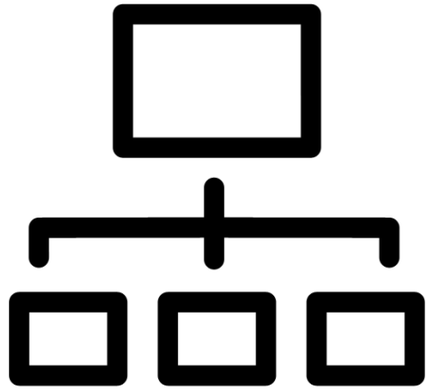
Boolean Circuits



(Contd.)

Karp-Lipton Theorem

If $NP \subseteq P_{/poly}$, then the polynomial hierarchy collapses to the second level.

$$\mathbf{NP} \subseteq \mathbf{P}_{/\mathbf{poly}} \Rightarrow \Pi_2 \subseteq \Sigma_2$$

$$\forall u \in \{0,1\}^{p(n)} \exists v \in \{0,1\}^{q(n)} \phi(u,v)$$

$$\mathbf{NP} \subseteq \mathbf{P}_{/\mathrm{poly}} \Rightarrow \Pi_2 \subseteq \Sigma_2$$

$$\forall u \in \{0,1\}^{p(n)} \exists v \in \{0,1\}^{q(n)} \phi(u,v)$$

$$\mathbf{NP} \subseteq \mathbf{P}_{/\mathbf{poly}} \Rightarrow \Pi_2 \subseteq \Sigma_2$$

$$\forall u \in \{0,1\}^{p(n)} \exists v \in \{0,1\}^{q(n)} \phi(u,v)$$

There **exists** a polynomial-sized* circuit that can *compute the certificate v.*

$$\mathbf{NP} \subseteq \mathbf{P_{/poly}} \Rightarrow \Pi_2 \subseteq \Sigma_2$$

$$\forall u \in \{0,1\}^{p(n)} \exists v \in \{0,1\}^{q(n)} \phi(u,v)$$

There **exists** a polynomial-sized* circuit that can *compute the certificate v.*

*If the size of this circuit is q(n); then it has a representation that uses at most $q^2(n)$ bits.

$$\mathbf{NP} \subseteq \mathbf{P}_{/poly} \Rightarrow \Pi_2 \subseteq \Sigma_2$$

$$\forall u \in \{0,1\}^{p(n)} \exists v \in \{0,1\}^{q(n)} \phi(u, v)$$

There **exists** a polynomial-sized* circuit that can *compute the certificate v.*

*If the size of this circuit is q(n); then it has a representation that uses at most $q^2(n)$ bits.

$$\exists w \in \{0,1\}^{q^2(n)} \forall u \{0,1\}^{p(n)} \phi(u, \quad)$$

$$\mathbf{NP} \subseteq \mathbf{P_{/poly}} \Rightarrow \Pi_2 \subseteq \Sigma_2$$

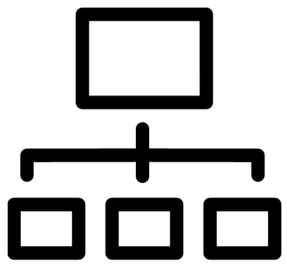
$$\forall u \in \{0,1\}^{p(n)} \exists v \in \{0,1\}^{q(n)} \phi(u,v)$$

There **exists** a polynomial-sized* circuit that can *compute the certificate v.*

*If the size of this circuit is q(n); then it has a representation that uses at most $q^2(n)$ bits.

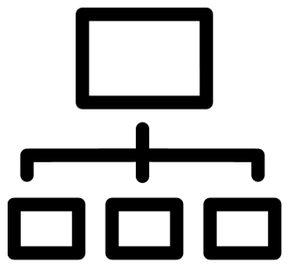
$$\exists w \in \{0,1\}^{q^2(n)} \forall u \{0,1\}^{p(n)} \phi(u, C_w(\phi, u))$$

1 iff there is a satisfying assignment that sets x_1 to 1.



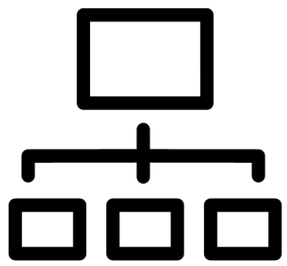
(ϕ)

1 iff there is a satisfying assignment that sets x_1 to 1.



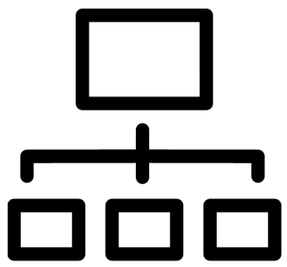
(ϕ)

1 iff there is a satisfying assignment that sets x_1 to b_1 and x_2 to 1.



