinitely many) inputs
- Non-uniform: A different "program" for each input size

Non-Uniform Computation

- Uniform: Same program for all (the infinitely many) inputs
- Non-uniform: A different "program" for each input size
  - Then complexity of building the program and executing the program

Non-Uniform Computation

- Uniform: Same program for all (the infinitely many) inputs
- Non-uniform: A different "program" for each input size
  - Then complexity of building the program and executing the program
  - Sometimes will focus on the latter alone

Non-Uniform Computation

- Uniform: Same program for all (the infinitely many) inputs
- Non-uniform: A different "program" for each input size
  - Then complexity of building the program and executing the program
  - Sometimes will focus on the latter alone
  - Not entirely realistic if the program family is uncomputable or very complex to compute

Non-uniform advice

Non-uniform advice

- Program: TM M and advice strings $\{A_n\}$

Non-uniform advice

- Program: TM M and advice strings $\{A_n\}$
  - M given $A_{|x|}$ along with x

Non-uniform advice

- Program: TM M and advice strings $\{A_n\}$
  - M given $A_{|x|}$ along with x
  - A_n can be the program for inputs of size n

Non-uniform advice

- Program: TM M and advice strings $\{A_n\}$
  - M given $A_{|x|}$ along with x
  - A_n can be the program for inputs of size n
  - $|A_n|=2^n$ is sufficient

Non-uniform advice

- Program: TM M and advice strings $\{A_n\}$
  - M given $A_{|x|}$ along with x
  - A_n can be the program for inputs of size n
  - $|A_n|=2^n$ is sufficient
  - But $\{A_n\}$ can be uncomputable (even if just one bit long)

Non-uniform advice

- Program: TM M and advice strings $\{A_n\}$
  - M given $A_{|x|}$ along with x
  - A_n can be the program for inputs of size n
  - $|A_n|=2^n$ is sufficient
  - But $\{A_n\}$ can be uncomputable (even if just one bit long)
    - e.g. advice to decide undecidable unary languages

P/poly and P/log

P/poly and P/log

- DTIME(T)/a

P/poly and P/log

- DTIME(T)/a
  - Languages decided by a TM in time T(n) using non-uniform advice of length a(n)

P/poly and P/log

- DTIME(T)/a
  - Languages decided by a TM in time T(n) using non-uniform advice of length a(n)
- P/poly = $\cup_{c,d,k>0}$ DTIME(kn^c)/kn^d

P/poly and P/log

- DTIME(T)/a
  - Languages decided by a TM in time T(n) using non-uniform advice of length a(n)
- P/poly = $\cup_{c,d,k>0}$ DTIME(kn^c)/kn^d
- P/log = $\cup_{c,k>0}$ DTIME(kn^c)/k log n

NP vs. P/log, P/poly

NP vs. P/log, P/poly

- P/log (or even DTIME(1)/1) has undecidable languages

NP vs. P/log, P/poly

- P/log (or even DTIME(1)/1) has undecidable languages
  - e.g. unary undecidable languages

NP vs. P/log, P/poly

- P/log (or even DTIME(1)/1) has undecidable languages
  - e.g. unary undecidable languages
  - So P/log cannot be contained in any of the uniform complexity classes

NP vs. P/log, P/poly

- P/log (or even DTIME(1)/1) has undecidable languages
  - e.g. unary undecidable languages
  - So P/log cannot be contained in any of the uniform complexity classes
- P/log contains P

NP vs. P/log, P/poly

- P/log (or even DTIME(1)/1) has undecidable languages
  - e.g. unary undecidable languages
  - So P/log cannot be contained in any of the uniform complexity classes
- P/log contains P
  - Does P/log or P/poly contain NP?

$NP \subseteq P/\log \Rightarrow NP=P$

$NP \subseteq P/log \Rightarrow NP=P$

- Recall finding witness for an NP language is Turing reducible to deciding the language

Recall

Search using Decision

- Suppose given "oracles" for deciding all NP languages, can we easily find certificates?
  - Yes! So, if decision easy (decision-oracles realizable), then search is easy too!
- Say, given x, need to find w s.t. $(x,w) \in L'$ (if such w exists)
  - consider L_1 in NP: $(x,y) \in L_1$ iff $\exists z$ s.t. $(x,yz) \in L'$. (i.e., can y be a prefix of a certificate for x).
  - Query L_1-oracle with (x,0) and (x,1). If $\exists w$, one of the two must be positive: say $(x,0) \in L_1$; then first bit of w be 0.
  - For next bit query L_1-oracle with (x,00) and (x,01)

Recall

Search using Decision

- Suppose given "oracles" for deciding all NP languages, can we easily find certificates?
  - Yes! So, if decision easy (decision-oracles re... search is easy too!

