Towards P≠NP from Extended Frege lower bounds

Ján Pich

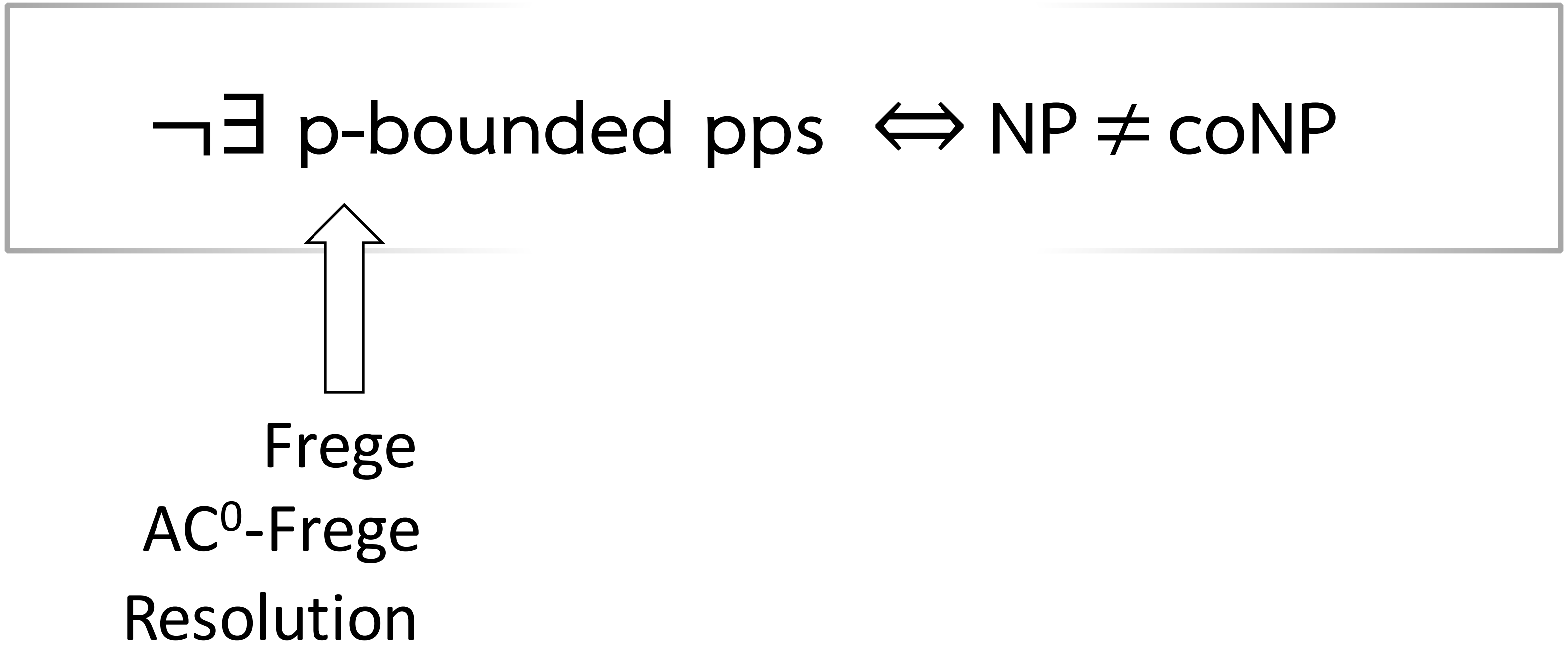
University of Oxford

joint work with **Rahul Santhanam**

Proof complexity

$\neg\exists$ p-bounded pps $\Leftrightarrow$ NP $\neq$ coNP

Proof complexity



$\neg\exists$ p-bounded pps $\Leftrightarrow$ NP $\neq$ coNP

Frege

AC^0-Frege

Resolution

Proof complexity

$\neg\exists$ p-bounded pps $\Leftrightarrow$ NP $\neq$ coNP

$\Uparrow$

Frege

AC^0-Frege

Resolution

Cook-Reckhow program

Proof complexity

$\neg\exists$ p-bounded pps $\Leftrightarrow$ NP $\neq$ coNP

⇑

Frege

AC^0-Frege

Resolution

Cook-Reckhow program

Cook-Reckhow program

$\neg\exists$ p-bounded pps $\Leftrightarrow$ NP $\neq$ coNP

Frege

AC^0-Frege

Resolution

EF lower bounds $\overset{?}{\Rightarrow}$ P $\neq$ NP

Cook-Reckhow program

$\neg\exists$ p-bounded pps $\Leftrightarrow$ NP $\neq$ coNP

Frege

AC^0-Frege

Resolution

lifting $\Rightarrow$ monotone P/poly lbs

IPS lb $\Rightarrow$ VP$\neq$VNP

R lb $\Rightarrow$ P$\neq$NP T_R -consistent