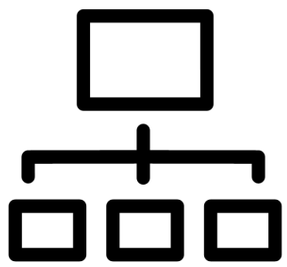
(ϕ,b_1)

1 iff there is a satisfying assignment that sets x_1 to 1.



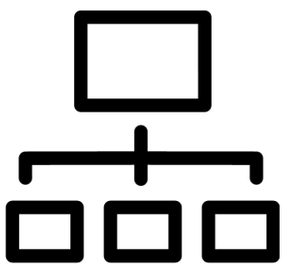
(ϕ)

1 iff there is a satisfying assignment that sets **x_1 to b_1** and x_2 to 1.



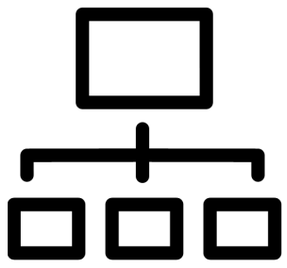
(ϕ,b_1)

1 iff there is a satisfying assignment that sets **x_1 to b_1, x_2 to b_2**, and x_3 to 1.



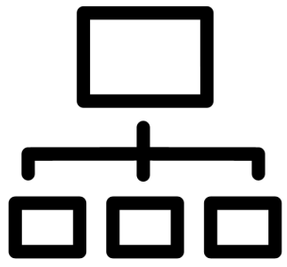
(ϕ,b_1,b_2)

1 iff there is a satisfying assignment that sets x_1 to 1.



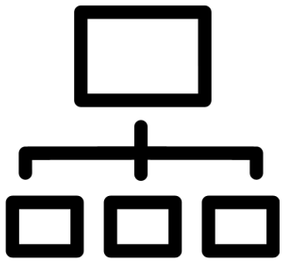
(ϕ)

1 iff there is a satisfying assignment that sets x_1 **to** b_1 and x_2 to 1.



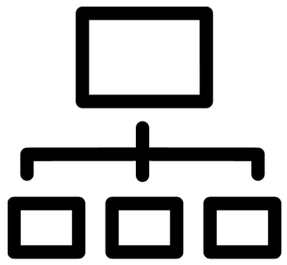
(ϕ, b_1)

1 iff there is a satisfying assignment that sets x_1 **to** b_1, x_2 **to** b_2, and x_3 to 1.



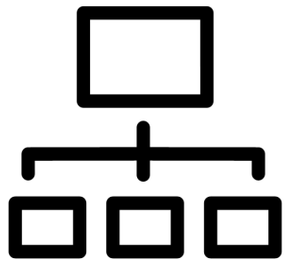
(ϕ, b_1, b_2)

1 iff there is a satisfying assignment that sets x_1 to 1.



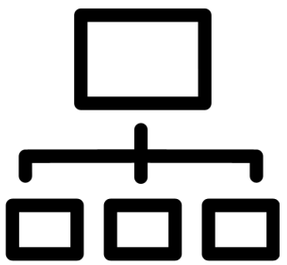
(ϕ)

1 iff there is a satisfying assignment that sets x_1 **to** b_1 and x_2 to 1.



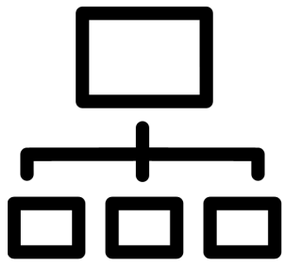
(ϕ, b_1)

1 iff there is a satisfying assignment that sets x_1 **to** b_1, x_2 **to** b_2, and x_3 to 1.



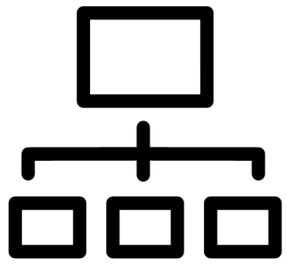
(ϕ, b_1, b_2)

1 iff there is a satisfying assignment that sets x_1 to 1.



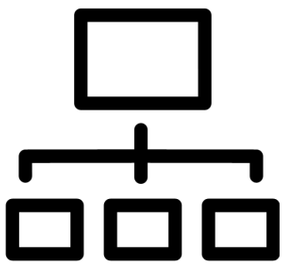
(ϕ)

1 iff there is a satisfying assignment that sets x_1 **to** b_1 and x_2 to 1.



(ϕ, b_1)

1 iff there is a satisfying assignment that sets x_1 **to** b_1, x_2 **to** b_2, and x_3 to 1.



(ϕ, b_1, b_2)

C_1 C_2 C_3 ...