Use L_2 so that (x,z,pad) in L_2 iff (x,z) in L_1. Can query L_2 with same size instances

- Say, given x, need to find w s.t. $(x,w) \in L'$ (if s...
  - consider L_1 in NP: $(x,y) \in L_1$ iff $\exists z$ s.t. $(x,yz) \in L'$. (i.e., can y be a prefix of a certificate for x).
  - Query L_1-oracle with (x,0) and (x,1). If $\exists$w, one of the two must be positive: say $(x,0) \in L_1$; then first bit of w be 0.
  - For next bit query L_1-oracle with (x,00) and (x,01)

NP $\subseteq$ P/log $\Rightarrow$ NP=P

- Recall finding witness for an NP language is Turing reducible to deciding the language

$NP \subseteq P/log \Rightarrow NP=P$

- Recall finding witness for an NP language is Turing reducible to deciding the language
- If $NP \subseteq P/log$, then for each L in NP, there is a poly-time TM with log advice which can find witness (via self-reduction)

$NP \subseteq P/log \Rightarrow NP=P$

- Recall finding witness for an NP language is Turing reducible to deciding the language
- If $NP \subseteq P/log$, then for each L in NP, there is a poly-time TM with log advice which can find witness (via self-reduction)
- Guess advice (poly many), and for each guessed advice, run the TM and see if it finds witness

$NP \subseteq P/log \Rightarrow NP=P$

- Recall finding witness for an NP language is Turing reducible to deciding the language
- If $NP \subseteq P/log$, then for each L in NP, there is a poly-time TM with log advice which can find witness (via self-reduction)
- Guess advice (poly many), and for each guessed advice, run the TM and see if it finds witness
- If no advice worked (one of them was correct), then input not in language

$NP \subseteq P/poly \Rightarrow PH=\Sigma_2^P$

$NP \subseteq P/poly \Rightarrow PH = \Sigma_2^P$

- Will show $\Pi_2^P = \Sigma_2^P$

$NP \subseteq P/poly \Rightarrow PH=\Sigma_2^P$

- Will show $\Pi_2^P = \Sigma_2^P$
- Consider $L = \{x \mid \forall w_1\ (x,w_1) \in L'\} \in \Pi_2^P$ where $L' = \{(x,w_1) \mid \exists w_2\ F(x,w_1,w_2)\} \in NP$

$NP \subseteq P/poly \Rightarrow PH=\Sigma_2^P$

- Will show $\Pi_2^P = \Sigma_2^P$
- Consider $L = \{x|\ \forall w_1\ (x,w_1) \in L'\ \} \in \Pi_2^P$ where $L' = \{(x,w_1)|\ \exists w_2\ F(x,w_1,w_2)\} \in NP$
  - If $NP \subseteq P/poly$ then consider M with advice $\{A_n\}$ which finds witness for L': i.e. if $(x,w_1) \in L'$, then $M(x,w_1; A_n)$ outputs a witness w_2 s.t. $F(x,w_1,w_2)$

$NP \subseteq P/poly \Rightarrow PH=\Sigma_2^P$

- Will show $\Pi_2^P = \Sigma_2^P$
- Consider $L = \{x | \forall w_1\ (x,w_1) \in L' \} \in \Pi_2^P$ where $L' = \{(x,w_1) | \exists w_2\ F(x,w_1,w_2)\} \in NP$
    - If $NP \subseteq P/poly$ then consider M with advice $\{A_n\}$ which finds witness for L': i.e. if $(x,w_1) \in L'$, then $M(x,w_1; A_n)$ outputs a witness w_2 s.t. $F(x,w_1,w_2)$
    - $L = \{x | \exists z\ \forall w_1\ F(x, w_1, M(x,w_1; z)) \}$

Boolean Circuits

Boolean Circuits

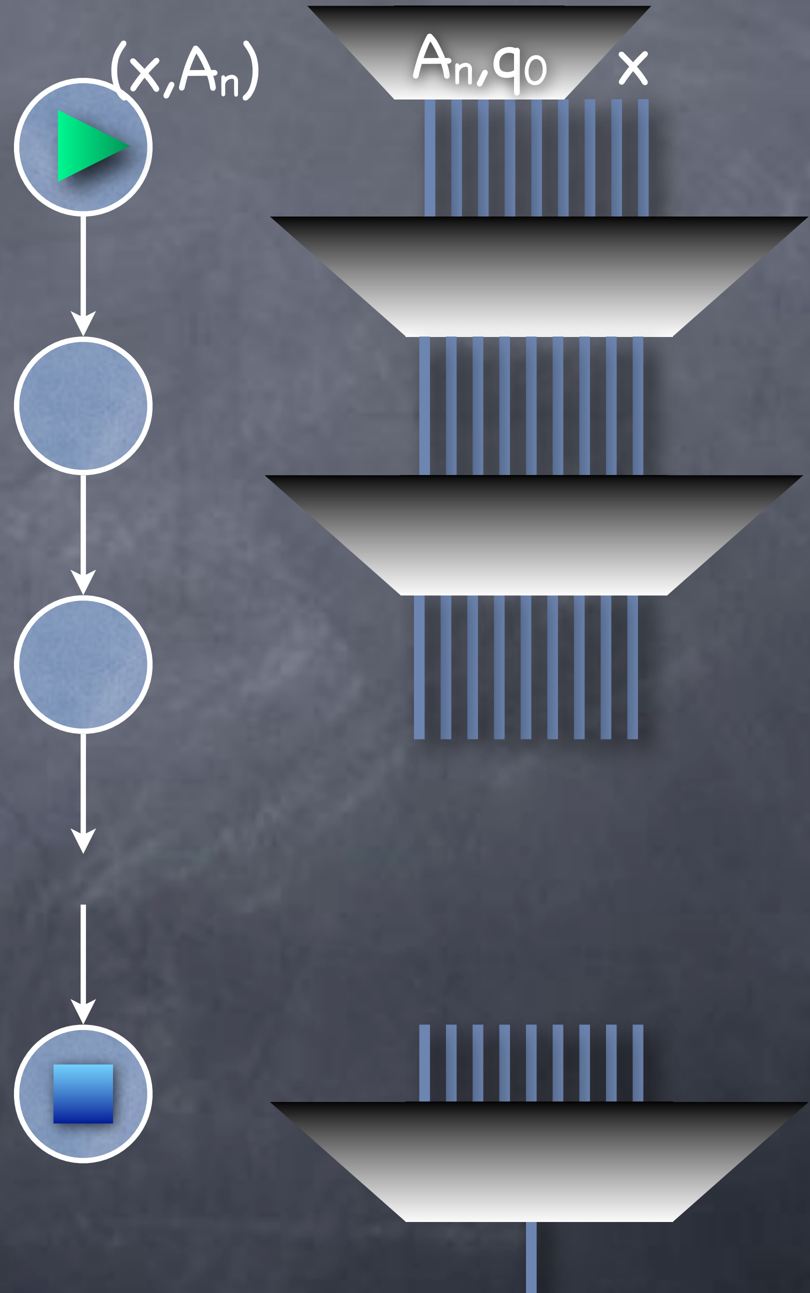
- Non-uniformity: circuit family $\{C_n\}$