EF lower bounds $\overset{?}{\Rightarrow}$ P $\neq$ NP

Cook-Reckhow program

$\neg\exists$ p-bounded pps $\Leftrightarrow$ NP $\neq$ coNP

$\Uparrow$

Frege

AC^0-Frege

Resolution

lifting $\Rightarrow$ monotone P/poly lbs

IPS lb $\Rightarrow$ VP$\neq$VNP

R lb $\Rightarrow$ P$\neq$NP T_R -consistent

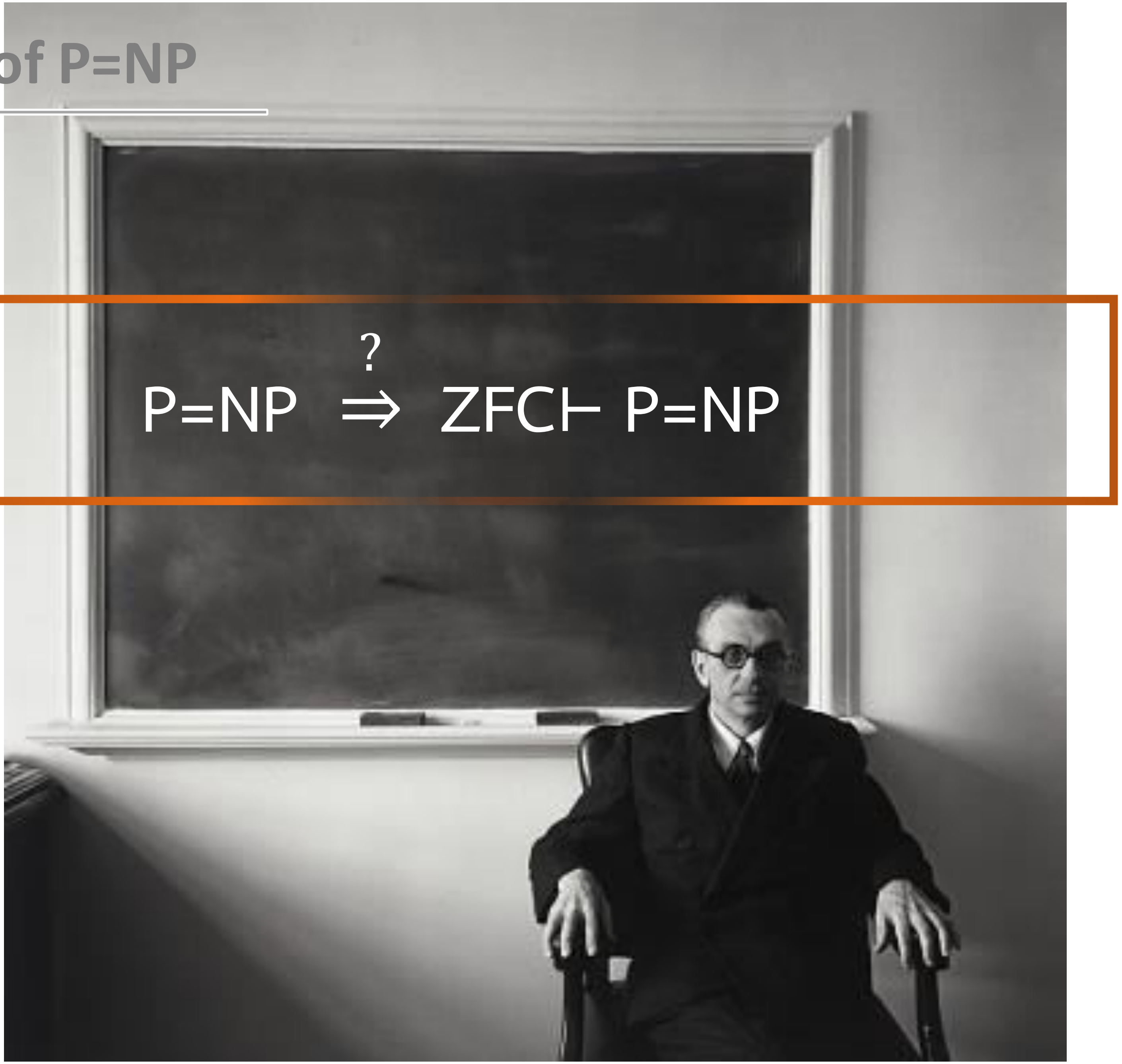
EF lower bounds $\overset{?}{\Rightarrow}$ P $\neq$ NP

Impagliazzo’s worlds shortly before collision

Proof complexity

Impagliazzo’s worlds shortly before collision

Self-provability of P=NP



$$P=NP \overset{?}{\Rightarrow} ZFC\vdash P=NP$$

Self-provability of P=NP

$\mathsf{SAT}_n(x, y) \equiv$ “formula x satisfied by assignment y”

Witnessing P $\neq$ NP

$$\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{10k}] \quad \overset{?}{\Rightarrow} \quad \begin{array}{l} \exists \text{ p-time } f \text{ s.t. } \forall C \in \mathsf{Circuit}[n^k] \\ \mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C))) \end{array}$$

Self-provability of P=NP

$\mathsf{SAT}_n(x, y)$ ≡ “formula x satisfied by assignment y”

