Hardness Magnification for all Sparse NP Languages

Lijie Chen
MIT

Ce Jin
Tsinghua U.

Ryan Williams
MIT

Minimum Circuit Size Problem

Problem: MCSP$[s(m)]$
· **Given:** $f: \{0,1\}^m \to \{0,1\}$ as a truth table of length $n = 2^m$
· **Decide:** Does f have a circuit of size at most $s(m)$?

Minimum Circuit Size Problem

Problem: MCSP$[s(m)]$
· **Given:** $f: \{0,1\}^m \to \{0,1\}$ as a truth table of length $n = 2^m$
· **Decide:** Does f have a circuit of size at most $s(m)$?

MCSP$[s(m)] \in \mathbf{NP}$**;** solvable in $n \cdot 2^{\tilde{O}(s(m))}$ time**.**

Minimum Circuit Size Problem

Problem: MCSP$[s(m)]$
· **Given:** $f: \{0,1\}^m \to \{0,1\}$ as a truth table of length $n = 2^m$
· **Decide:** Does f have a circuit of size at most $s(m)$?

MCSP$[s(m)] \in \mathbf{NP}$; solvable in $n \cdot 2^{\tilde{O}(s(m))}$ time.

We believe MCSP$[m^{10}] \notin \mathbf{P/poly}$!
(otherwise, no strong PRGs exist [Razborov-Rudich])

Minimum Circuit Size Problem

Problem: MCSP$[s(m)]$
· **Given:** $f: \{0,1\}^m \to \{0,1\}$ as a truth table of length $n = 2^m$
· **Decide:** Does f have a circuit of size at most $s(m)$?

MCSP$[s(m)] \in \mathbf{NP}$; solvable in $n \cdot 2^{\tilde{O}(s(m))}$ time.

We believe MCSP$[m^{10}] \notin \mathbf{P/poly}$!
(otherwise, no strong PRGs exist [Razborov-Rudich])

If MCSP$[m^{10}]$ ***doesn't have*** circuits of $n \cdot \mathrm{polylog}\, n$ size and $\mathrm{polylog}\, n$ depth, then $\mathbf{NP} \not\subset \mathbf{P/poly}$.

(McKay-Murray-Williams'19)

Minimum Circuit Size Problem

Problem: MCSP$[s(m)]$
· **Given:** $f: \{0,1\}^m \to \{0,1\}$ as a truth table of length $n = 2^m$
· **Decide:** Does f have a circuit of size at most $s(m)$?

MCSP$[s(m)] \in \mathbf{NP}$; solvable in $n \cdot 2^{\tilde{O}(s(m))}$ time.

We believe MCSP$[m^{10}] \notin \mathbf{P/poly}$!
(otherwise, no strong PRGs exist [Razborov-Rudich])

If MCSP$[m^{10}]$ ***doesn't have*** circuits of $n \cdot \mathrm{polylog}\, n$ size and $\mathrm{polylog}\, n$ depth, then $\mathbf{NP} \not\subset \mathbf{P/poly}$.

(McKay-Murray-Williams'19)

"Hardness Magnification"

Hardness Magnification for MCSP

(Input length $n = 2^m$)

If MCSP[m^{10}] doesn't have circuits of $n \cdot \mathrm{polylog}\, n$ size and $\mathrm{polylog}\, n$ depth, then $\mathbf{NP} \not\subset \mathbf{P/poly}$.

(McKay-Murray-Williams'19)

Similar magnification results for MKtP (Minimum *time-bounded Kolmogorov Complexity*, $\mathrm{Kt}(x)$)

Hardness Magnification for MCSP

(Input length $n = 2^m$)

If MCSP$[m^{10}]$ doesn't have circuits of $n \cdot \mathrm{polylog}\, n$ size and $\mathrm{polylog}\, n$ depth, then $\mathbf{NP} \not\subset \mathbf{P/poly}$.

(McKay-Murray-Williams'19)

Similar magnification results for MKtP (Minimum *time-bounded Kolmogorov Complexity*, $\mathrm{Kt}(x)$)

Kt(x) = "measure of how much info needed to generate x quickly"

MKtP ≈ MCSP with "EXP-oracle gates"

Hardness Magnification for MCSP

(Input length $n = 2^m$)

If MCSP$[m^{10}]$ doesn't have circuits of $n \cdot \mathrm{polylog}\, n$ size and $\mathrm{polylog}\, n$ depth, then $\mathbf{NP} \not\subset \mathbf{P/poly}$.

(McKay-Murray-Williams'19)

Similar magnification results for MKtP (Minimum *time-bounded Kolmogorov Complexity*, $\mathrm{Kt}(x)$)

Kt(x) = "measure of how much info needed to generate x quickly"

MKtP ≈ MCSP with "EXP-oracle gates"

("Gap-MKtP$[a, b]$": distinguish between $\mathrm{Kt}(x) \leq a$ and $\mathrm{Kt}(x) \geq b$)

If Gap-MKtP$[m^{10}, m^{10} + O(m)]$ **doesn't have** $n^3 \mathrm{polylog}\, n$-size (De Morgan) Formulas, then $\mathbf{EXP} \not\subset \mathbf{NC^1}$.

(Oliveira-Pich-Santhanam'19)

Hardness Magnification for MCSP

(Input length $n = 2^m$)

If MCSP[m^{10}] doesn't have circuits of $n \cdot \mathrm{polylog}\, n$ size and $\mathrm{polylog}\, n$ depth, then $\mathbf{NP} \not\subset \mathbf{P/poly}$.

(McKay-Murray-Williams'19)

Similar magnification results for MKtP (Minimum *time-bounded Kolmogorov Complexity*, $\mathrm{Kt}(x)$)

Kt(x) = "measure of how much info needed to generate x quickly"

MKtP ≈ MCS

("Gap-MKtP[$\geq b$)

If Gap-MKtP n-size

(De Morgan

nam'19)

(Other Hardness Magnification Results)

$n^{1-\varepsilon}$-approximate Clique [Sri'03]

Average-case MCSP [OS'18]

k-Vertex-Cover [OS'18]

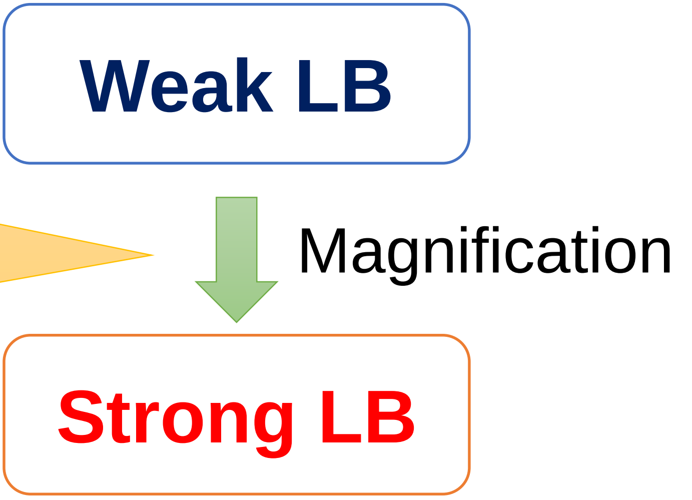
low-depth circuit LBs for $\mathbf{NC^1}$ [AK'10,CT'19]

sublinear-depth circuit LBs for $\mathbf{P}$ [LW'13]

…

How to view Hardness Magnification?