Boolean Circuits

- Non-uniformity: circuit family $\{C_n\}$
    - Given non-uniform computation $(M,\{A_n\})$, can define equivalent $\{C_n\}$

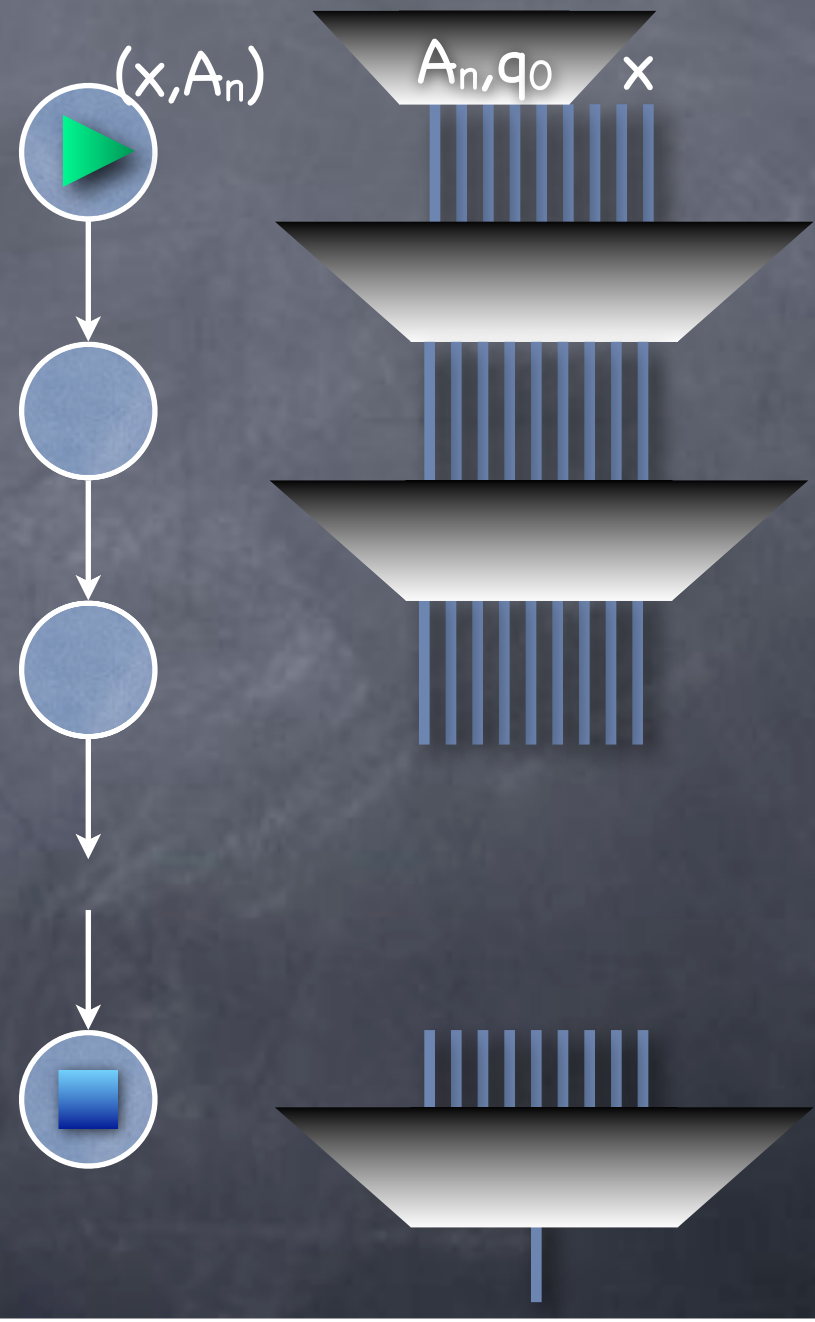
Boolean Circuits

- Non-uniformity: circuit family $\{C_n\}$
  - Given non-uniform computation $(M,\{A_n\})$, can define equivalent $\{C_n\}$