A Simple Lower Bound

There exists a boolean function

$$f : \{0,1\}^n \to \{0,1\}$$

that cannot be computed by circuits of size

_____

Space of *all* boolean functions

$$f : \{0,1\}^n \to \{0,1\}$$

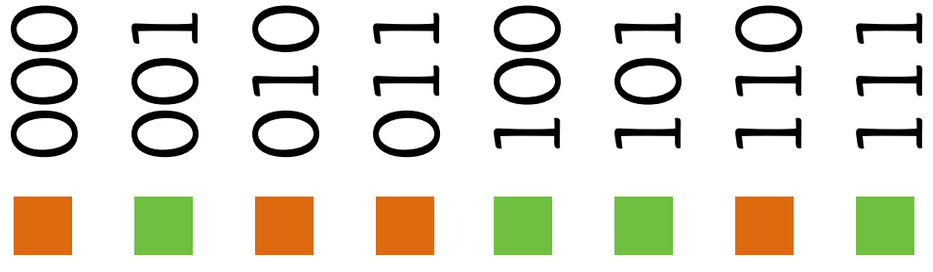
Space of *all* boolean functions

$$f : \{0,1\}^n \to \{0,1\}$$

000
001
010
011
100
101
110
111

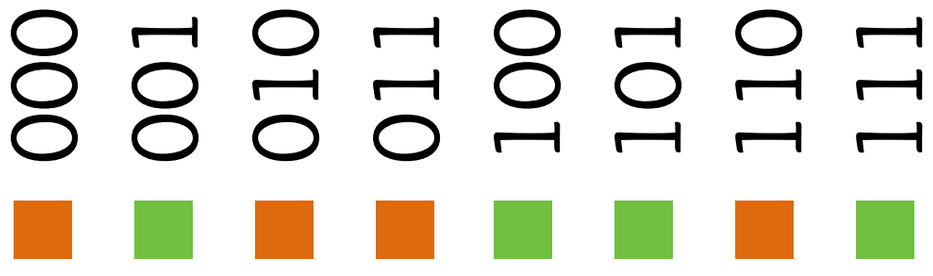
Space of *all* boolean functions

$$f : \{0,1\}^n \to \{0,1\}$$



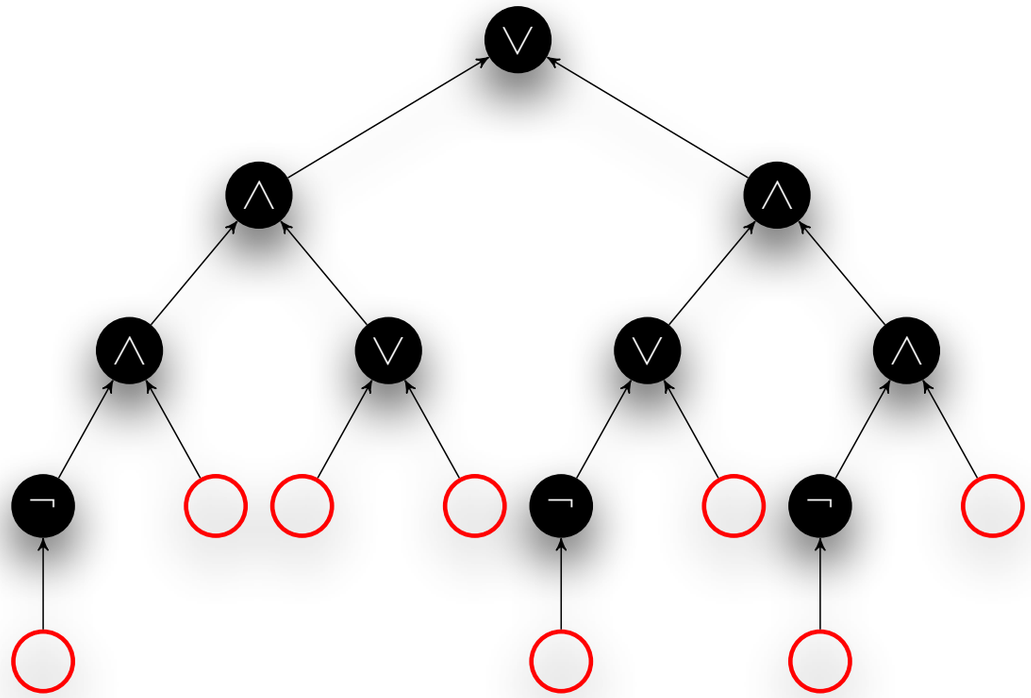
Space of *all* boolean functions

$$f : \{0,1\}^n \to \{0,1\}$$

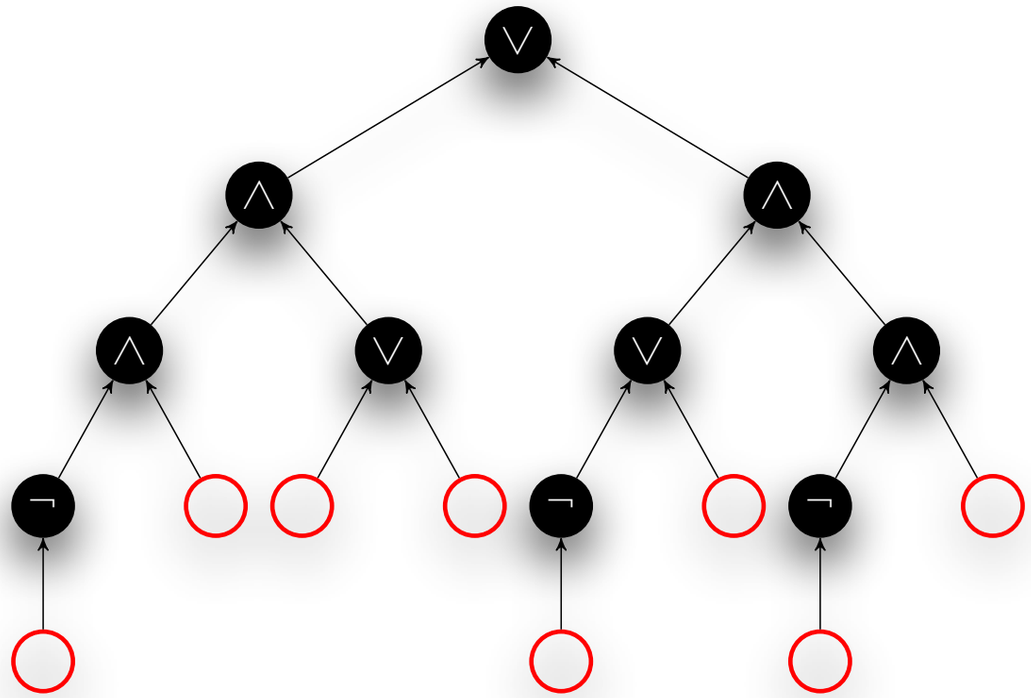


Number of these functions: 2^{2^n}

Space of *all* boolean circuits



Space of *all* boolean circuits



Number of these circuits: $2^{ct \log t}$

2^{2^n}

Boolean
Functions

$2^{ct \log t}$

Boolean
Circuits

2^{2^n}

Boolean
Functions

$2^{ct \log t}$

Boolean
Circuits

Let $t = 2^n/n$

2^{2^n}

Boolean
Functions

$2^{ct \log t}$

Boolean
Circuits

Let $t = 2^n/n(c+1)$

There exists a boolean function

$$f : \{0,1\}^n \to \{0,1\}$$

that cannot be computed by circuits of size

$$\_\_\_\_\_$$

There exists a boolean function

$$f : \{0,1\}^n \to \{0,1\}$$

that cannot be computed by circuits of size

$$2^n/10n$$

Non-Uniform Hierarchy Theorem

$h(n) < g(n)$

Non-Uniform Hierarchy Theorem

For g(n) “bigger” than h(n), we have:

$$\mathbf{SIZE}(h(n)) \subsetneq \mathbf{SIZE}(g(n))$$

$$h(n) < g(n)$$

Non-Uniform Hierarchy Theorem