Suggests new approaches to **proving strong lower bounds**?



How to view Hardness Magnification?

Suggests new approaches to **proving strong lower bounds**?

Weak LB

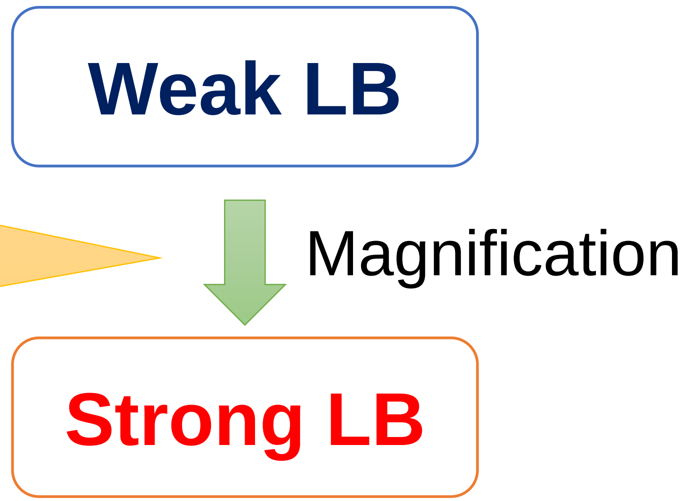
Magnification

Strong LB

It is argued that HM can bypass the **Natural Proof Barrier** [Razborov-Rudich]

How to view Hardness Magnification?

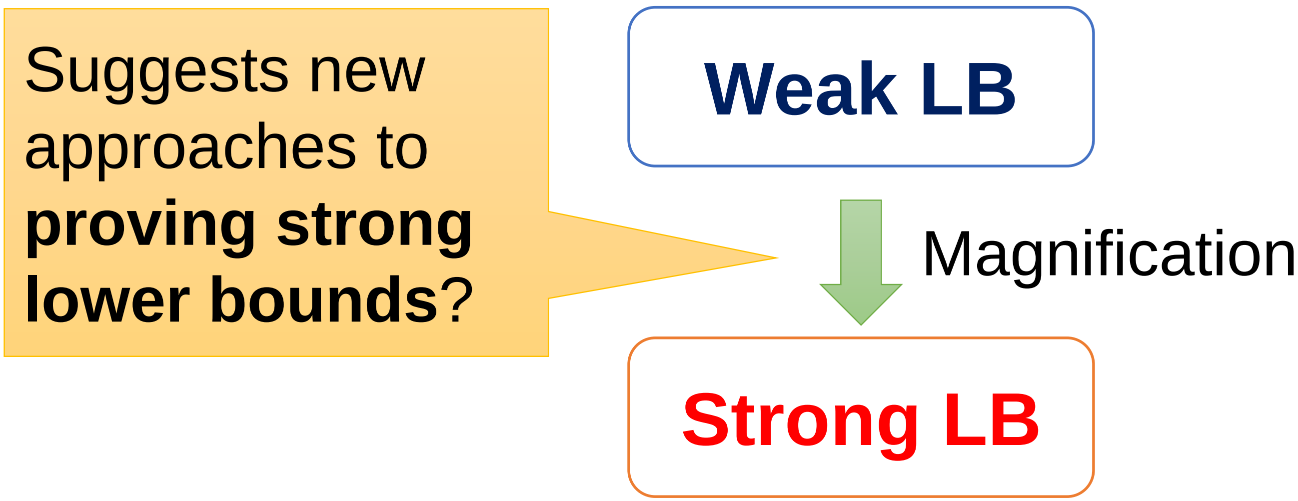
Suggests new approaches to **proving strong lower bounds**?



It is argued that HM can bypass the **Natural Proof Barrier** [Razborov-Rudich]

- **A heuristic argument** [AK'10, OS'18]: HM seems to yield strong LBs only for *certain* functions, not for *most* of them (violating the "largeness" condition of Natural Proofs)

How to view Hardness Magnification?



It is argued that HM can bypass the **Natural Proof Barrier** [Razborov-Rudich]

- **A heuristic argument** [AK'10, OS'18]: HM seems to yield strong LBs only for *certain* functions, not for *most* of them (violating the "largeness" condition of Natural Proofs)
- **A real theorem** [CHOPRS to appear in ITCS'20]
  In some cases, the required weak LB actually implies the *non-existence* of natural proofs

Extending Known Lower Bounds?

(Input length $n = 2^m$)

If Gap-MKtP$[m^{10}, m^{10} + O(m)]$

- **doesn't have** $n^3 \mathrm{polylog}\, n$-size (De Morgan) Formulas, then

$\mathbf{EXP} \not\subset \mathbf{NC^1}$.

[OPS'19]

Extending Known Lower Bounds?

(Input length $n = 2^m$)

If Gap-MKtP$[m^{10}, m^{10} + O(m)]$
・**doesn't have** $n^3 \text{polylog}\, n$-size (De Morgan) Formulas, then
$\mathbf{EXP} \not\subset \mathbf{NC^1}$.

[OPS'19]

We know how to prove $n^{1.99}$-size formula lower bound for Gap-MKtP ! [OPS'19]

Extending Known Lower Bounds?

(Input length $n = 2^m$)

If Gap-MKtP$[m^{10}, m^{10} + O(m)]$
· **doesn't have** $n^3 \text{polylog}\, n$-size (De Morgan) Formulas, then
$\mathbf{EXP} \not\subset \mathbf{NC^1}$.

[OPS'19]

We know how to prove $n^{1.99}$-size formula lower bound for Gap-MKtP ! [OPS'19]

Can we improve it by a factor of $n^{1+\varepsilon}$?

Extending Known Lower Bounds?

(Input length $n = 2^m$)

If Gap-MKtP$[m^{10}, m^{10} + O(m)]$

- **doesn't have** $n^3\text{polylog}\, n$-size (De Morgan) Formulas, then $\mathbf{EXP} \not\subset \mathbf{NC^1}$.
- **doesn't have** $n \cdot \text{polylog}\, n$-size Formula-$\oplus$, then $\mathbf{EXP} \not\subset \mathbf{NC^1}$.