Witnessing P ≠ NP

$$\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{10k}] \overset{?}{\Rightarrow} \exists \text{ p-time } f \text{ s.t. } \forall C \in \mathsf{Circuit}[n^k]$$

$$\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))$$

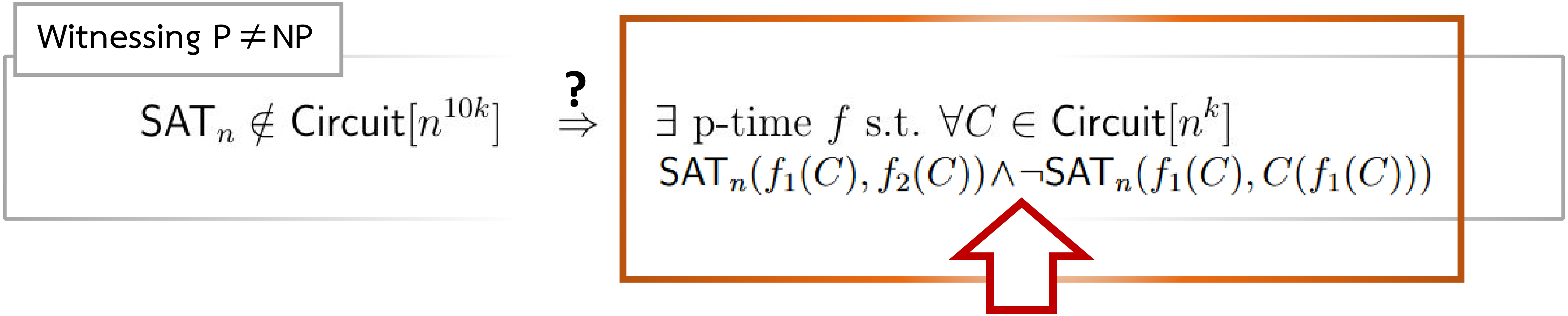
random

⇩

$$h \text{ is one-way} \Rightarrow \text{“}h(x) = h(a)\text{” is a hard } \mathsf{SAT}\text{-instance}$$

Self-provability of P=NP

$\mathsf{SAT}_n(x, y) \equiv$ "formula x satisfied by assignment y"



Witnessing P $\neq$ NP

$$\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{10k}] \overset{?}{\Rightarrow}$$

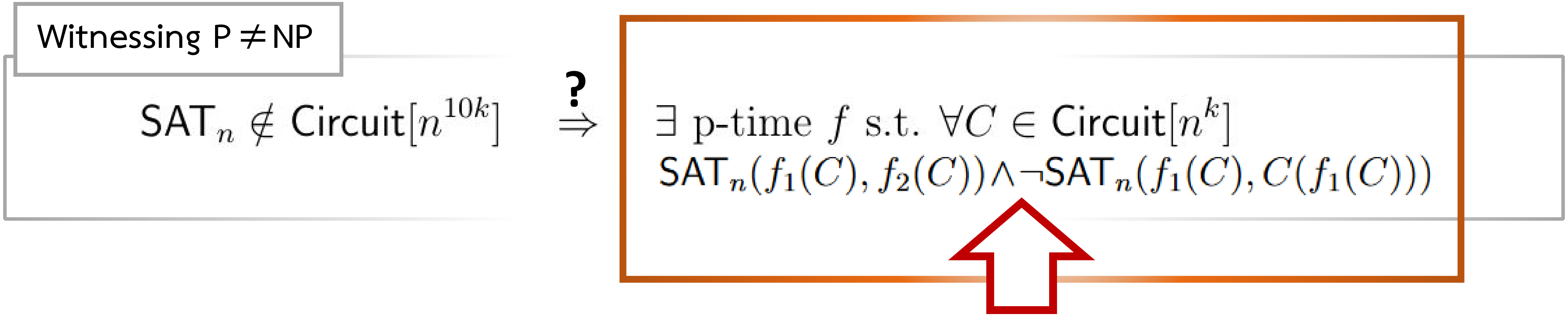
$$\exists \text{ p-time } f \text{ s.t. } \forall C \in \mathsf{Circuit}[n^k]$$
$$\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))$$

h is one-way $\Rightarrow$ "$h(x) = h(a)$" is a hard SAT-instance

E hard for subexponential-size circuits

Self-provability of P=NP

$\mathsf{SAT}_n(x,y) \equiv$ "formula x satisfied by assignment y"



Witnessing P$\neq$NP

$$\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{10k}] \overset{?}{\Rightarrow} \exists \text{ p-time } f \text{ s.t. } \forall C \in \mathsf{Circuit}[n^k]$$

$$\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))$$

h is one-way $\Rightarrow$ "$h(x) = h(a)$" is a hard SAT-instance

E hard for subexponential-size circuits

[Gutfreund Shaltiel Ta-Shma]-style constructions in uniform setting

Self-provability of P=NP

$\mathsf{SAT}_n(x,y)$ ≡ "formula x satisfied by assignment y"

Witnessing P $\neq$ NP

$$\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{10k}] \overset{?}{\Rightarrow} \exists \text{ p-time } f \text{ s.t. } \forall C \in \mathsf{Circuit}[n^k]$$
$$\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))$$

$\exists$ p-time f s.t. $w_n^k(f) \in \mathsf{TAUT}$?

$$w_n^k(f) := [\mathsf{SAT}_n(x,y) \rightarrow \mathsf{SAT}_n(x, C(x))] \vee [\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))]$$

variables: x, y, C

Self-provability of P=NP

$\mathsf{SAT}_n(x, y) \equiv$ “formula x satisfied by assignment y”