For g(n) “bigger” than h(n), we have:

$$\mathbf{SIZE}(h(n)) \subsetneq \mathbf{SIZE}(g(n))$$

$$h(n) < g(n) < 2^n/n$$

Non-Uniform Hierarchy Theorem

For g(n) “bigger” than h(n), we have:

$$\mathbf{SIZE}(h(n)) \subsetneq \mathbf{SIZE}(g(n))$$

$$n < h(n) < g(n) < 2^n/n$$

Any boolean function from $\{0,1\}^n$ to $\{0,1\}$
can be decided by circuits of size 2^n.

Any boolean function from $\{0,1\}^n$ to $\{0,1\}$
can be decided by circuits of size 2^n.

There exists boolean function from $\{0,1\}^n$ to $\{0,1\}$
cannot be decided by circuits of size $2^n/10n$.

$$\mathbf{SIZE}(n) \subsetneq \mathbf{SIZE}(n^2)$$

$$\mathbf{SIZE}(n) \subsetneq \mathbf{SIZE}(n^2)$$

Any boolean function from $\{0,1\}^{2\log n}$ to $\{0,1\}$
can be decided by circuits of size n^2.

$$\mathbf{SIZE}(n) \subsetneq \mathbf{SIZE}(n^2)$$

Any boolean function from $\{0,1\}^{2\log n}$ to $\{0,1\}$ **can** be decided by circuits of size n^2.

There exists boolean function from $\{0,1\}^{2\log n}$ to $\{0,1\}$ **cannot** be decided by circuits of size $n^2/2(\log n)$.

Definition

Definition

The class NC.

Definition

The class NC.

A language L is **NC^d** if L can be decided by a family of circuits $\{C_n\}$ where C_n has:

- poly(n) size and
- depth $O(\log^d n)$.

Definition

The class NC.

A language L is **NC^d** if L can be decided by a family of circuits $\{C_n\}$ where C_n has:

- poly(n) size and
- depth $O(\log^d n)$.

