Lecture 22 To left or to right

A different complexity measure

A different complexity measure
Number of bits of input read

A different complexity measure
 Number of bits of input read
 For simpler problems

A different complexity measure
 Number of bits of input read
 For simpler problems
 Interested in lower-bounds

A different complexity measure
 Number of bits of input read
 For simpler problems
 Interested in lower-bounds
 So even allow unbounded computational power

A different complexity measure Number of bits of input read For simpler problems Interested in lower-bounds

So even allow unbounded computational power

Simpler combinatorial structure (need not) understand P vs. NP etc.)

 Configuration graph of a computation, as it reads each bit

Configuration graph of a computation, as it reads each bit



 Configuration graph of a computation, as it reads each bit

For n-bit input, depth at most n



- Configuration graph of a computation, as it reads each bit
 - For n-bit input, depth at most n
 - Some paths may be shorter



- Configuration graph of a computation, as it reads each bit
 - For n-bit input, depth at most n
 - Some paths may be shorter
- DTree(L) = min_{alg A} max_{input x} T_{A,x} where T_{A,x} is the number of bits of x read by A





Simpler problems

Simpler problems

OR(x)=1 if at least one bit of x is 1

Simpler problems

 \bigcirc OR(x)=1 if at least one bit of x is 1

PARITY(x)=1 if odd number of bits of x are 1

Simpler problems

 \bigcirc OR(x)=1 if at least one bit of x is 1

PARITY(x)=1 if odd number of bits of x are 1

 SAT_c(x) if x is a satisfying assignment for circuit (or circuit family) C

Simpler problems

 \bigcirc OR(x)=1 if at least one bit of x is 1

PARITY(x)=1 if odd number of bits of x are 1

 SAT_c(x) if x is a satisfying assignment for circuit (or circuit family) C

CONNECTED(G) = 1 if G is the adjacency matrix of a connected graph

Simpler problems

 \odot OR(x)=1 if at least one bit of x is 1

- PARITY(x)=1 if odd number of bits of x are 1
- SAT_c(x) if x is a satisfying assignment for circuit (or circuit family) C
- CONNECTED(G) = 1 if G is the adjacency matrix of a connected graph

 We are interested in showing DTree lower-bounds for these problems

Identifying one input which will cause a shallow decision tree to go wrong: Given a decision tree find inputs which lead it to the same leaf but must have different outputs

Identifying one input which will cause a shallow decision tree to go wrong: Given a decision tree find inputs which lead it to the same leaf but must have different outputs

@ e.g.: DTree(OR) = n (i.e., any correct decision tree will need to read all bits in the worst case)

Identifying one input which will cause a shallow decision tree to go wrong: Given a decision tree find inputs which lead it to the same leaf but must have different outputs

@ e.g.: DTree(OR) = n (i.e., any correct decision tree will need to read all bits in the worst case)

Start with all inputs

Identifying one input which will cause a shallow decision tree to go wrong: Given a decision tree find inputs which lead it to the same leaf but must have different outputs

e.g.: DTree(OR) = n (i.e., any correct decision tree will need to read all bits in the worst case)

Start with all inputs

At first node restrict to inputs which answer 0, and consider the tree's behavior on such inputs

Identifying one input which will cause a shallow decision tree to go wrong: Given a decision tree find inputs which lead it to the same leaf but must have different outputs

e.g.: DTree(OR) = n (i.e., any correct decision tree will need to read all bits in the worst case)

Start with all inputs

At first node restrict to inputs which answer 0, and consider the tree's behavior on such inputs

On second node, further restrict to inputs which answer O

Identifying one input which will cause a shallow decision tree to go wrong: Given a decision tree find inputs which lead it to the same leaf but must have different outputs

e.g.: DTree(OR) = n (i.e., any correct decision tree will need to read all bits in the worst case)

- Start with all inputs
- At first node restrict to inputs which answer 0, and consider the tree's behavior on such inputs
- On second node, further restrict to inputs which answer O
- Before n nodes, set of inputs contain Oⁿ and another input, no matter what bits where queried at the nodes

Tree(CONNECTED) = n(n-1)/2 (i.e., all possible edges)

Tree(CONNECTED) = n(n-1)/2 (i.e., all possible edges)

If possible, answer "No," but maintain the invariant that edges answered "Yes" plus unqueried edges form a connected graph.

Tree(CONNECTED) = n(n-1)/2 (i.e., all possible edges)

If possible, answer "No," but maintain the invariant that edges answered "Yes" plus unqueried edges form a connected graph.