Witnessing P $\neq$ NP

$$\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{10k}] \overset{?}{\Rightarrow} \exists \text{ p-time } f \text{ s.t. } \forall C \in \mathsf{Circuit}[n^k] \; \mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))$$

$\exists$ p-time f s.t. $w_n^k(f) \in \mathsf{TAUT}$?

$$w_n^k(f) := [\mathsf{SAT}_n(x, y) \rightarrow \mathsf{SAT}_n(x, C(x))] \vee [\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))]$$

variables: x, y, C

$\Uparrow$

encodes n^k-size circuits

Self-provability of P=NP

$\mathsf{SAT}_n(x, y) \equiv$ "formula x satisfied by assignment y"

Witnessing P $\neq$ NP

$$\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{10k}] \overset{?}{\Rightarrow} \exists \text{ p-time } f \text{ s.t. } \forall C \in \mathsf{Circuit}[n^k]$$

$$\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))$$

$\exists$ p-time f s.t. $w_n^k(f) \in \mathsf{TAUT}$?

$$w_n^k(f) := [\mathsf{SAT}_n(x, y) \to \mathsf{SAT}_n(x, C(x))] \vee [\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))]$$

variables: x, y, C

⇧

encodes n^k-size circuits

$w_n^k(f) \in \mathsf{TAUT}$

⇩

$\mathsf{EF} + w^k(f)$

Self-provability of P=NP

$\mathsf{SAT}_n(x,y) \equiv$ "formula x satisfied by assignment y"

Witnessing P $\neq$ NP

$\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{10k}] \overset{?}{\Rightarrow} \exists$ p-time f s.t. $\forall C \in \mathsf{Circuit}[n^k]$
$\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))$

$\exists$ p-time f s.t. $w_n^k(f) \in \mathsf{TAUT}$?

$$w_n^k(f) := [\mathsf{SAT}_n(x,y) \to \mathsf{SAT}_n(x, C(x))] \vee [\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))]$$

variables: x, y, C

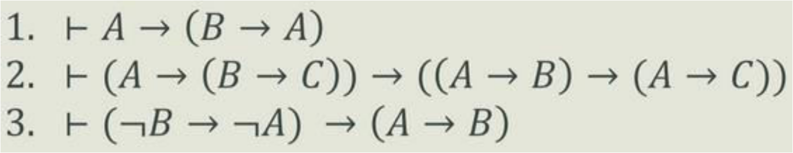
$\Uparrow$

encodes n^k-size circuits

$$w_n^k(f) \in \mathsf{TAUT}$$

$$\Downarrow$$

$$\mathsf{EF} + w^k(f)$$



1. $\vdash A \to (B \to A)$
2. $\vdash (A \to (B \to C)) \to ((A \to B) \to (A \to C))$
3. $\vdash (\neg B \to \neg A) \to (A \to B)$

Self-provability of P=NP

$\mathsf{SAT}_n(x,y) \equiv$ "formula x satisfied by assignment y"

Witnessing P $\neq$ NP

$$\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{10k}] \quad \overset{?}{\Rightarrow} \quad \exists \text{ p-time } f \text{ s.t. } \forall C \in \mathsf{Circuit}[n^k]$$
$$\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))$$

$\exists$ p-time f s.t. $w_n^k(f) \in \mathsf{TAUT}$?

$$w_n^k(f) := [\mathsf{SAT}_n(x,y) \to \mathsf{SAT}_n(x, C(x))] \vee [\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))]$$

variables: x, y, C

$\Uparrow$

encodes n^k-size circuits

$$w_n^k(f) \in \mathsf{TAUT}$$
$$\Downarrow$$
$$\mathsf{SAT}_n \in \mathsf{Circuit}[n^{k/10}] \quad \Rightarrow \quad \mathsf{EF} + w^k(f) \vdash \text{“}\mathsf{SAT}_n \in \mathsf{Circuit}[n^k]\text{”}$$

Self-provability of P=NP

$\mathsf{SAT}_n(x,y) \equiv$ "formula x satisfied by assignment y"

Witnessing P $\neq$ NP

$$\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{10k}] \overset{?}{\Rightarrow} \exists \text{ p-time } f \text{ s.t. } \forall C \in \mathsf{Circuit}[n^k]$$
$$\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))$$

$\exists$ p-time f s.t. $w_n^k(f) \in \mathsf{TAUT}$?

$$w_n^k(f) := [\mathsf{SAT}_n(x,y) \rightarrow \mathsf{SAT}_n(x, C(x))] \vee [\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))]$$

variables: x, y, C

$\Uparrow$

encodes n^k-size circuits

$$w_n^k(f) \in \mathsf{TAUT}$$
$$\Downarrow$$
$$\mathsf{SAT}_n \in \mathsf{Circuit}[n^{k/10}] \quad \Rightarrow \quad \mathsf{EF} + w^k(f) \vdash \text{“}\mathsf{SAT}_n \in \mathsf{Circuit}[n^k]\text{”}$$
$$\Rightarrow \quad \mathsf{EF} + w^k(f) \text{ is p-bounded}$$

Self-provability of P=NP

$\mathsf{SAT}_n(x, y) \equiv$ "formula x satisfied by assignment y"