The class **NC** is $U_{i\geq 1} NC^i$.

Definition

Definition

The class AC.

Definition

The class AC.

The class $\mathbf{AC}^i$ is defined similarly to $\mathbf{NC}^i$ except that gates are allowed to have unbounded fan-in.

Definition

The class AC.

The class $\mathbf{AC}^i$ is defined similarly to $\mathbf{NC}^i$ except that gates are allowed to have unbounded fan-in.

The class **AC** is $U_{i\geq 0}NC^i$.

Definition

The class AC.

The class $\mathbf{AC^i}$ is defined similarly to $\mathbf{NC^i}$ except that gates are allowed to have unbounded fan-in.

The class $\mathbf{AC}$ is $U_{i\geq 0}NC^i$.

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

Definition

The class AC.

The class $\mathbf{AC^i}$ is defined similarly to $\mathbf{NC^i}$ except that gates are allowed to have unbounded fan-in.

The class $\mathbf{AC}$ is $U_{i\geq 0}NC^i$.

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

Parity is in $\mathbf{NC^1}$.

Does every problem in P admit an efficient parallel implementation?

In other words, is P = **NC**?

Definition

P-Completeness

A language is P-complete if it is in P
and every language in P
is **log-space reducible** to it.

P-Completeness: Consequences

Let L be a P-complete language. Then,

L belongs to **NC** if and only if P = **NC.**
L belongs to **L** if and only if P = **L.**

(**L** is the class of all languages that can be decided in log-space.)

GOAL

GOAL

SAT cannot be solved in polynomial time *and* poly-logarithmic space.

Definition

Definition

TISP(T(n),S(n)**)** := the set of languages decided by a TM M that on *every* input x:

- takes at most O(T(n)) steps, and,
- uses at most O(S(n)) cells of its read-write tape;

where n := |x|.