Yes edges by themselves are connected only if set of unqueried edges is empty

Tree(CONNECTED) = n(n-1)/2 (i.e., all possible edges)

- If possible, answer "No," but maintain the invariant that edges answered "Yes" plus unqueried edges form a connected graph.
- Yes edges by themselves are connected only if set of unqueried edges is empty
 - Otherwise some Yes edge was unforced: consider the cycle formed by an unqueried edge and the connected Yes graph

Tree(CONNECTED) = n(n-1)/2 (i.e., all possible edges)

- If possible, answer "No," but maintain the invariant that edges answered "Yes" plus unqueried edges form a connected graph.
- Yes edges by themselves are connected only if set of unqueried edges is empty
 - Otherwise some Yes edge was unforced: consider the cycle formed by an unqueried edge and the connected Yes graph

Intil then, graph can be connected or disconnected: by setting all unqueried edges to Yes or all to No

Elusive Languages

Elusive Languages

Languages which require the decision tree to read all the bits in the worst case
Languages which require the decision tree to read all the bits in the worst case

e.g.: OR, PARITY, CONNECTED

Languages which require the decision tree to read all the bits in the worst case

Argued using adversary strategies

Languages which require the decision tree to read all the bits in the worst case

Argued using adversary strategies

Maj(x) = 1 iff #1s in x > #0s (assume |x| odd)

Languages which require the decision tree to read all the bits in the worst case

Argued using adversary strategies

Maj(x) = 1 iff #1s in x > #0s (assume |x| odd)

Adversary strategy: alternately answer 0 and 1

Tree of AND gates and OR gates (monotonic)

Tree of AND gates and OR gates (monotonic)Each variable (leaf) used only once

Tree of AND gates and OR gates (monotonic)
Each variable (leaf) used only once
Is elusive

Tree of AND gates and OR gates (monotonic)
Each variable (leaf) used only once

Is elusive

Answer so that each gate kept undetermined until all its leaf-descendants are queried

Tree of AND gates and OR gates (monotonic)

- Seach variable (leaf) used only once
- Is elusive

Answer so that each gate kept undetermined until all its leaf-descendants are queried

Service

@ 1-certificate

1-certificate

For x s.t. L(x)=1, a subset of the bits of x which proves that L(x)=1 : c s.t. x|c⇒x∈L (i.e., no x' s.t. L(x')=0 and has the same values at those positions)

1-certificate

 For x s.t. L(x)=1, a subset of the bits of x which proves that L(x)=1 : c s.t. x|c⇒x∈L (i.e., no x' s.t. L(x')=0 and has the same values at those positions)

Ø O-certificate: similarly for x∉L, c s.t. $x|c \Rightarrow x ∉L$

1-certificate

For x s.t. L(x)=1, a subset of the bits of x which proves that L(x)=1 : c s.t. x|c⇒x∈L (i.e., no x' s.t. L(x')=0 and has the same values at those positions)

Ø O-certificate: similarly for x∉L, c s.t. $x|c \Rightarrow x ∉L$

Can be much lower than DTree(L) because for different x's different sets of bits can be used

1-certificate

For x s.t. L(x)=1, a subset of the bits of x which proves that L(x)=1 : c s.t. x|c⇒x∈L (i.e., no x' s.t. L(x')=0 and has the same values at those positions)

Ø O-certificate: similarly for x∉L, c s.t. $x|c \Rightarrow x ∉L$

Can be much lower than DTree(L) because for different x's different sets of bits can be used

Produced by someone who has seen all bits of x

I-certificate

For x s.t. L(x)=1, a subset of the bits of x which proves that L(x)=1 : c s.t. x|c⇒x∈L (i.e., no x' s.t. L(x')=0 and has the same values at those positions)

Ø O-certificate: similarly for x∉L, c s.t. $x|c \Rightarrow x ∉L$

Can be much lower than DTree(L) because for different x's different sets of bits can be used

Produced by someone who has seen all bits of x

I-Cert(L): max_{x∈L} min_{c: x|c⇒x∈L} |c| (e.g. 1-Cert(OR) = 1)

I-certificate

- For x s.t. L(x)=1, a subset of the bits of x which proves that L(x)=1 : c s.t. x|c⇒x∈L (i.e., no x' s.t. L(x')=0 and has the same values at those positions)
- Ø O-certificate: similarly for x∉L, c s.t. $x|c \Rightarrow x ∉L$
- Can be much lower than DTree(L) because for different x's different sets of bits can be used
 - Produced by someone who has seen all bits of x
- I-Cert(L): max_{x∈L} min_{c: x|c⇒x∈L} |c| (e.g. 1-Cert(OR) = 1)
- O − Cert(L): $\max_{x \notin L} \min_{c: x \mid c \Rightarrow x \notin L} |c|$ (e.g. 0 − Cert(OR) = n)

A Decision tree algorithm

A Decision tree algorithm

 Start with a pool of all O-certificates and all 1-certificates (for various x)

A Decision tree algorithm

 Start with a pool of all O-certificates and all 1-certificates (for various x)