[OPS'19]

Formula-$\oplus$: De Morgan Formulas where each leaf node computes XOR of a subset of input bits

Extending Known Lower Bounds?

(Input length $n = 2^m$)

If Gap-MKtP$[m^{10}, m^{10} + O(m)]$

- **doesn't have** $n^3 \text{polylog}\, n$-size (De Morgan) Formulas, then $\mathbf{EXP} \not\subset \mathbf{NC^1}$.
- **doesn't have** $n \cdot \text{polylog}\, n$-size Formula-⊕, then $\mathbf{EXP} \not\subset \mathbf{NC^1}$.

Known LB against Formula-⊕(Tal'16) :
$\mathbf{F_2}$-Inner-Product $\notin$ $\mathbf{Formula\text{-}\oplus}\ [\boldsymbol{n^2} / \mathbf{polylog}\ \boldsymbol{n}]$

Stronger LB than required

Extending Known Lower Bounds?

(Input length $n = 2^m$)

If Gap-MKtP$[m^{10}, m^{10} + O(m)]$

- **doesn't have** $n^3 \text{polylog}\, n$-size (De Morgan) Formulas, then $\mathbf{EXP} \not\subset \mathbf{NC^1}$.
- **doesn't have** $n \cdot \text{polylog}\, n$-size Formula-⊕, then $\mathbf{EXP} \not\subset \mathbf{NC^1}$.

Known LB against Formula-⊕(Tal'16) :

$\mathbf{F_2}$-Inner-Product $\notin \mathbf{Formula\text{-}\oplus}\ [\boldsymbol{n^2 / \text{polylog}\, n}]$

Much easier than Gap-MKtP??!

Stronger LB than required

Extending Known Lower Bounds?

(Input length $n = 2^m$)

If Gap-MKtP$[m^{10}, m^{10} + O(m)]$

- **doesn't have** $n^3 \mathrm{polylog}\, n$-size (De Morgan) Formulas, then $\mathbf{EXP} \not\subset \mathbf{NC^1}$.
- **doesn't have** $n \cdot \mathrm{polylog}\, n$-size Formula-$\oplus$, then $\mathbf{EXP} \not\subset \mathbf{NC^1}$.

Known LB against Formula-$\oplus$(Tal'16) :

$\mathbf{F_2}$-Inner-Product $\notin$ $\mathbf{Formula\text{-}\oplus}\left[\boldsymbol{n^2 / \mathrm{polylog}\, n}\right]$

Much easier than Gap-MKtP??!

Stronger LB than required

Can we adapt the proof techniques to Gap-MKtP?

How to view Hardness Magnification?

Suggests new approaches to **proving strong lower bounds**?

Indicates proving "weak" lower bounds are even harder than previously thought??

Weak LB

↓ Magnification

Strong LB

How to view Hardness Magnification?

Suggests new approaches to **proving strong lower bounds**?

Indicates proving "weak" lower bounds are even harder than previously thought??

Weak LB

Magnification

Strong LB

- Hardness magnification:

  Proving ***almost-linear size lower bounds*** is already as hard as proving ***super-polynomial lower bounds***…

(Input length $n = 2^m$)

If MCSP$[m^{10}]$ **doesn't have** circuits of $n \cdot \mathrm{polylog}\, n$ size and $\mathrm{polylog}\, n$ depth, **then** $\mathbf{NP} \not\subset \mathbf{P/poly}$.

If Gap-MKtP$[m^{10}, m^{10} + O(m)]$

- **doesn't have** $n^3 \mathrm{polylog}\, n$-size (De Morgan) Formula, **then** $\mathbf{EXP} \not\subset \mathbf{NC^1}$.
- **doesn't have** $n \cdot \mathrm{polylog}\, n$-size Formula-$\oplus$, **then** $\mathbf{EXP} \not\subset \mathbf{NC^1}$.

What is special about MCSP and MKtP?

Is it because they are "compression" problems?

Problem: MCSP$[s(m)]$

- **Given:** $f: \{0,1\}^m \to \{0,1\}$ as a truth table of length $n = 2^m$
- **Decide:** Does f have a circuit of size at most $s(m)$?

(Input length $n = 2^m$)

If MCSP$[m^{10}]$ **doesn't have** circuits of $n \cdot \mathrm{polylog}\, n$ size and $\mathrm{polylog}\, n$ depth, **then** $\mathbf{NP} \not\subset \mathbf{P/poly}$.

If Gap-MKtP$[m^{10}, m^{10} + O(m)]$

- **doesn't have** $n^3 \mathrm{polylog}\, n$-size (De Morgan) Formula, **then** $\mathbf{EXP} \not\subset \mathbf{NC^1}$.
- **doesn't have** $n \cdot \mathrm{polylog}\, n$-size Formula-$\oplus$, **then** $\mathbf{EXP} \not\subset \mathbf{NC^1}$.

What is special about MCSP and MKtP?
Is it because they are "compression" problems?

Observation: MCSP$[m^{10}]$ and MKtP$[m^{10}]$ are ***sparse*** languages!

MCSP$[s(m)]$ is $2^{\tilde{O}(s(m))}$-sparse;
there are at most $2^{\tilde{O}(s(m))}$ many circuits!

Problem: MCSP$[s(m)]$

- **Given:** $f: \{0,1\}^m \to \{0,1\}$ as a truth table of length $n = 2^m$
- **Decide:** Does f have a circuit of size at most $s(m)$?

(Input length $n = 2^m$)

If MCSP$[m^{10}]$ **doesn't have** circuits of $n \cdot \mathrm{polylog}\, n$ size and $\mathrm{polylog}\, n$ depth, **then** $\mathbf{NP} \not\subset \mathbf{P/poly}$.

If Gap-MKtP$[m^{10}, m^{10} + O(m)]$

- **doesn't have** $n^3 \mathrm{polylog}\, n$-size (De Morgan) Formula, **then** $\mathbf{EXP} \not\subset \mathbf{NC^1}$.
- **doesn't have** $n \cdot \mathrm{polylog}\, n$-size Formula-$\oplus$, **then** $\mathbf{EXP} \not\subset \mathbf{NC^1}$.

What is special about MCSP and MKtP?

Is it because they are "compression" problems?

Observation: MCSP$[m^{10}]$ and MKtP$[m^{10}]$ are ***sparse*** languages!

MCSP$[s(m)]$ is $2^{\tilde{O}(s(m))}$-sparse;

there are at most $2^{\tilde{O}(s(m))}$ many circuits!