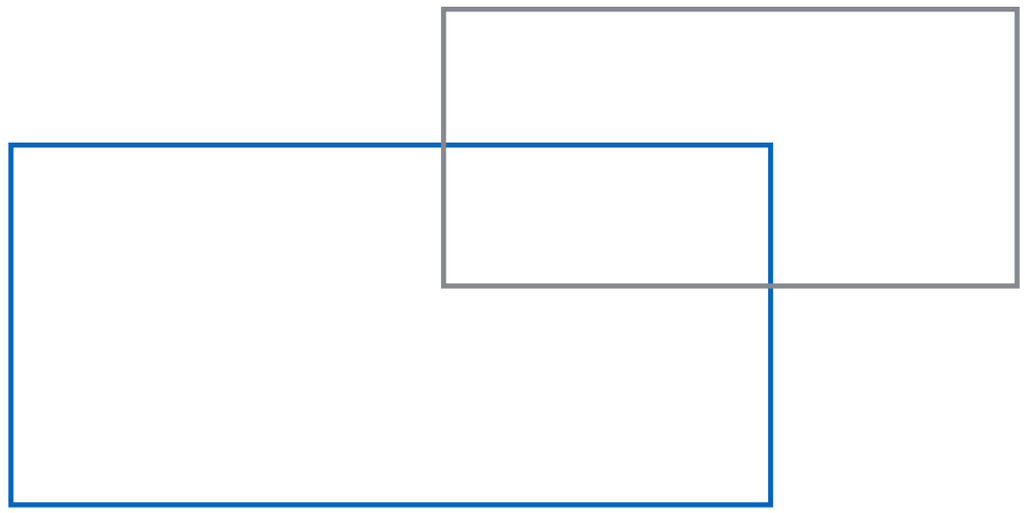
PLAN

PLAN

$$\mathbf{NTIME}(n) \not\subseteq \mathbf{TISP}(n^{1.2}, n^{0.2})$$

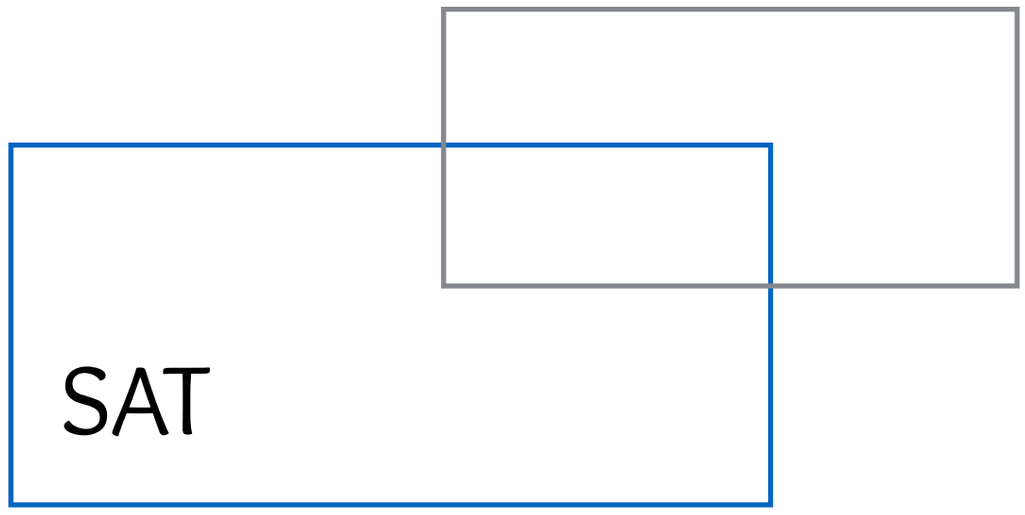
PLAN

$\mathbf{NTIME}(n) \not\subseteq \mathbf{TISP}(n^{1.2}, n^{0.2})$



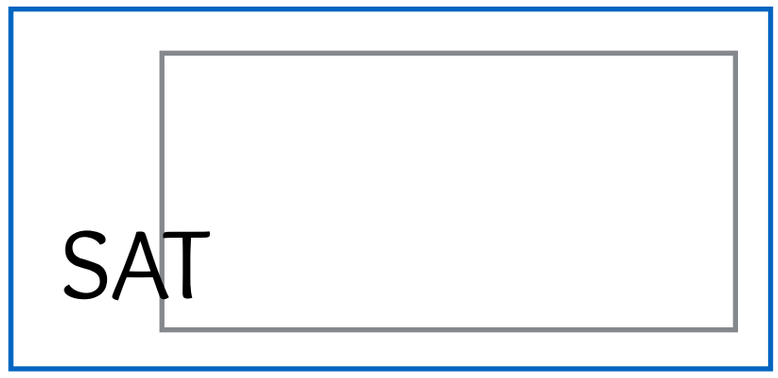
PLAN

$\mathbf{NTIME}(n) \not\subseteq \mathbf{TISP}(n^{1.2}, n^{0.2})$



PLAN

$\mathbf{NTIME}(n) \not\subseteq \mathbf{TISP}(n^{1.2}, n^{0.2})$



(Cook-Levin)