While both pools non-empty

A Decision tree algorithm

 Start with a pool of all O-certificates and all 1-certificates (for various x)

While both pools non-empty

Pick a O-certificate, and query all (remaining) bits in it

A Decision tree algorithm

- Start with a pool of all O-certificates and all 1-certificates (for various x)
- While both pools non-empty
 - Pick a O-certificate, and query all (remaining) bits in it
 - If a good O-certificate, terminate with O. Else, remove all
 O and 1 certificates inconsistent with the bits revealed

A Decision tree algorithm

- Start with a pool of all O-certificates and all 1-certificates (for various x)
- While both pools non-empty
 - Pick a O-certificate, and query all (remaining) bits in it
 - If a good O-certificate, terminate with O. Else, remove all
 O and 1 certificates inconsistent with the bits revealed
- One pool must be non-empty. Output the corresponding answer

A Decision tree algorithm

 Start with a pool of all O-certificates and all 1-certificates (for various x)

While both pools non-empty

- Pick a O-certificate, and query all (remaining) bits in it
- If a good O-certificate, terminate with O. Else, remove all O and 1 certificates inconsistent with the bits revealed
- One pool must be non-empty. Output the corresponding answer

Clearly correct. Number of bits read?

An undetermined O-certificate has at least one unrevealed conflicting bit with each undetermined 1-certificate

An undetermined O-certificate has at least one unrevealed conflicting bit with each undetermined 1-certificate

Otherwise it is possible to have an x consistent with both those certificates!

An undetermined O-certificate has at least one unrevealed conflicting bit with each undetermined 1-certificate

Otherwise it is possible to have an x consistent with both those certificates!

Picking such a O-certificate and querying reduces number of unrevealed bits of each remaining 1-certificate by at least 1

An undetermined O-certificate has at least one unrevealed conflicting bit with each undetermined 1-certificate

Otherwise it is possible to have an x consistent with both those certificates!

Picking such a O-certificate and querying reduces number of unrevealed bits of each remaining 1-certificate by at least 1

Initially at most 1Cert(L) bits in each 1-certificate

An undetermined O-certificate has at least one unrevealed conflicting bit with each undetermined 1-certificate

Otherwise it is possible to have an x consistent with both those certificates!

Picking such a O-certificate and querying reduces number of unrevealed bits of each remaining 1-certificate by at least 1

Initially at most 1Cert(L) bits in each 1-certificate

So at most 1Cert(L) iterations

An undetermined O-certificate has at least one unrevealed conflicting bit with each undetermined 1-certificate

Otherwise it is possible to have an x consistent with both those certificates!

Picking such a O-certificate and querying reduces number of unrevealed bits of each remaining 1-certificate by at least 1

Initially at most 1Cert(L) bits in each 1-certificate

So at most 1Cert(L) iterations

In each iteration at most OCert(L) bits queried

Example: AND-OR trees

Seample: AND-OR trees

O-certificate: enough variables so that can evaluate just one input wire for AND gates, and all input wires for OR gates
$DTree(L) \leq OCert(L) \times 1Cert(L)$

Seample: AND-OR trees

- O-certificate: enough variables so that can evaluate just one input wire for AND gates, and all input wires for OR gates
- 1-certificate: enough variables so that can evaluate just one input wire for OR gates, and all input wires for AND gates

$DTree(L) \leq OCert(L) \times 1Cert(L)$

Seample: AND-OR trees

- O-certificate: enough variables so that can evaluate just one input wire for AND gates, and all input wires for OR gates
- 1-certificate: enough variables so that can evaluate just one input wire for OR gates, and all input wires for AND gates
- If regular AND-OR tree, OCert(L) x 1Cert(L) = number of leaves = DTree(L)

Ø Various techniques

Arithmetization: write the boolean function for L as a multi-linear polynomial of n boolean variables. Then degree is a lower-bound on DTree(L)

- Arithmetization: write the boolean function for L as a multi-linear polynomial of n boolean variables. Then degree is a lower-bound on DTree(L)
- Topological criterion for monotone functions: construct a simplicial complex corresponding to the monotone boolean function. If the simplicial complex "not collapsible" then DTree(L)=n

- Arithmetization: write the boolean function for L as a multi-linear polynomial of n boolean variables. Then degree is a lower-bound on DTree(L)
- Topological criterion for monotone functions: construct a simplicial complex corresponding to the monotone boolean function. If the simplicial complex "not collapsible" then DTree(L)=n
- Sensitivity" is a lower-bound on DTree(L)

- Arithmetization: write the boolean function for L as a multi-linear polynomial of n boolean variables. Then degree is a lower-bound on DTree(L)
- Topological criterion for monotone functions: construct a simplicial complex corresponding to the monotone boolean function. If the simplicial complex "not collapsible" then DTree(L)=n
- Sensitivity" is a lower-bound on DTree(L)
- Will explore some in exercises