Witnessing P $\neq$ NP

$$\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{10k}] \overset{?}{\Rightarrow} \exists \text{ p-time } f \text{ s.t. } \forall C \in \mathsf{Circuit}[n^k]$$
$$\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))$$

$\exists$ p-time f s.t. $w_n^k(f) \in \mathsf{TAUT}$?

$$w_n^k(f) := [\mathsf{SAT}_n(x, y) \rightarrow \mathsf{SAT}_n(x, C(x))] \vee [\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))]$$

variables: x, y, C

$\Uparrow$

encodes n^k-size circuits

$$w_n^k(f) \in \mathsf{TAUT}$$

$$\Downarrow$$

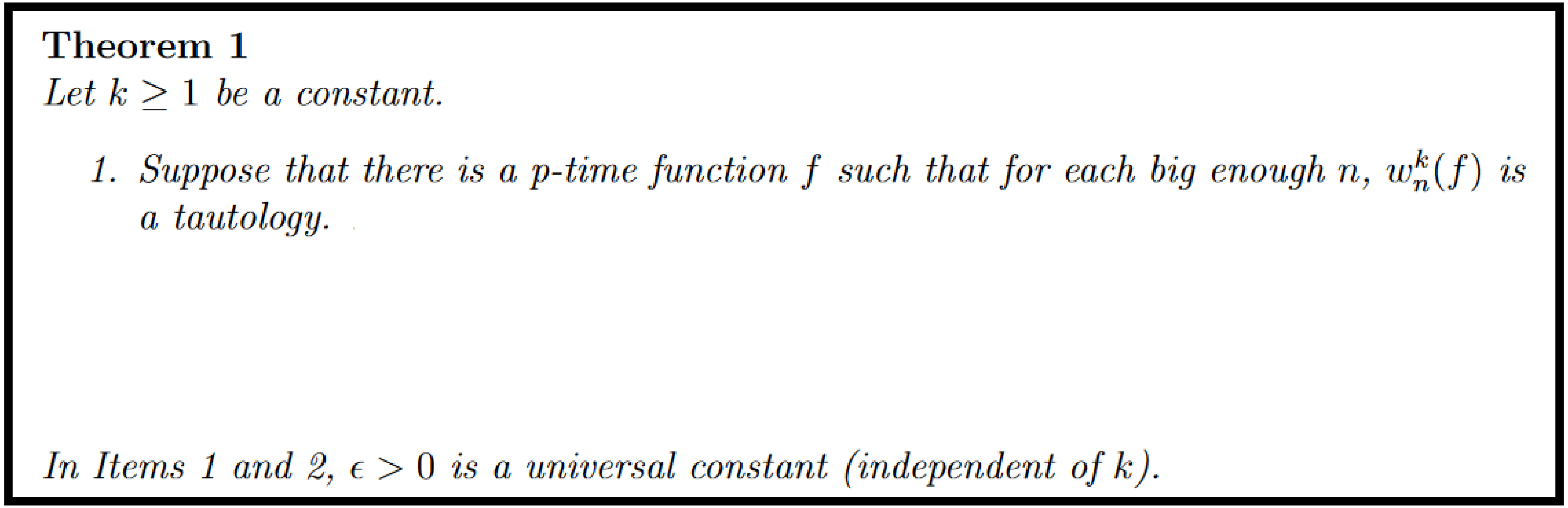
$$\mathsf{SAT}_n \in \mathsf{Circuit}[n^{k/10}] \Rightarrow \mathsf{EF} + w^k(f) \vdash \text{“}\mathsf{SAT}_n \in \mathsf{Circuit}[n^k]\text{”}$$

$$\Rightarrow \mathsf{EF} + w^k(f) \text{ is p-bounded}$$

$(\phi \in \mathsf{TAUT} \Rightarrow \mathsf{EF} \vdash \neg \mathsf{SAT}(\neg\phi, C(\neg\phi)) \Rightarrow \mathsf{EF} + w^k(f) \vdash \neg \mathsf{SAT}(\neg\phi, y) \Rightarrow \mathsf{EF} + w^k(f) \vdash \phi)$