Our result: Hardness magnification holds for ***all*** sparse $\mathbf{NP}$ languages!

HM for all sparse NP languages

Theorem 1:

Let L be ***any*** $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language.

· If L doesn't have $\boldsymbol{n^{1.01}}$-size circuits, then **for all** $\boldsymbol{k}$**,** $\mathbf{NP} \not\subset \mathbf{SIZE}[\boldsymbol{n^k}]$.

HM for all sparse NP languages

Theorem 1:

Let L be ***any*** $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language.

· If L doesn't have $\boldsymbol{n^{1.01}}$-size circuits, then **for all $\boldsymbol{k}$, $\mathbf{NP} \not\subset \mathbf{SIZE}[\boldsymbol{n^k}]$**.

· If L doesn't have $\boldsymbol{n^{3.01}}$-size formulas, then **for all $\boldsymbol{k}$, $\mathbf{NP}$ doesn't have $\boldsymbol{n^k}$-size formulas**.

· If L doesn't have $\boldsymbol{n^{2.01}}$-size branching programs, then **for all $\boldsymbol{k}$, $\mathbf{NP}$ doesn't have $\boldsymbol{n^k}$-size branching programs**.

Similar results for other models!

HM for all sparse NP languages

Theorem 1:

Let L be ***any*** $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language.

· If L doesn't have $\boldsymbol{n^{1.01}}$-size circuits, then **for all $\boldsymbol{k}$, $\mathbf{NP} \not\subset \mathbf{SIZE}[\boldsymbol{n^k}]$**.

· If L doesn't have $\boldsymbol{n^{3.01}}$-size formulas, then **for all $\boldsymbol{k}$, $\mathbf{NP}$ doesn't have $\boldsymbol{n^k}$-size formulas**.

· If L doesn't have $\boldsymbol{n^{2.01}}$-size branching programs, then **for all $\boldsymbol{k}$, $\mathbf{NP}$ doesn't have $\boldsymbol{n^k}$-size branching programs**.

Similar results for other models!

Compared with [MMW'19]: Our techniques yield weaker consequences (e.g. they get $\mathbf{NP} \not\subset \mathbf{P/poly}$), but apply to more restricted models.

HM for all sparse NP languages

Theorem 1:

Let L be ***any*** $2^{n^{o(1)}}$*-sparse* $\mathbf{NP}$ language.

· If L doesn't have $\boldsymbol{n^{1.01}}$-size circuits, then **for all $\boldsymbol{k}$, $\mathbf{NP} \not\subset \mathbf{SIZE}[\boldsymbol{n^k}]$**.

· If L doesn't have $\boldsymbol{n^{3.01}}$-size formulas, then
for all $\boldsymbol{k}$, $\mathbf{NP}$ doesn't have $\boldsymbol{n^k}$-size formulas.

· If L doesn't have $\boldsymbol{n^{2.01}}$-size branching programs, then
for all $\boldsymbol{k}$, $\mathbf{NP}$ doesn't have $\boldsymbol{n^k}$-size branching programs.

Similar results for other models!

Compared with [MMW'19]: Our techniques yield weaker consequences (e.g. they get $\mathbf{NP} \not\subset \mathbf{P/poly}$), but apply to more restricted models.

(Best known formula LB: $\boldsymbol{n^3/\mathrm{polylog}\, n}$) [Håstad 90s, Tal]

(Best known branching program LB: $\boldsymbol{n^2/\mathrm{polylog}\, n}$) [Nečiporuk 60s]

Hardness Magnification for MCSP

(Input length $n = 2^m$)

Theorem 2:

If MCSP$[m^{10}]$ doesn't have $n^3 \mathrm{polylog}\, n$-size (De Morgan) Formulas, then $\mathbf{PSPACE} \not\subset$ (nonuniform) $\mathbf{NC^1}$.

Similar results for other models!

Hardness Magnification for MCSP

(Input length $n = 2^m$)

Theorem 2:

> If MCSP$[m^{10}]$ doesn't have $n^3 \mathrm{polylog}\, n$-size (De Morgan) Formulas, then $\mathbf{PSPACE} \not\subset$ (nonuniform) $\mathbf{NC^1}$.

Similar results for other models!

Best MCSP lower bound (Cheraghchi-Kabanets-Lu-Myrisiotis'19) :
MCSP$[2^m/10m]$ requires $n^{3-o(1)}$-size formulas.
(doesn't work for m^{10}…)

Hardness Magnification for MCSP

(Input length $n = 2^m$)

Theorem 2:

If MCSP$[m^{10}]$ doesn't have $n^3 \mathrm{polylog}\, n$-size (De Morgan) Formulas, then $\mathbf{PSPACE} \not\subset$ (nonuniform) $\mathbf{NC^1}$.

Similar results for other models!

Best MCSP lower bound (Cheraghchi-Kabanets-Lu-Myrisiotis'19) :
MCSP$[2^m/10m]$ requires $n^{3-o(1)}$-size formulas.
(doesn't work for $m^{10}\ldots$)

Similar results for MKtP$[m^{10}]$ and $\mathbf{EXP} \not\subset \mathbf{NC^1}$ (improving upon [OPS'19] which required lower bounds for Gap-MKtP)

Algorithms with small non-uniformity

Theorem 3:

Let L be a $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language not computable by an $\boldsymbol{n^{1.01}}$**-time** $\boldsymbol{n^{0.01}}$**-space** deterministic algorithm with $\boldsymbol{n^{0.01}}$ **bits of advice**, then $\mathbf{NP} \not\subset \mathbf{SIZE}[\boldsymbol{n^k}]$ **for all** $\boldsymbol{k}$.

Algorithms with small non-uniformity

Theorem 3:

Let L be a $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language not computable by an $\boldsymbol{n^{1.01}}$**-time** $\boldsymbol{n^{0.01}}$**-space** deterministic algorithm with $\boldsymbol{n^{0.01}}$ **bits of advice**, then $\mathbf{NP} \not\subset \mathbf{SIZE}[\boldsymbol{n^k}]$ **for all** $\boldsymbol{k}$.

The hypothesis is "close" to what we can prove!

There is a $\left(\boldsymbol{2^{n^{0.01}} \cdot n}\right)$-sparse language $L \in \mathbf{DTIME}[\tilde{O}(n^{1.01})]$, not computable by an $\boldsymbol{n^{1.01}}$**-time** deterministic algorithm **with** $\boldsymbol{n^{0.01}}$ **bits of advice**.