Recall two views of randomized computation

Recall two views of randomized computation

Randomly decide (based on fresh coin flips, and queries and answers so far) what variable to query

Recall two views of randomized computation

Randomly decide (based on fresh coin flips, and queries and answers so far) what variable to query

Flip all coins up front and then run a deterministic computation

Recall two views of randomized computation

- Randomly decide (based on fresh coin flips, and queries and answers so far) what variable to query
- Flip all coins up front and then run a deterministic computation

◎ i.e., randomly choose a (deterministic) decision tree

Complexity measure

- Complexity measure
 - Sected number of bits read, max over all inputs

- Complexity measure
 - Sected number of bits read, max over all inputs
 - Note: No error allowed (Las Vegas)

- Complexity measure
 - Sected number of bits read, max over all inputs
 - Note: No error allowed (Las Vegas)
- Random decision tree chosen independent of the (adversarial) input. i.e., input chosen "before" the random choice

- Complexity measure
 - Sected number of bits read, max over all inputs
 - Note: No error allowed (Las Vegas)
- Random decision tree chosen independent of the (adversarial) input. i.e., input chosen "before" the random choice
 - Gets more power over the "adversary"

- Complexity measure
 - Sected number of bits read, max over all inputs
 - Note: No error allowed (Las Vegas)
- Random decision tree chosen independent of the (adversarial) input. i.e., input chosen "before" the random choice
 - Gets more power over the "adversary"
 - Adversary can't find a single pair of inputs that force many reads for all random choices

- Complexity measure
 - Sected number of bits read, max over all inputs
 - Note: No error allowed (Las Vegas)
- Random decision tree chosen independent of the (adversarial) input. i.e., input chosen "before" the random choice
 - Gets more power over the "adversary"
 - Adversary can't find a single pair of inputs that force many reads for all random choices

Question: How to prove lower-bounds against randomization?

Interested in expected cost (running time)

Interested in expected cost (running time)



Interested in expected cost (running time)



- Interested in expected cost (running time)
- Standard setting: Pick your randomized algorithm R; input x given adversarially



- Interested in expected cost (running time)
- Standard setting: Pick your randomized algorithm R; input x given adversarially
 - Or may allow random input: not useful to the adversary)



- Interested in expected cost (running time)
- Standard setting: Pick your randomized algorithm R; input x given adversarially
 - (Or may allow random input: not useful to the adversary)
- Another setting: Given adversarial input distribution X; pick your deterministic algorithm A



- Interested in expected cost (running time)
- Standard setting: Pick your randomized algorithm R; input x given adversarially
 - Or may allow random input: not useful to the adversary)
- Another setting: Given adversarial input distribution X; pick your deterministic algorithm A
 - (Allowing randomized algorithm no better)



- Interested in expected cost (running time)
- Standard setting: Pick your randomized algorithm R; input x given adversarially
 - Or may allow random input: not useful to the adversary)
- Another setting: Given adversarial input distribution X; pick your deterministic algorithm A
 - (Allowing randomized algorithm no better)
- Both have the same expected cost!! (not obvious: follows from LP duality)



• $\min_{\text{rand-alg R}} \max_{\text{input x}} E_{A \leftarrow R}[T_{A,x}] = \max_{\text{inp-distr x}} \min_{\text{alg A}} E_{x \leftarrow x}[T_{A,x}]$

Simpler, but useful direction: for <u>any</u> randomized alg R and <u>any</u> input-distribution X, maximput × E_{A←R}[T_{A,x}] ≥ min_{alg A} E_{x←X}[T_{A,x}]

- $\min_{\text{rand-alg R}} \max_{\text{maxinput x}} E_{A \leftarrow R}[T_{A,x}] = \max_{\text{inp-distr X}} \min_{\text{alg A}} E_{X \leftarrow X}[T_{A,x}]$
- Simpler, but useful direction: for <u>any</u> randomized alg R and <u>any</u> input-distribution X, maximput x E_{A←R}[T_{A,X}] ≥ min_{alg A} E_{X←X}[T_{A,X}]
 - If every algorithm A performs badly on an input-distribution X, then a randomized combination of those algorithms also perform badly on X. If R does badly on X, on some x in its support it does at least as badly (x depends on R)

- Simpler, but useful direction: for <u>any</u> randomized alg R and <u>any</u> input-distribution X, $\max_{input \times} E_{A \leftarrow R}[T_{A,X}] \ge \min_{alg A} E_{X \leftarrow X}[T_{A,X}]$
 - If every algorithm A performs badly on an input-distribution X, then a randomized combination of those algorithms also perform badly on X. If R does badly on X, on some x in its support it does at least as badly (x depends on R)
 - Useful: Can show lower-bound for randomized algorithms via lower-bound on distributional complexity for deterministic algorithms