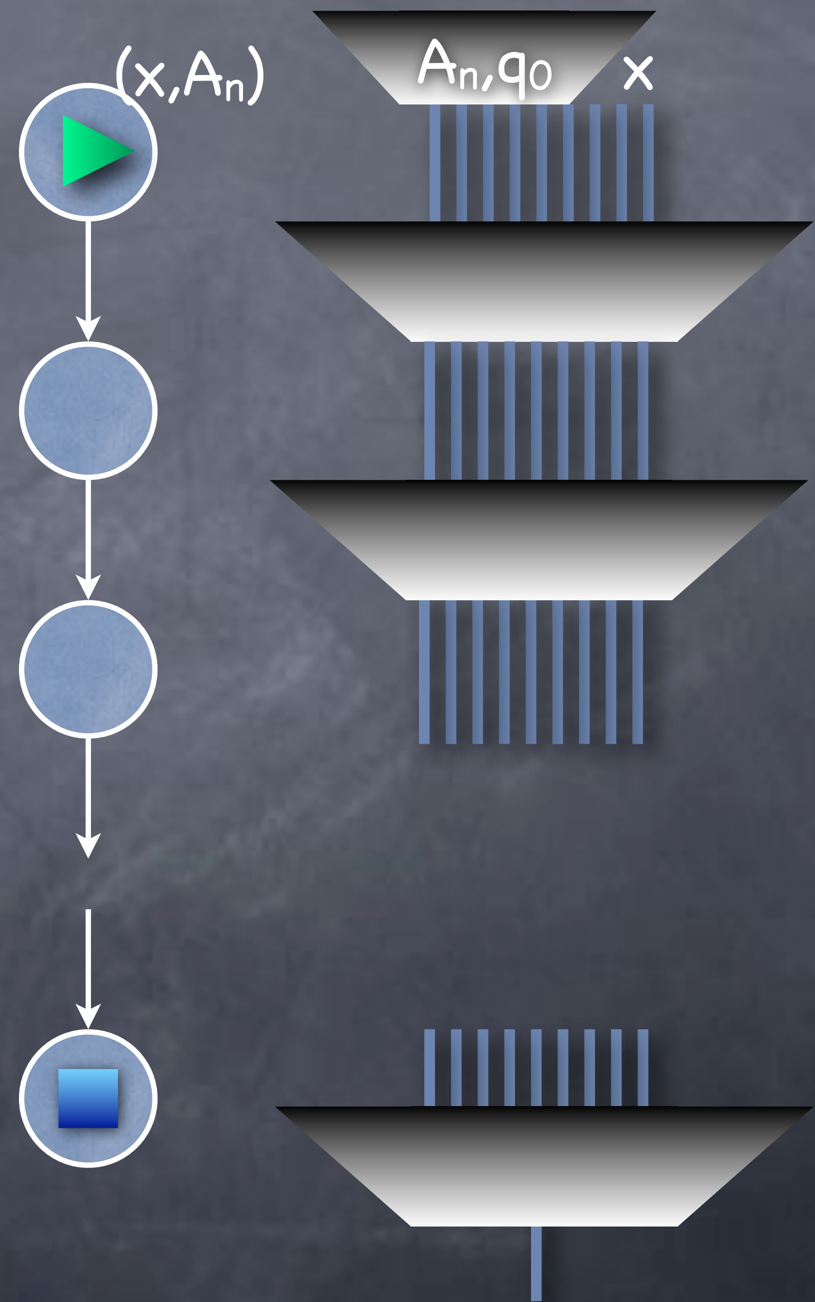
Boolean Circuits

- Non-uniformity: circuit family $\{C_n\}$
  - Given non-uniform computation $(M,\{A_n\})$, can define equivalent $\{C_n\}$
    - Advice A_n is hard-wired into circuit C_n