(Adaptation of time hierarchy theorem)

Algorithms with small non-uniformity

Theorem 3:

Let L be a $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language not computable by an $\boldsymbol{n^{1.01}}$**-time** $\boldsymbol{n^{0.01}}$**-space** deterministic algorithm with $\boldsymbol{n^{0.01}}$ **bits of advice**, then $\mathbf{NP} \not\subset \mathbf{SIZE}[\boldsymbol{n^k}]$ **for all** $\boldsymbol{k}$.

The hypothesis is "close" to what we can prove!

There is a $\left(\boldsymbol{2^{n^{0.01}}} \cdot \boldsymbol{n}\right)$-sparse language $L \in \mathbf{DTIME}[\tilde{O}(n^{1.01})]$, not computable by an $\boldsymbol{n^{1.01}}$**-time** deterministic algorithm **with** $\boldsymbol{n^{0.01}}$ **bits of advice**.

(Adaptation of time hierarchy theorem)

Can we make it sparser?

Proof of Theorem 1.2

Let L be ***any*** $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language.

· If L doesn't have $\boldsymbol{n^{3.01}}$-size formulas, then **for every $\boldsymbol{k}$, $\mathbf{NP}$ doesn't have $\boldsymbol{n^k}$-size formulas**.

Proof of Theorem 1.2

Assume: $\mathbf{NP}$ has n^k-size formulas for some k.

Goal: Design $n^{3.01}$-size formulas for $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language L.

Intuition

Assume: $\mathbf{NP}$ has n^k-size formulas for some k.

Goal: Design $n^{3.01}$-size formulas for $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language L.

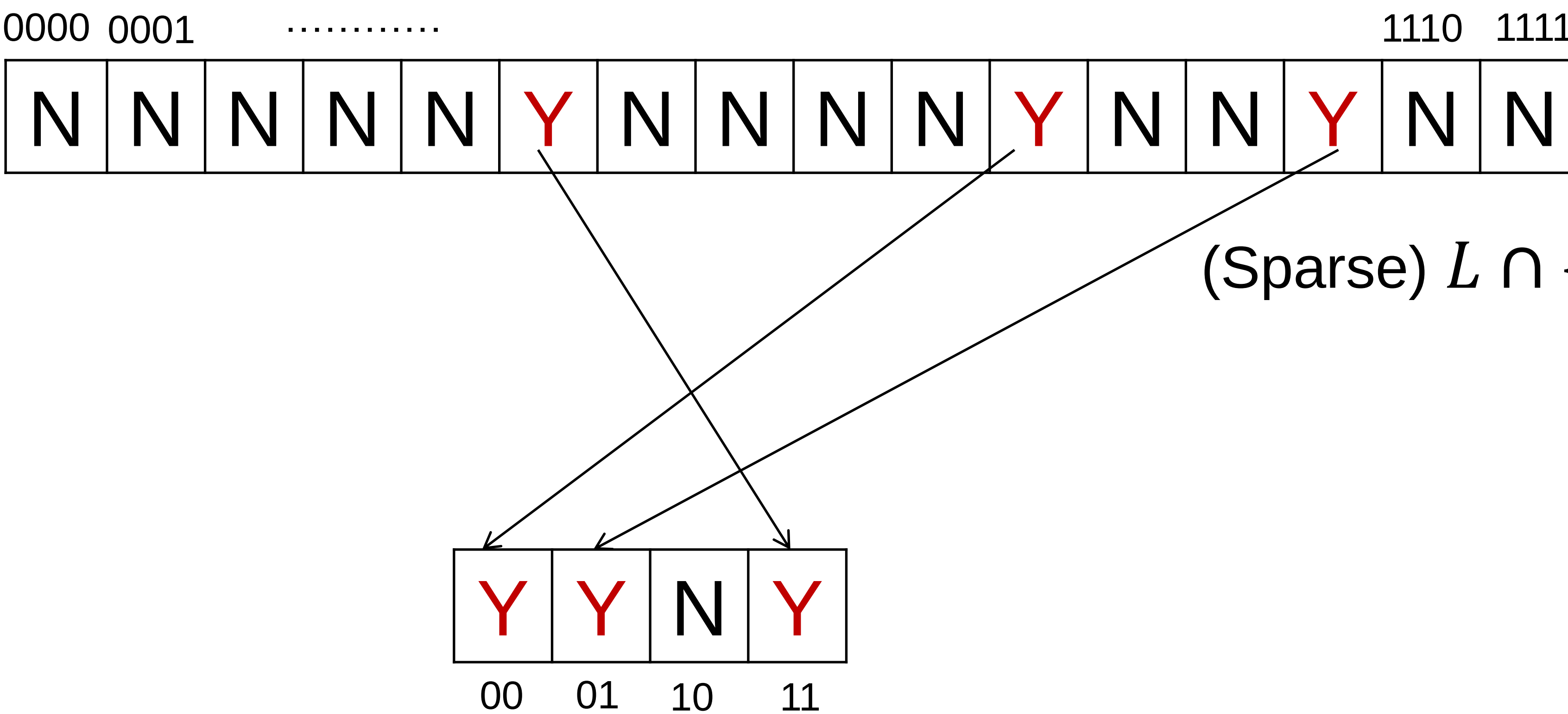
0000	0001	....												1110	1111
N	N	N	N	N	Y	N	N	N	N	Y	N	N	Y	N	N

(Sparse) $L \cap \{0,1\}^n$

Intuition

Assume: $\mathbf{NP}$ has n^k-size formulas for some k.

Goal: Design $n^{3.01}$-size formulas for $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language L.



(Sparse) $L \cap \{0,1\}^n$

(Dense) Auxiliary $\mathbf{NP}$ language $K \cap \{0,1\}^{n^{0.001/k}}$ ("kernel problem")

Intuition

Assume: $\mathbf{NP}$ has n^k-size formulas for some k.

Goal: Design $n^{3.01}$-size formulas for $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language L.

0000	0001	…………												1110	1111
N	N	N	N	N	Y	N	N	N	N	Y	N	N	Y	N	N

(Sparse) $L \cap \{0,1\}^n$

Y	Y	N	Y
00	01	10	11

We will construct cubic-size formulas for L, with oracle access to K.

(Dense) Auxiliary $\mathbf{NP}$ language $K \cap \{0,1\}^{n^{0.001/k}}$ (“kernel problem”)

Proof of Theorem 1.2

Assume: $\mathbf{NP}$ has n^k-size formulas for some k.

Goal: Design $n^{3.01}$-size formulas for $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language L.

Set $t := \boldsymbol{n^{0.001/k}} > \log(\text{Sparsity of } L)$.