Roadmap

$$\mathbf{NTIME}(n) \subseteq \mathbf{TISP}(n^{1.2}, n^{0.2})$$

Roadmap

$$\mathbf{NTIME}(n) \subseteq \mathbf{TISP}(n^{1.2}, n^{0.2})$$

$$\mathbf{NTIME}(n^{10}) \subseteq \mathbf{TISP}(n^{12}, n^{2})$$

Roadmap

$$\mathbf{NTIME}(n) \subseteq \mathbf{TISP}(n^{1.2}, n^{0.2})$$

$$\mathbf{NTIME}(n^{10}) \subseteq \mathbf{TISP}(n^{12}, n^{2})$$

$$\mathbf{TISP}(n^{12}, n^{2}) \subseteq \Sigma_2\mathrm{TIME}(n^{8})$$

Roadmap

$$\mathbf{NTIME}(n) \subseteq \mathbf{TISP}(n^{1.2}, n^{0.2})$$

$$\mathbf{NTIME}(n^{10}) \subseteq \mathbf{TISP}(n^{12}, n^{2})$$

$$\mathbf{TISP}(n^{12}, n^{2}) \subseteq \Sigma_2\mathrm{TIME}(n^{8})$$

$$\Sigma_2\mathrm{TIME}(n^{8}) \subseteq \mathbf{NTIME}(n^{9.6})$$

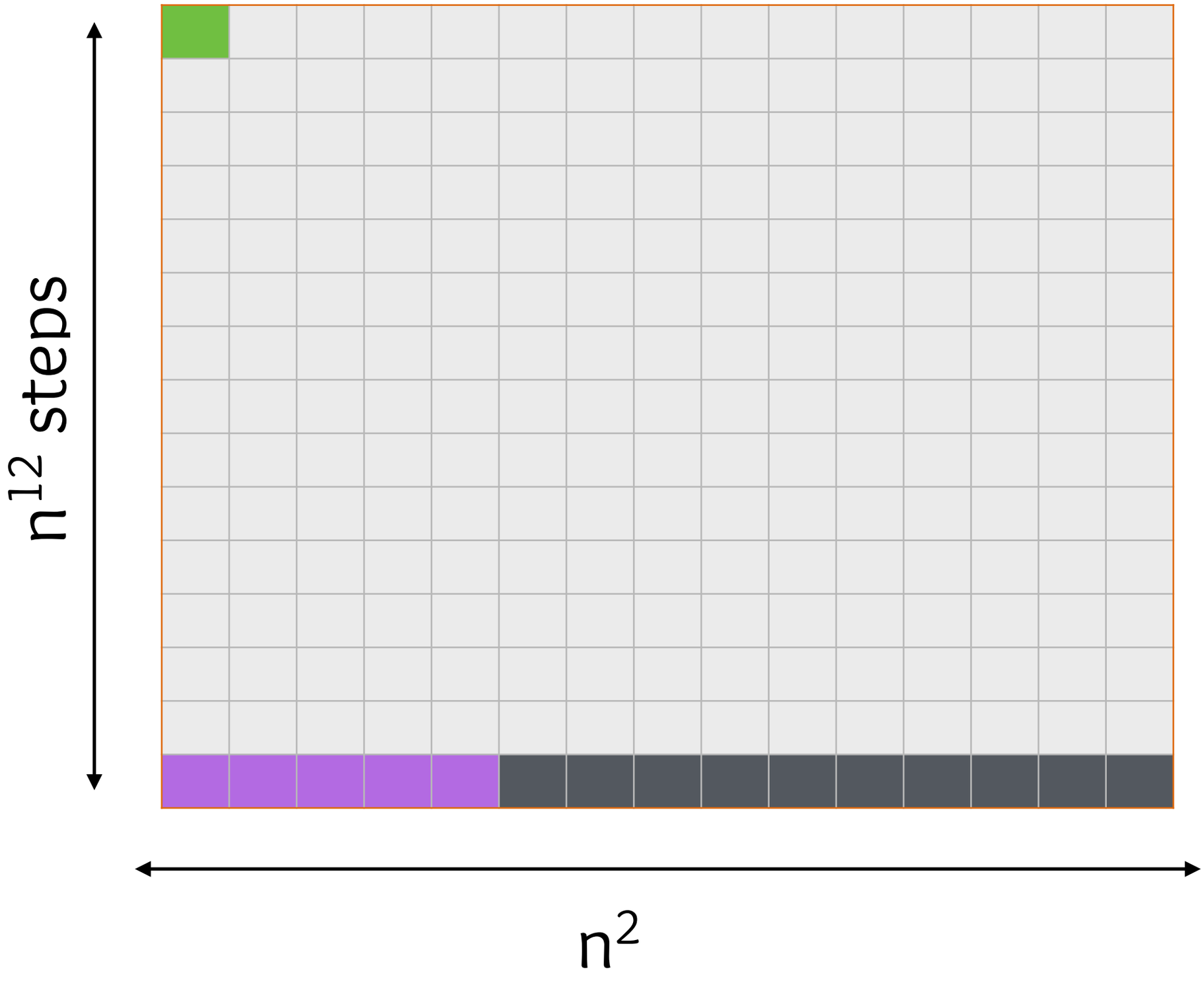
Roadmap

$$\mathbf{NTIME}(n) \subseteq \mathbf{TISP}(n^{1.2}, n^{0.2})$$

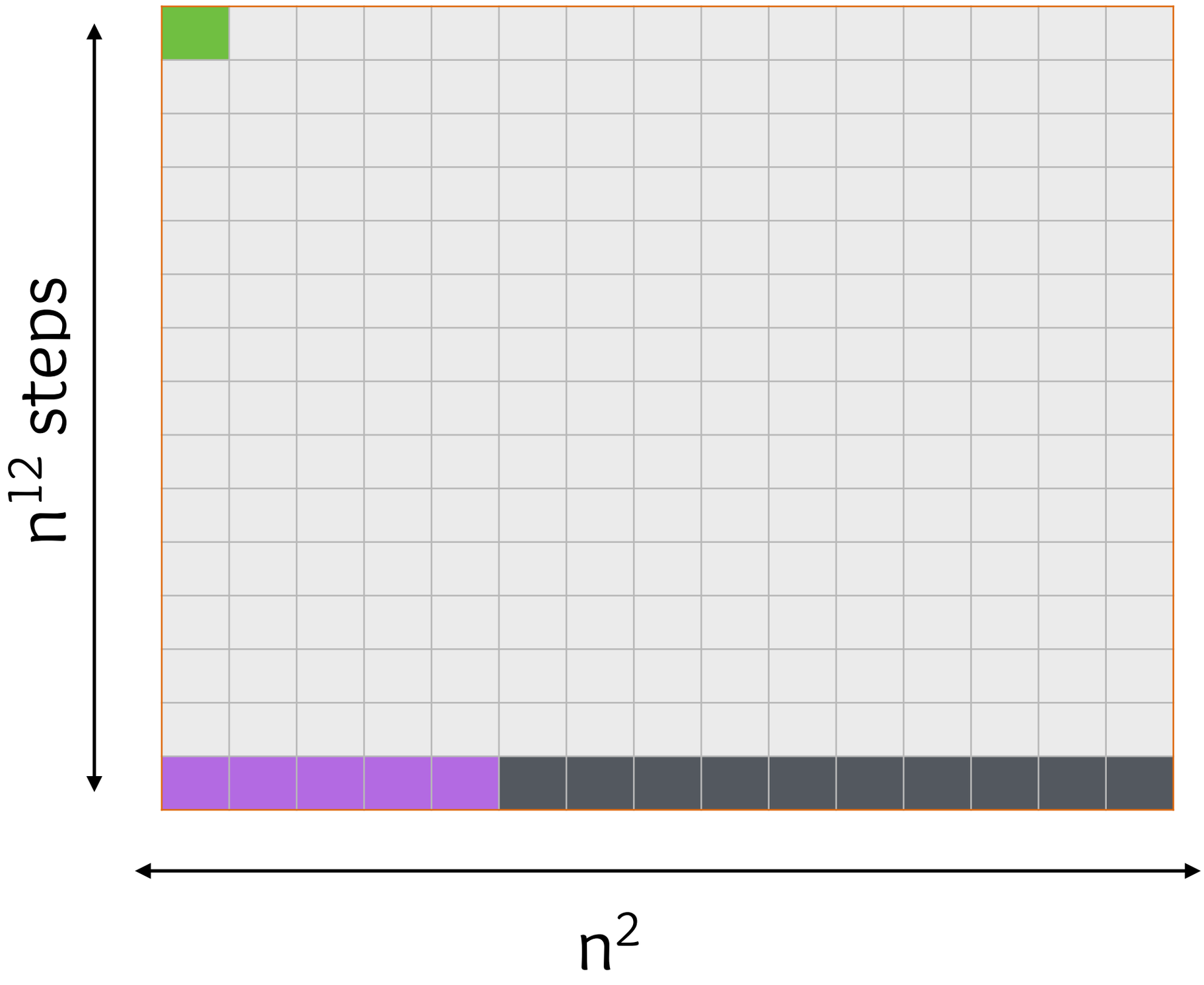
$$\mathbf{NTIME}(n^{10}) \subseteq \mathbf{TISP}(n^{12}, n^{2})$$