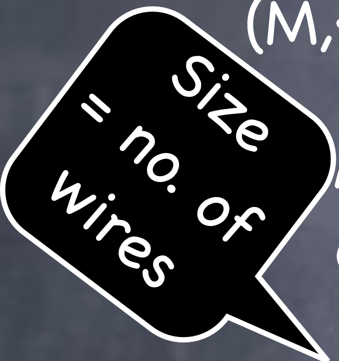
Boolean Circuits

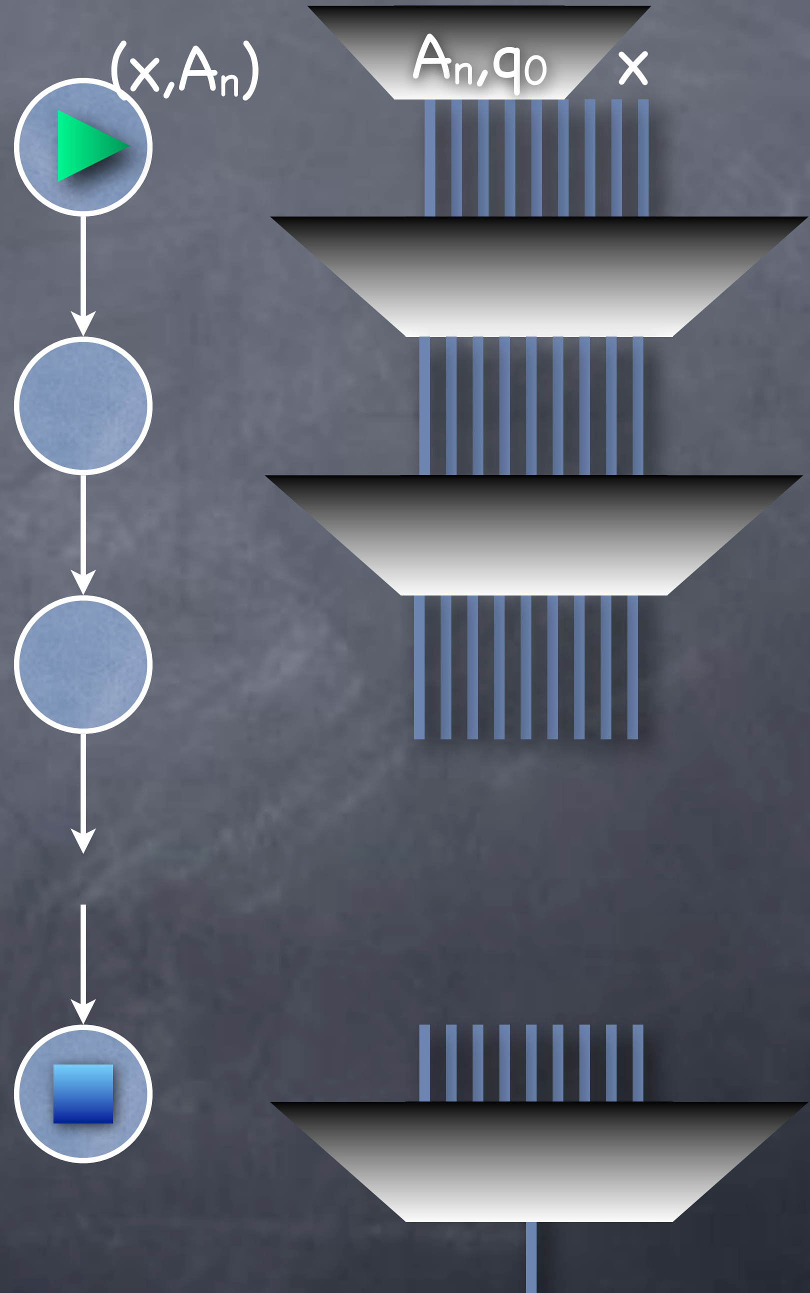
- Non-uniformity: circuit family $\{C_n\}$
  - Given non-uniform computation $(M,\{A_n\})$, can define equivalent $\{C_n\}$
    - Advice A_n is hard-wired into circuit C_n
    - Size of circuit polynomially related to running time of TM



Boolean Circuits

- Non-uniformity: circuit family $\{C_n\}$
  - Given non-uniform computation $(M,\{A_n\})$, can define equivalent $\{C_n\}$
    - Advice A_n is hard-wired into circuit C_n
    - Size of circuit polynomially related to running time of TM



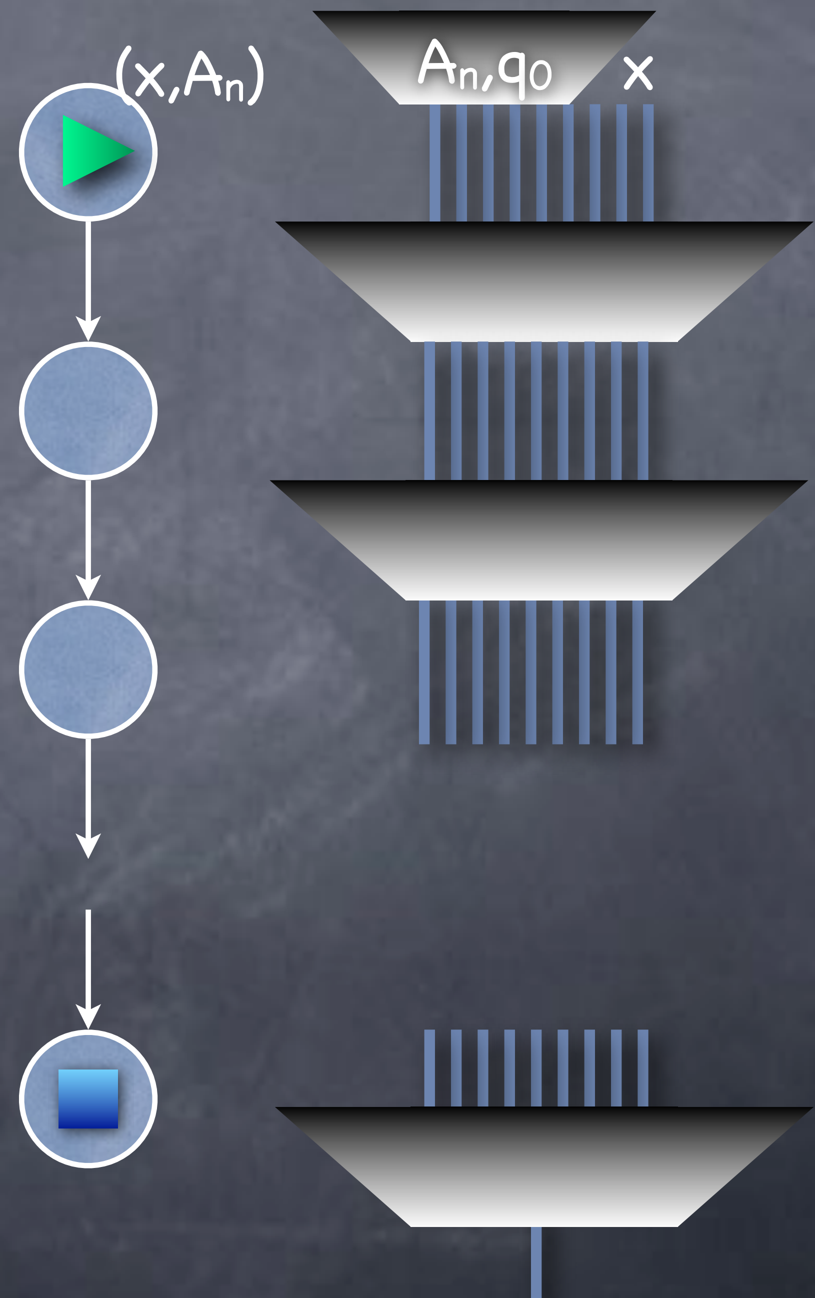


Boolean Circuits

- Non-uniformity: circuit family $\{C_n\}$
  - Given non-uniform computation $(M,\{A_n\})$, can define equivalent $\{C_n\}$
    - Advice A_n is hard-wired into circuit C_n
    - Size of circuit polynomially related to running time of TM