Circuit complexity ⇐ proof complexity & witnessing of P≠NP

Circuit complexity ⇐ proof complexity & witnessing of P≠NP

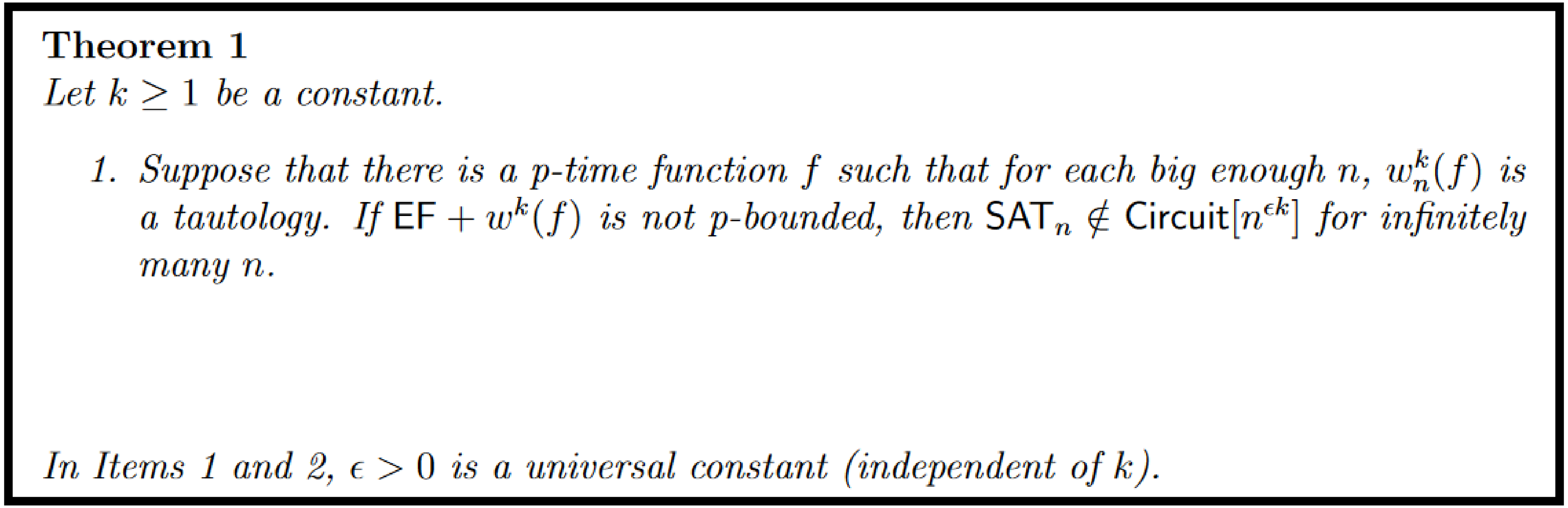


Theorem 1
Let $k \geq 1$ be a constant.

1. *Suppose that there is a p-time function f such that for each big enough n, $w_n^k(f)$ is a tautology.*

In Items 1 and 2, $\epsilon > 0$ is a universal constant (independent of k).

Circuit complexity ⇐ proof complexity & witnessing of P≠NP



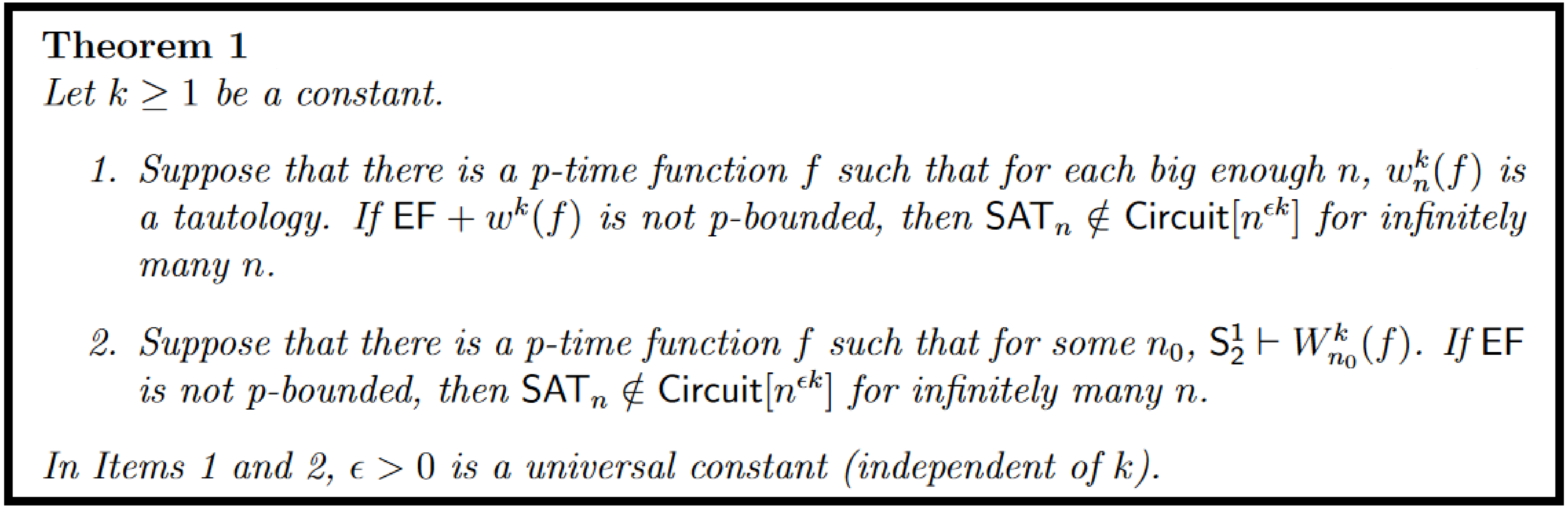
Theorem 1

Let $k \geq 1$ be a constant.

1. *Suppose that there is a p-time function f such that for each big enough n, $w_n^k(f)$ is a tautology. If $\mathsf{EF} + w^k(f)$ is not p-bounded, then $\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{\epsilon k}]$ for infinitely many n.*

In Items 1 and 2, $\epsilon > 0$ is a universal constant (independent of k).