Standard hashing tricks imply:

There is a hash function $H_s: \{0,1\}^n \to \{0,1\}^{O(t)}$ that is

- Perfect: maps YES-instances of L into ***distinct*** images
- described by an $O(t)$-bit seed s
- linear over $\mathbf{F}_2$

(there is a "correct" seed s that makes the hash function H_s perfect)

Proof of Theorem 1.2

Assume: $\mathbf{NP}$ has n^k-size formulas for some k.

Goal: Design $n^{3.01}$-size formulas for $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language L.

Set $t \coloneqq \boldsymbol{n^{0.001/k}} > \log(\text{Sparsity of } L)$.

Standard hashing tricks imply:

There is a hash function $H_s\colon \{0,1\}^n \to \{0,1\}^{O(t)}$ that is

- Perfect: maps YES-instances of L into ***distinct*** images
- described by an $O(t)$-b ed s
- linear over $\mathbf{F}_2$

(Construction: pick some coordinates from the Error Correcting Code)

Proof of Theorem 1.2

Assume: $\mathbf{NP}$ has n^k-size formulas for some k.

Goal: Design $n^{3.01}$-size formulas for $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language L.

$(t \coloneqq n^{0.001/k} > \log(\text{Sparsity of } L))$

(Perfect hash $H_s: \{0,1\}^n \to \{0,1\}^{O(t)}$ with seed $|s| = O(t)$)

Define an $O(t)$-input auxiliary NP problem K ("kernel problem"):

Input: Hash seed s, hash value h, index $i \in [n]$
Output: The i-th bit of ***some*** $x \in L$ such that $H_s(x) = h$.

For the "correct" s, this x is ***unique***

Proof of Theorem 1.2

Assume: $\mathbf{NP}$ has n^k-size formulas for some k.

Goal: Design $n^{3.01}$-size formulas for $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language L.

$(t := n^{0.001/k} > \log(\text{Sparsity of } L))$

(Perfect hash $H_s\colon\{0,1\}^n \to \{0,1\}^{O(t)}$ with seed $|s| = O(t)$)

Define an $O(t)$-input auxiliary NP problem K (“kernel problem”):

Input: Hash seed s, hash value h, index $i \in [n]$
Output: The i-th bit of ***some*** $x \in L$ such that $H_s(x) = h$.

$\mathbf{NP}$ has n^k-size formulas ⇒ K has formulas of size $n^{0.001}$!

Proof of Theorem 1.2

Assume: $\mathbf{NP}$ has n^k-size formulas for some k.

Goal: Design $n^{3.01}$-size formulas for $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language L.

$(t := n^{0.001/k} > \log(\text{Sparsity of } L))$

(Perfect hash $H_s: \{0,1\}^n \to \{0,1\}^{O(t)}$ with seed $|s| = O(t)$)

Define an $O(t)$-input auxiliary NP problem K ("kernel problem"):

Input: Hash seed s, hash value h, index $i \in [n]$
Output: The i-th bit of ***some*** $x \in L$ such that $H_s(x) = h$.

$\mathbf{NP}$ has n^k-size formulas ⇒ K has formulas of size $n^{0.001}$!
On input (s, h, i), guess (x, y), where y witnesses $x \in L$.
Accept ⇔ $x_i = 1$ and $H_s(x) = h$.

Proof of Theorem 1.2

Assume: $\mathbf{NP}$ has n^k-size formulas for some k.

Goal: Design $n^{3.01}$-size formulas for $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language L.

$(t := n^{0.001/k} > \log(\text{Sparsity of } L))$

(Perfect hash $H_s: \{0,1\}^n \to \{0,1\}^{O(t)}$ with seed |s| $= O(t)$)

Define an $O(t)$-input auxiliary NP problem K ("kernel problem"):

Input: Hash seed s, hash value h, index $i \in [n]$
Output: The i-th bit of ***some*** $x \in L$ such that $H_s(x) = h$.

Claim: for the "correct" s, the following decides L:

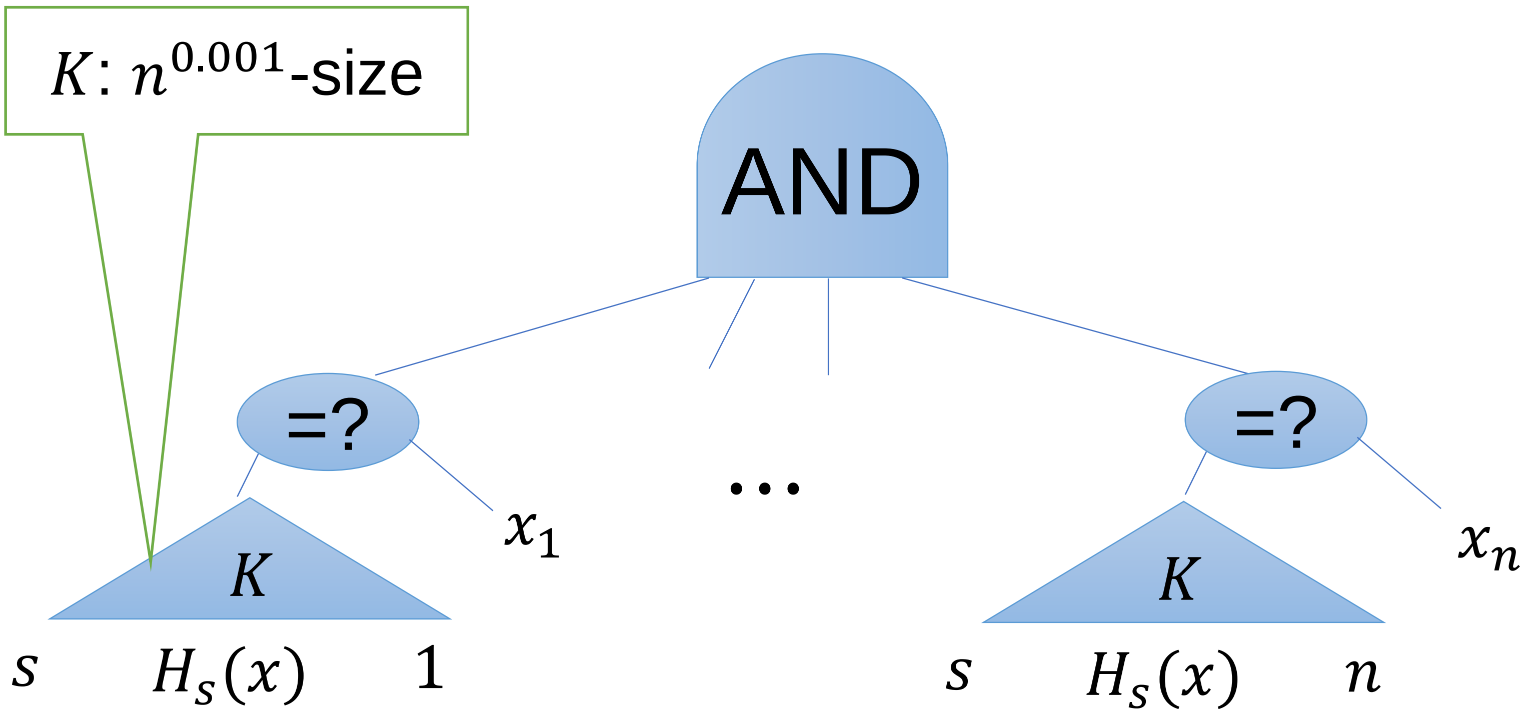
On input $x \in \{0,1\}^n$, accept iff:

$$\forall i \in [n],\ K(s, H_s(x), i) = x_i$$

Goal: Design $\boldsymbol{n^{3.01}}$-size formulas for $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language L.