Size = no. of wires

  - Conversely, given $\{C_n\}$, can use description of C_n as advice A_n for a "universal" TM

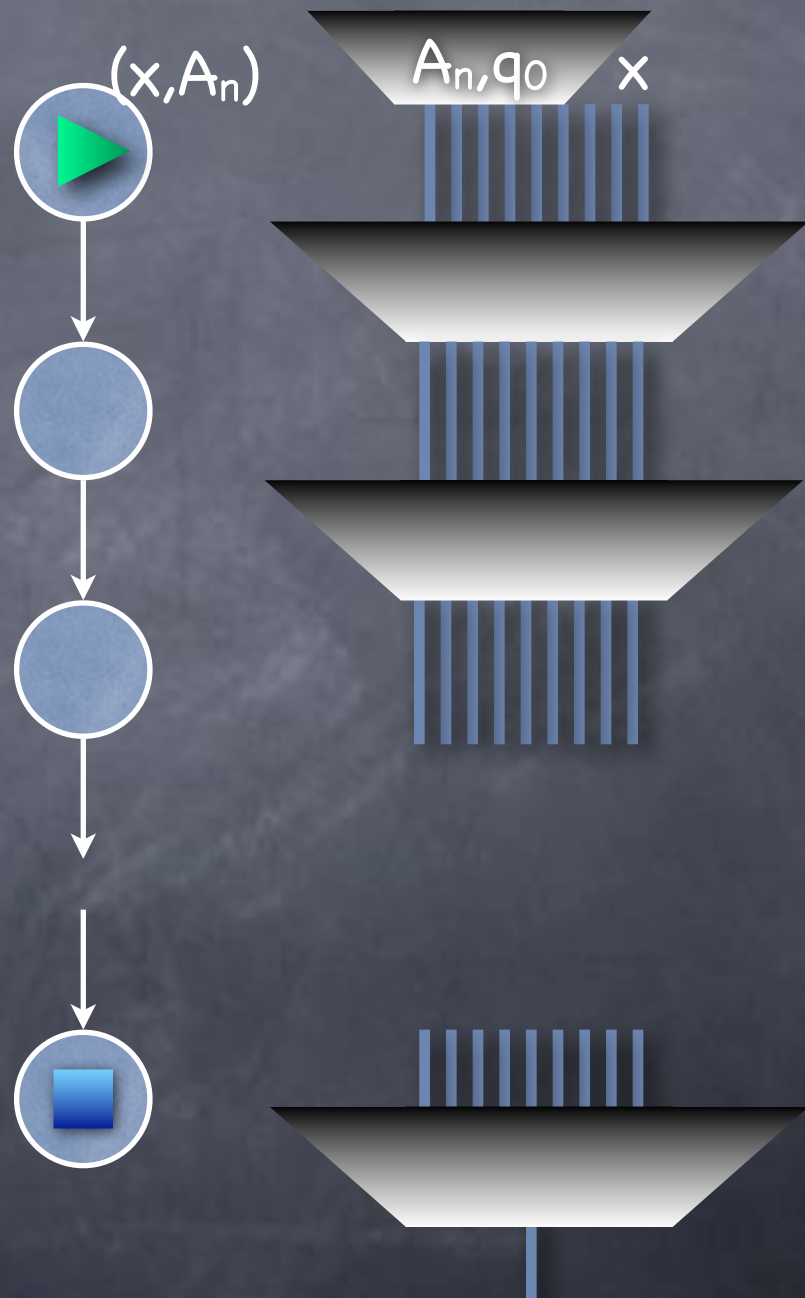


Boolean Circuits

- Non-uniformity: circuit family $\{C_n\}$
  - Given non-uniform computation $(M,\{A_n\})$, can define equivalent $\{C_n\}$

Size = no. of wires

    - Advice A_n is hard-wired into circuit C_n
    - Size of circuit polynomially related to running time of TM
  - Conversely, given $\{C_n\}$, can use description of C_n as advice A_n for a "universal" TM
    - $|A_n|$ comparable to size of circuit C_n



SIZE(T)

SIZE(T)

- SIZE(T): languages solved by circuit families of size T(n)

SIZE(T)

- SIZE(T): languages solved by circuit families of size T(n)
- P/poly = SIZE(poly)

SIZE(T)

- SIZE(T): languages solved by circuit families of size T(n)
- P/poly = SIZE(poly)
  - SIZE(poly) ⊆ P/poly: Size T circuit can be described in O(T log T) bits (advice). Universal TM can evaluate this circuit in poly time

SIZE(T)

- SIZE(T): languages solved by circuit families of size T(n)
- P/poly = SIZE(poly)
  - SIZE(poly) $\subseteq$ P/poly: Size T circuit can be described in O(T log T) bits (advice). Universal TM can evaluate this circuit in poly time
  - P/poly $\subseteq$ SIZE(poly): Transformation from Cook's theorem, with advice string hardwired into circuit