Circuit complexity ⇐ proof complexity & witnessing of P≠NP



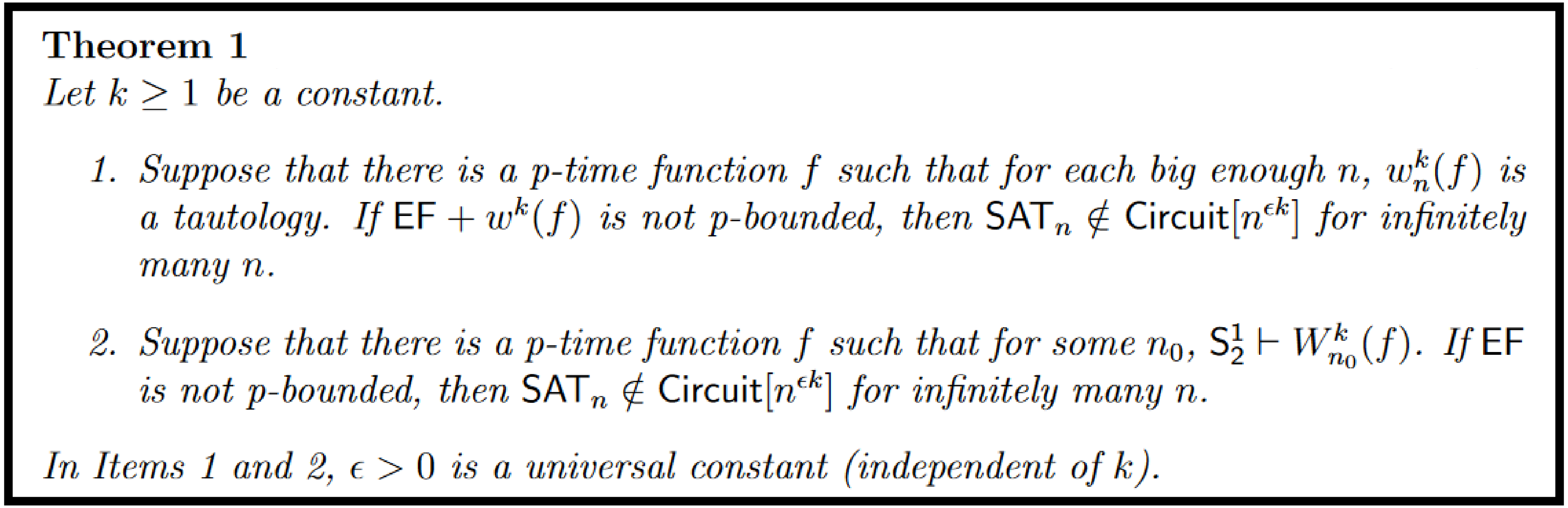
Theorem 1
Let $k \geq 1$ be a constant.

1. *Suppose that there is a p-time function f such that for each big enough n, $w_n^k(f)$ is a tautology. If $\mathsf{EF} + w^k(f)$ is not p-bounded, then $\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{\epsilon k}]$ for infinitely many n.*

2. *Suppose that there is a p-time function f such that for some n_0, $\mathsf{S}^1_2 \vdash W^k_{n_0}(f)$. If EF is not p-bounded, then $\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{\epsilon k}]$ for infinitely many n.*

In Items 1 and 2, $\epsilon > 0$ is a universal constant (independent of k).

Circuit complexity ⇐ proof complexity & witnessing of P≠NP



Theorem 1
Let $k \geq 1$ be a constant.

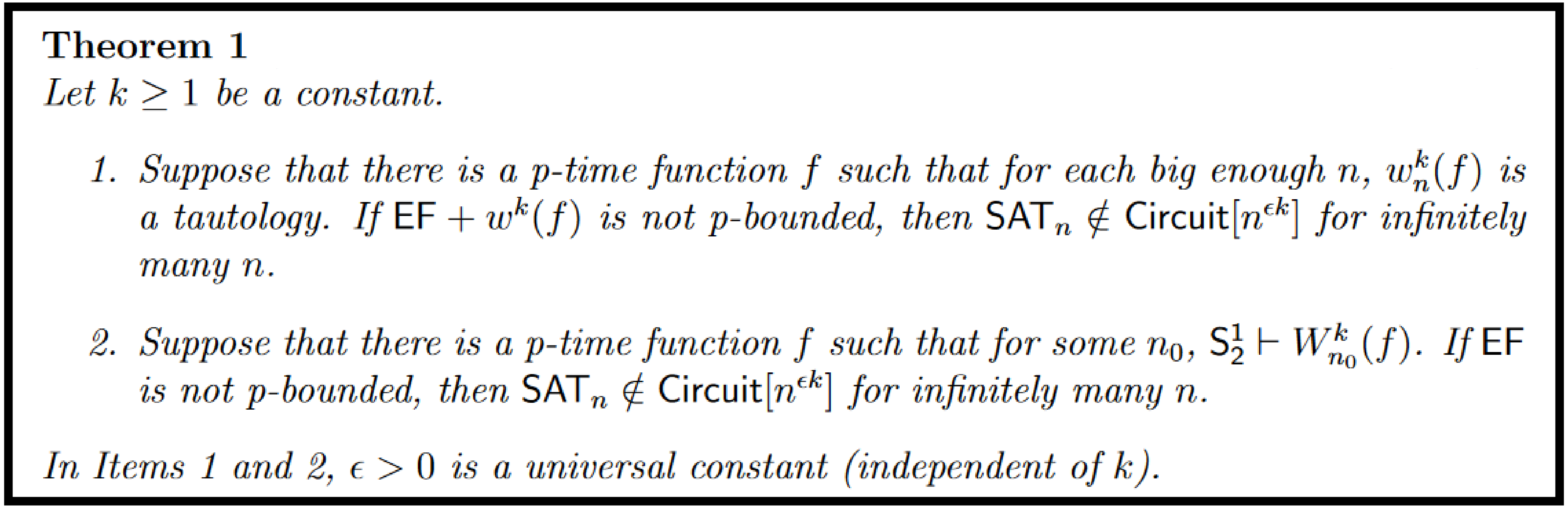
1. *Suppose that there is a p-time function f such that for each big enough n, $w_n^k(f)$ is a tautology. If $\mathsf{EF} + w^k(f)$ is not p-bounded, then $\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{\epsilon k}]$ for infinitely many n.*