$$\mathbf{TISP}(n^{12}, n^{2}) \subseteq \Sigma_2\mathrm{TIME}(n^{8})$$

$$\Sigma_2\mathrm{TIME}(n^{8}) \subseteq \mathbf{NTIME}(n^{9.6})$$


n^{12} steps
n^2

$$\mathbf{TISP}(n^{12},n^2) \subseteq \Sigma_2\mathrm{TIME}(n^8)$$



The configuration graph has:

1. nodes that require n^2 bits to describe,
2. an accepting path of length at most n^{12} on inputs that belong to L

$$\mathbf{TISP}(n^{12},n^2) \subseteq \Sigma_2\mathrm{TIME}(n^8)$$

[there exists, for all]

$$\mathbf{TISP}(n^{12},n^2) \subseteq \Sigma_2\mathrm{TIME}(n^8)$$

[there exists, for all]

there exists a path from $\mathbf{C_{start}}$ to $\mathbf{C_{end}}$
of length at most n^{12}.

$$\mathbf{TISP}(n^{12},n^2) \subseteq \Sigma_2\mathrm{TIME}(n^8)$$

[there exists, for all]

there exists a path from $\mathbf{C_{start}}$ to $\mathbf{C_{end}}$
of length at most n^{12}.

$$\mathbf{TISP}(n^{12},n^2) \subseteq \Sigma_2\mathrm{TIME}(n^8)$$

[there exists, for all]

there exists a path from $\mathbf{C_{start}}$ to $\mathbf{C_{end}}$
of length at most n^{12}.

$$\mathbf{TISP}(n^{12},n^2) \subseteq \Sigma_2\mathrm{TIME}(n^8)$$

[there exists, for all]

there exists a path from $\mathbf{C_{start}}$ to $\mathbf{C_{end}}$
of length at most n^{12}.

---

there exists a path from $\mathbf{C_{start}}$ to $\mathbf{C_{end}}$
via $C_1, C_2, \ldots, C_t$, where
for all i,
C_i is reachable from C_{i-1} in n^6 steps.

$$\mathbf{NTIME}(n) \subseteq \mathbf{TISP}(n^{1.2}, n^{0.2})$$

$$\mathbf{NTIME}(n) \subseteq \mathbf{DTIME}(n^{1.2})$$

$$\mathbf{NTIME}(n) \subseteq \mathbf{TISP}(n^{1.2}, n^{0.2})$$

$$\mathbf{NTIME}(n) \subseteq \mathbf{DTIME}(n^{1.2})$$

$$\Sigma_2\mathrm{TIME}(n^8) \subseteq \mathbf{NTIME}(n^{9.6})$$

$$\mathbf{NTIME}(n) \subseteq \mathbf{TISP}(n^{1.2}, n^{0.2})$$

$$\mathbf{NTIME}(n) \subseteq \mathbf{DTIME}(n^{1.2})$$

$$\Sigma_2\mathrm{TIME}(n^8) \subseteq \mathbf{NTIME}(n^{9.6})$$

[Proof on board]