SIZE bounds

SIZE bounds

- All languages (decidable or not) are in SIZE(T) for $T=O(n2^n)$

SIZE bounds

- All languages (decidable or not) are in SIZE(T) for $T=O(n2^n)$
  - Circuit encodes truth-table

SIZE bounds

- All languages (decidable or not) are in SIZE(T) for $T=O(n2^n)$
  - Circuit encodes truth-table
- Most languages need circuits of size $\Omega(2^n/n)$

SIZE bounds

- All languages (decidable or not) are in SIZE(T) for $T=O(n2^n)$
  - Circuit encodes truth-table
- Most languages need circuits of size $\Omega(2^n/n)$
  - Number of circuits of size T is at most T^{2T}

SIZE bounds

- All languages (decidable or not) are in SIZE(T) for $T=O(n2^n)$
  - Circuit encodes truth-table
- Most languages need circuits of size $\Omega(2^n/n)$
  - Number of circuits of size T is at most T^{2T}
  - If $T = 2^n/4n$, say, $T^{2T} < 2^{(2\hat{}n)/2}$

SIZE bounds

- All languages (decidable or not) are in SIZE(T) for $T=O(n2^n)$
  - Circuit encodes truth-table
- Most languages need circuits of size $\Omega(2^n/n)$
  - Number of circuits of size T is at most T^{2T}
  - If $T = 2^n/4n$, say, $T^{2T} < 2^{(2^n)/2}$
  - Number of languages = 2^{2^n}

SIZE hierarchy

SIZE hierarchy

- $SIZE(T') \subsetneq SIZE(T)$ if $T=\Omega(t2^t)$ and $T'=O(2^t/t)$, for $t(n)\leq n$

SIZE hierarchy

- SIZE(T') $\subsetneq$ SIZE(T) if $T=\Omega(t2^t)$ and $T'=O(2^t/t)$, for $t(n) \leq n$
  - e.g., $T(n) = n \log n$ and $T'(n) = n/\log n$

SIZE hierarchy

- SIZE(T′) $\subsetneq$ SIZE(T) if $T=\Omega(t2^t)$ and $T'=O(2^t/t)$, for $t(n) \le n$
  - e.g., T(n) = n log n and T′(n) = n/log n
  - Consider functions on t bits (ignoring n-t bits)

SIZE hierarchy

- SIZE(T′) $\subsetneq$ SIZE(T) if $T=\Omega(t2^t)$ and $T'=O(2^t/t)$, for $t(n) \leq n$
  - e.g., T(n) = n log n and T′(n) = n/log n
  - Consider functions on t bits (ignoring n-t bits)
    - All of them in SIZE(T), most not in SIZE(T′)

Uniform Circuits

Uniform Circuits

- Uniform circuit family: constructed by a TM

Uniform Circuits

- Uniform circuit family: constructed by a TM
  - Undecidable languages are undecidable for these circuits families

Uniform Circuits

- Uniform circuit family: constructed by a TM
  - Undecidable languages are undecidable for these circuits families
  - Can relate their complexity classes to classes defined using TMs

Uniform Circuits

- Uniform circuit family: constructed by a TM
  - Undecidable languages are undecidable for these circuits families
  - Can relate their complexity classes to classes defined using TMs
- Logspace-uniform:

Uniform Circuits

- Uniform circuit family: constructed by a TM
  - Undecidable languages are undecidable for these circuits families
  - Can relate their complexity classes to classes defined using TMs
- Logspace-uniform:
  - An O(log n) space TM can compute the circuit

NC^i and AC^i

NC^i and AC^i

- NC^i: class of languages decided by bounded fan-in logspace-uniform circuits of polynomial size and depth $O(\log^i n)$

NC^i and AC^i

- NC^i: class of languages decided by bounded fan-in logspace-uniform circuits of polynomial size and depth $O(\log^i n)$
  - AC^i: Similar, but unbounded fan-in circuits

NC^i and AC^i

- NC^i: class of languages decided by bounded fan-in logspace-uniform circuits of polynomial size and depth $O(\log^i n)$
  - AC^i: Similar, but unbounded fan-in circuits
- NC^0 and AC^0: constant depth circuits

NC^i and AC^i

- NC^i: class of languages decided by bounded fan-in logspace-uniform circuits of polynomial size and depth $O(\log^i n)$
  - AC^i: Similar, but unbounded fan-in circuits
- NC^0 and AC^0: constant depth circuits
  - NC^0 output depends on only a constant number of input bits

NC^i and AC^i

- NC^i: class of languages decided by bounded fan-in logspace-uniform circuits of polynomial size and depth $O(\log^i n)$
  - AC^i: Similar, but unbounded fan-in circuits
- NC^0 and AC^0: constant depth circuits
  - NC^0 output depends on only a constant number of input bits
  - $NC^0 \subsetneq AC^0$: Consider L = {1,11,111,...}

NC and AC

NC and AC

- NC = $\cup_{i>0}$ NC^i. Similarly AC.