On input $x \in \{0,1\}^n$, accept iff:

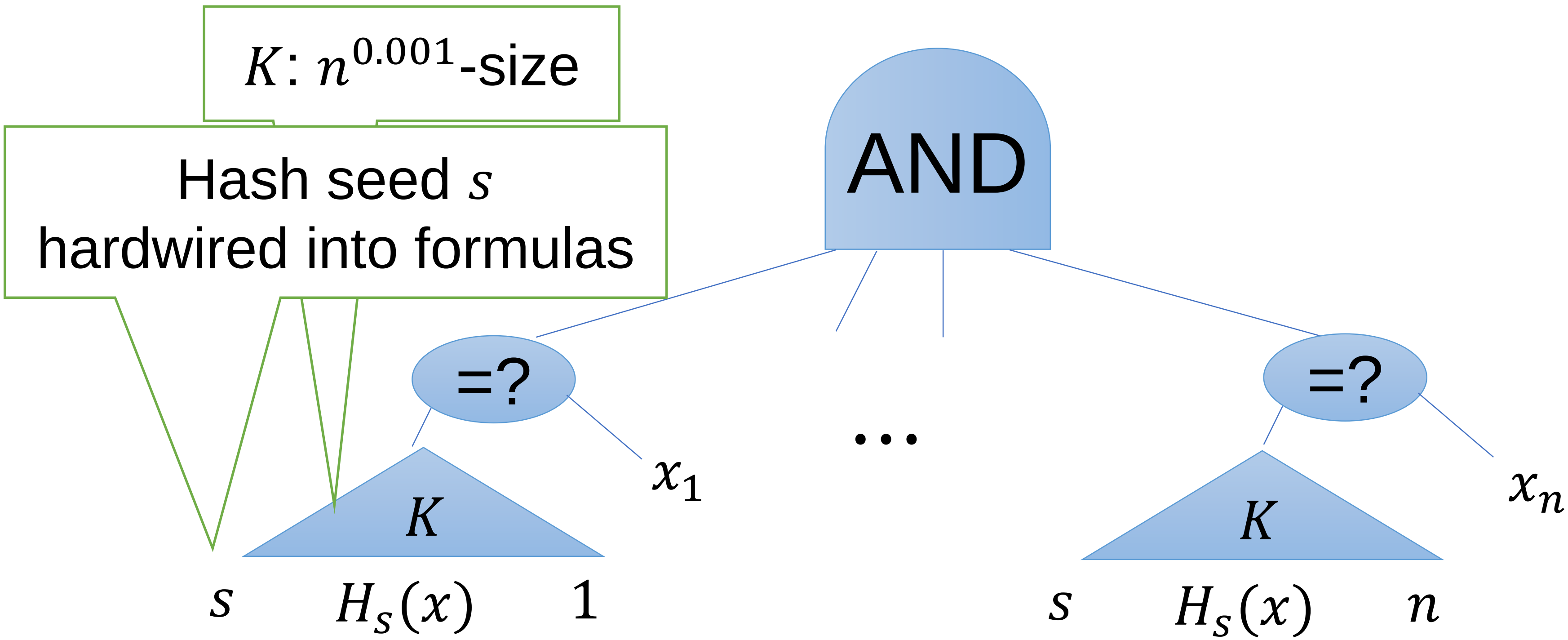
$$\forall i \in [n],\ K(s, H_s(x), i) = x_i$$



Goal: Design $\boldsymbol{n^{3.01}}$-size formulas for $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language L.

On input $x \in \{0,1\}^n$, accept iff:

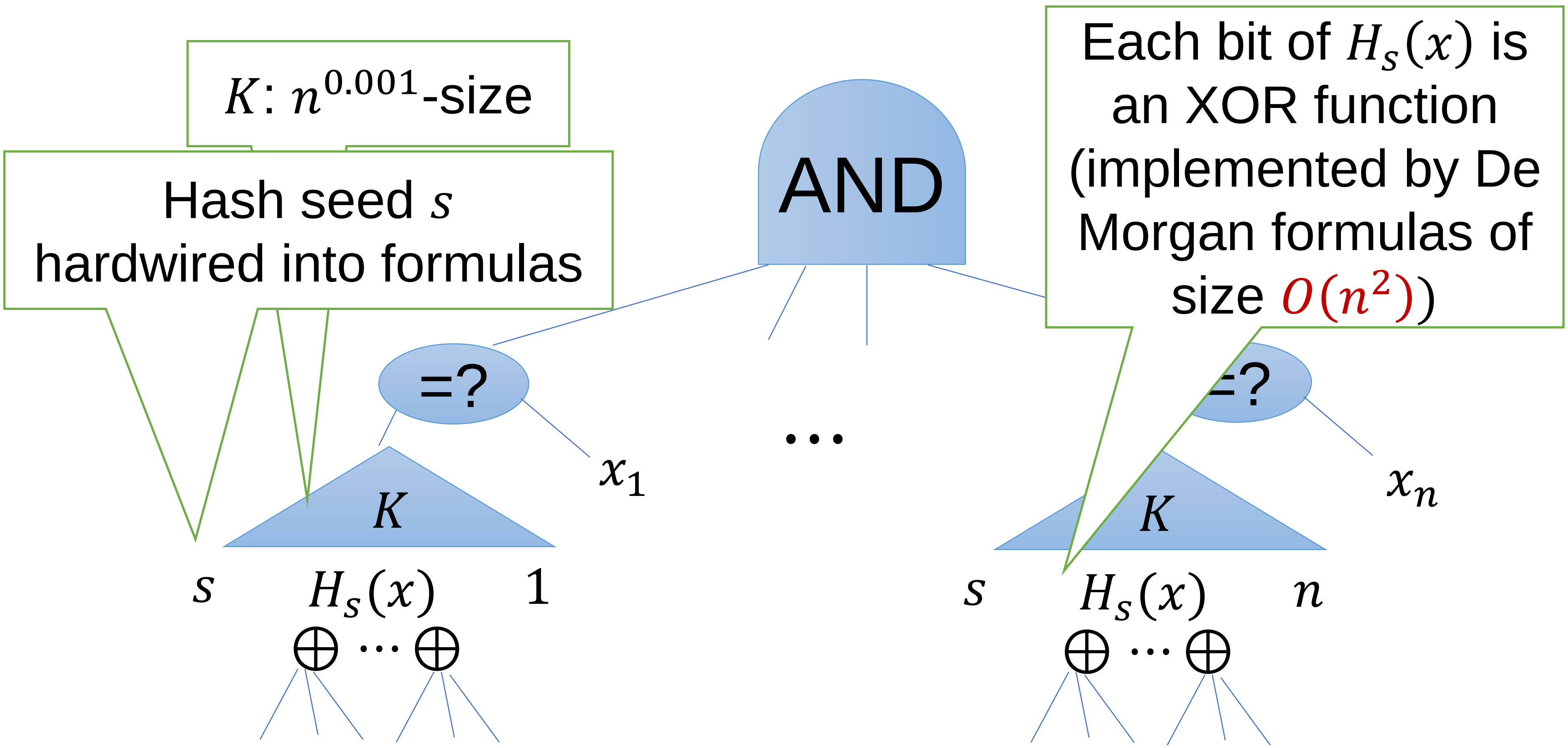
$$\forall i \in [n],\ K(s, H_s(x), i) = x_i$$