NC and AC

- $NC = \cup_{i>0} NC^i$. Similarly AC.
- $NC^i \subseteq AC^i \subseteq NC^{i+1}$

NC and AC

- NC = $\cup_{i>0}$ NC^i. Similarly AC.
- $NC^i \subseteq AC^i \subseteq NC^{i+1}$
  - Clearly $NC^i \subseteq AC^i$

NC and AC

- NC = $\cup_{i>0}$ NC^i. Similarly AC.
- $NC^i \subseteq AC^i \subseteq NC^{i+1}$
  - Clearly $NC^i \subseteq AC^i$
  - $AC^i \subseteq NC^{i+1}$ because polynomial fan-in can be reduced to constant fan-in by using a log depth tree

NC and AC

- $NC = \cup_{i>0} NC^i$. Similarly AC.
- $NC^i \subseteq AC^i \subseteq NC^{i+1}$
  - Clearly $NC^i \subseteq AC^i$
  - $AC^i \subseteq NC^{i+1}$ because polynomial fan-in can be reduced to constant fan-in by using a log depth tree
- So NC = AC

NC $\subseteq$ P

NC $\subseteq$ P

- Generate circuit of the right input size and evaluate on input

NC ⊆ P

- Generate circuit of the right input size and evaluate on input
- Generating the circuit

NC ⊆ P

- Generate circuit of the right input size and evaluate on input
- Generating the circuit
    - in logspace, so poly time; also circuit size is poly

NC $\subseteq$ P

- Generate circuit of the right input size and evaluate on input
- Generating the circuit
  - in logspace, so poly time; also circuit size is poly
- Evaluating the gates

NC ⊆ P

- Generate circuit of the right input size and evaluate on input
- Generating the circuit
  - in logspace, so poly time; also circuit size is poly
- Evaluating the gates
  - Poly(n) gates

NC ⊆ P

- Generate circuit of the right input size and evaluate on input
- Generating the circuit
  - in logspace, so poly time; also circuit size is poly
- Evaluating the gates
  - Poly(n) gates
  - Per gate takes O(1) time + time to look up output values of (already evaluated) gates

NC ⊆ P

- Generate circuit of the right input size and evaluate on input
- Generating the circuit
  - in logspace, so poly time; also circuit size is poly
- Evaluating the gates
  - Poly(n) gates
  - Per gate takes O(1) time + time to look up output values of (already evaluated) gates
- Open problem: Is NC = P?

Motivation for NC

Motivation for NC

- Fast parallel computation is (loosely) modeled as having poly many processors and taking poly-log time

Motivation for NC

- Fast parallel computation is (loosely) modeled as having poly many processors and taking poly-log time
  - Corresponds to NC (How?)

Motivation for NC

- Fast parallel computation is (loosely) modeled as having poly many processors and taking poly-log time
  - Corresponds to NC (How?)
  - Depth translates to time

Motivation for NC

- Fast parallel computation is (loosely) modeled as having poly many processors and taking poly-log time
  - Corresponds to NC (How?)
  - Depth translates to time
  - Total "work" is size of the circuit

Today

Today

- Non-uniform complexity

Today

- Non-uniform complexity
  - $P/1 \not\subseteq$ Decidable

Today

- Non-uniform complexity
  - $P/1 \not\subseteq$ Decidable
  - $NP \subseteq P/\log \Rightarrow NP = P$

Today

- Non-uniform complexity
  - $P/1 \not\subseteq$ Decidable
  - $NP \subseteq P/log \Rightarrow NP = P$
  - $NP \subseteq P/poly \Rightarrow PH = \Sigma_2^P$

Today

- Non-uniform complexity
  - P/1 $\not\subseteq$ Decidable
  - NP $\subseteq$ P/log $\Rightarrow$ NP = P
  - NP $\subseteq$ P/poly $\Rightarrow$ PH = Σ_2^P
- Non-uniform circuit Complexity

Today

- Non-uniform complexity
  - P/1 $\not\subseteq$ Decidable
  - NP $\subseteq$ P/log $\Rightarrow$ NP = P
  - NP $\subseteq$ P/poly $\Rightarrow$ PH = Σ_2^P
- Non-uniform circuit Complexity
  - SIZE(poly) = P/poly

Today

- Non-uniform complexity
  - P/1 $\not\subseteq$ Decidable
  - NP $\subseteq$ P/log $\Rightarrow$ NP = P
  - NP $\subseteq$ P/poly $\Rightarrow$ PH = Σ_2^P
- Non-uniform circuit Complexity
  - SIZE(poly) = P/poly
  - SIZE-hierarchy: SIZE(T') $\subsetneq$ SIZE(T) if $T=\Omega(t2^t)$, $T'=O(2^t/t)$

Today

- Non-uniform complexity
  - $P/1 \not\subseteq$ Decidable
  - $NP \subseteq P/\log \Rightarrow NP = P$
  - $NP \subseteq P/poly \Rightarrow PH = \Sigma_2^P$
- Non-uniform circuit Complexity
  - SIZE(poly) = P/poly
  - SIZE-hierarchy: $SIZE(T') \subsetneq SIZE(T)$ if $T=\Omega(t2^t)$, $T'=O(2^t/t)$
- Uniform Circuit Complexity

Today

- Non-uniform complexity
  - P/1 $\not\subseteq$ Decidable
  - NP $\subseteq$ P/log $\Rightarrow$ NP = P
  - NP $\subseteq$ P/poly $\Rightarrow$ PH = Σ_2^P
- Non-uniform circuit Complexity
  - SIZE(poly) = P/poly
  - SIZE-hierarchy: SIZE(T') $\subsetneq$ SIZE(T) if $T=\Omega(t2^t)$, $T'=O(2^t/t)$
- Uniform Circuit Complexity
  - $NC^i \subseteq AC^i \subseteq NC^{i+1} \subseteq NC = AC \subseteq P$