Goal: Design $\boldsymbol{n^{3.01}}$-size formulas for $2^{n^{o(1)}}$-*sparse* $\mathbf{NP}$ language L.

On input $x \in \{0,1\}^n$, accept iff:

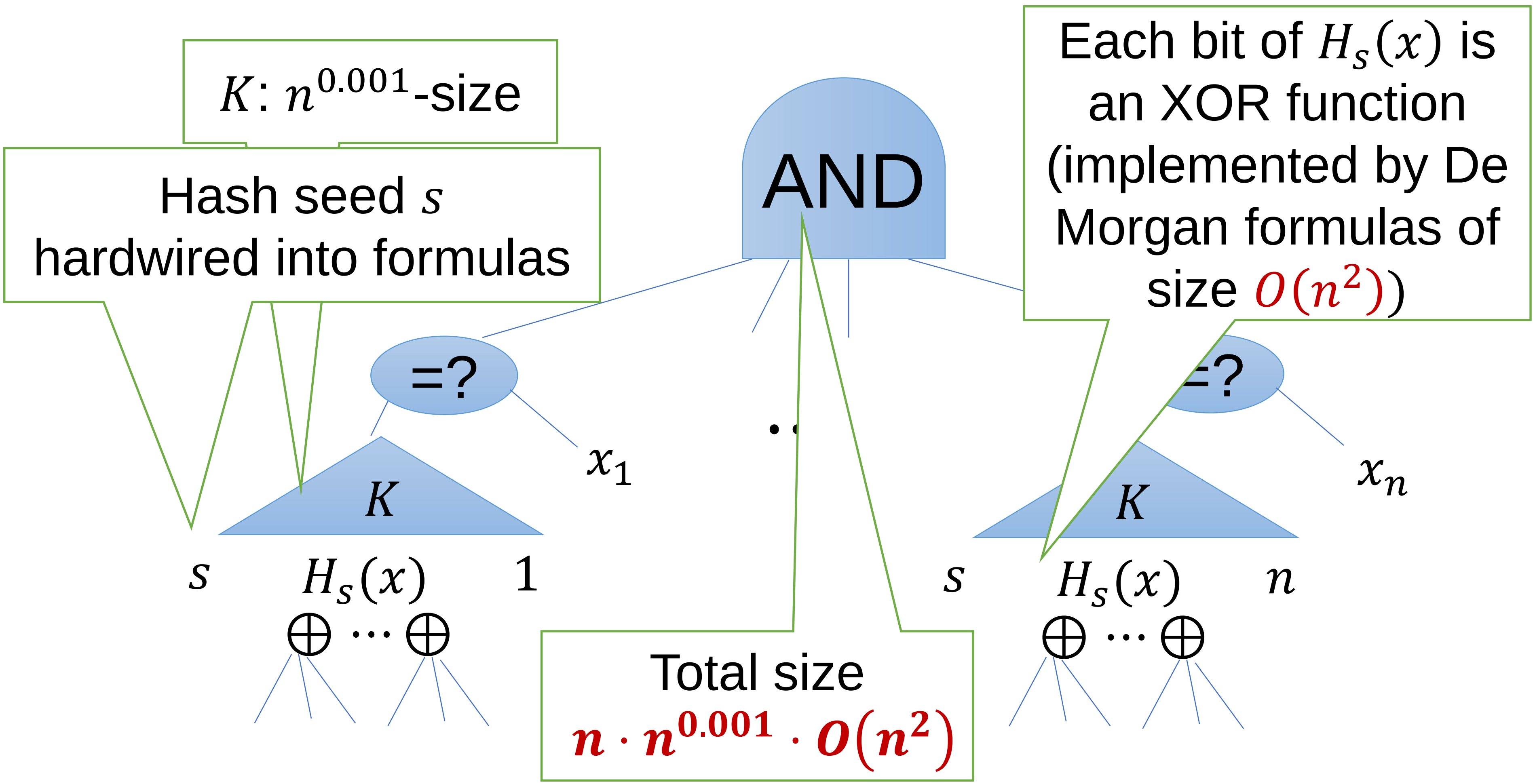
$$\forall i \in [n],\ K(s, H_s(x), i) = x_i$$



Goal: Design $n^{3.01}$-size formulas for $2^{n^{o(1)}}$-*sparse* **NP** language L.

On input $x \in \{0,1\}^n$, accept iff:

$$\forall i \in [n],\ K(s, H_s(x), i) = x_i$$



Open Problems

- Are there any **other natural sparse NP languages** for which one can prove some concrete lower bounds?

Open Problems

- Are there any **other natural sparse NP languages** for which one can prove some concrete lower bounds?

- Is it possible to show hardness magnification results for **"denser" variants of MCSP or MKtP, such as MCSP**$[2^m/m^3]$?

Open Problems

- Are there any **other natural sparse NP languages** for which one can prove some concrete lower bounds?
- Is it possible to show hardness magnification results for **"denser" variants of MCSP or MKtP, such as MCSP**$[2^m/m^3]$?

Thank you!