2. *Suppose that there is a p-time function f such that for some n_0, $\mathsf{S}_2^1 \vdash W_{n_0}^k(f)$. If EF is not p-bounded, then $\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{\epsilon k}]$ for infinitely many n.*

In Items 1 and 2, $\epsilon > 0$ is a universal constant (independent of k).

- Generalizes to stronger systems

Circuit complexity ⇐ proof complexity & witnessing of P≠NP



Theorem 1

Let $k \geq 1$ be a constant.

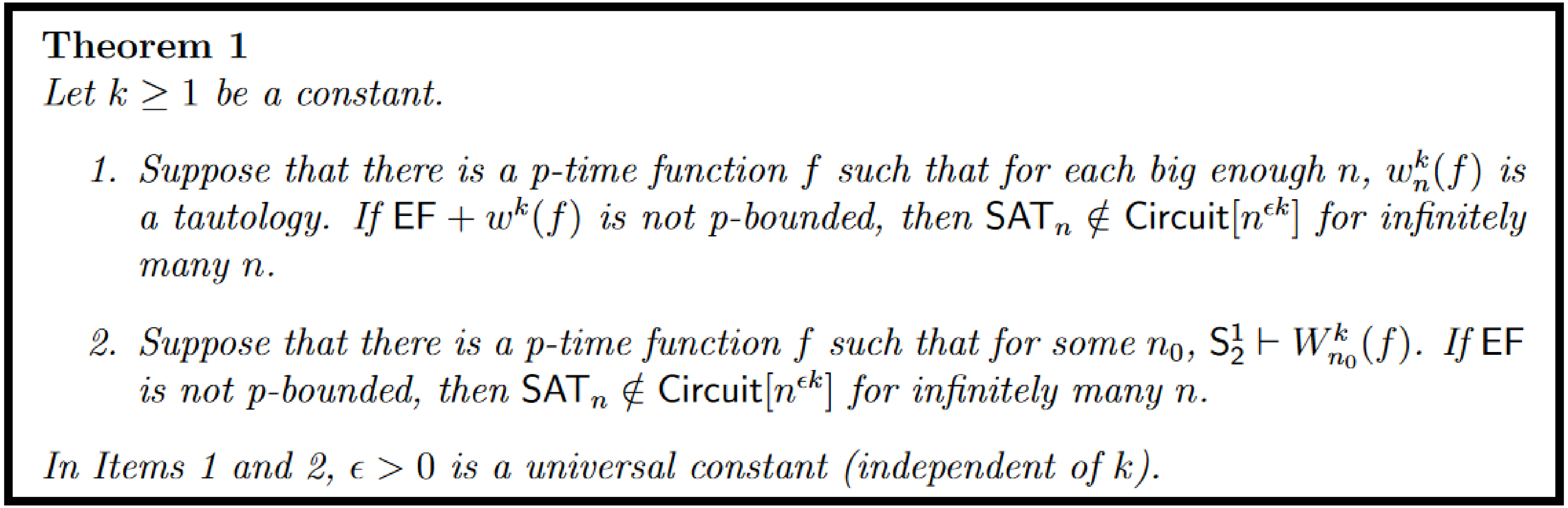
1. *Suppose that there is a p-time function f such that for each big enough n, $w_n^k(f)$ is a tautology. If $\mathsf{EF} + w^k(f)$ is not p-bounded, then $\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{\epsilon k}]$ for infinitely many n.*

2. *Suppose that there is a p-time function f such that for some n_0, $\mathsf{S}^1_2 \vdash W^k_{n_0}(f)$. If EF is not p-bounded, then $\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{\epsilon k}]$ for infinitely many n.*

In Items 1 and 2, $\epsilon > 0$ is a universal constant (independent of k).

Open problem: $w_n^k(f) \in \mathsf{TAUT}$?

Circuit complexity ⇐ proof complexity & witnessing of P≠NP



Theorem 1

Let $k \geq 1$ be a constant.

1. *Suppose that there is a p-time function f such that for each big enough n, $w^k_n(f)$ is a tautology. If $\mathsf{EF} + w^k(f)$ is not p-bounded, then $\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{\epsilon k}]$ for infinitely many n.*

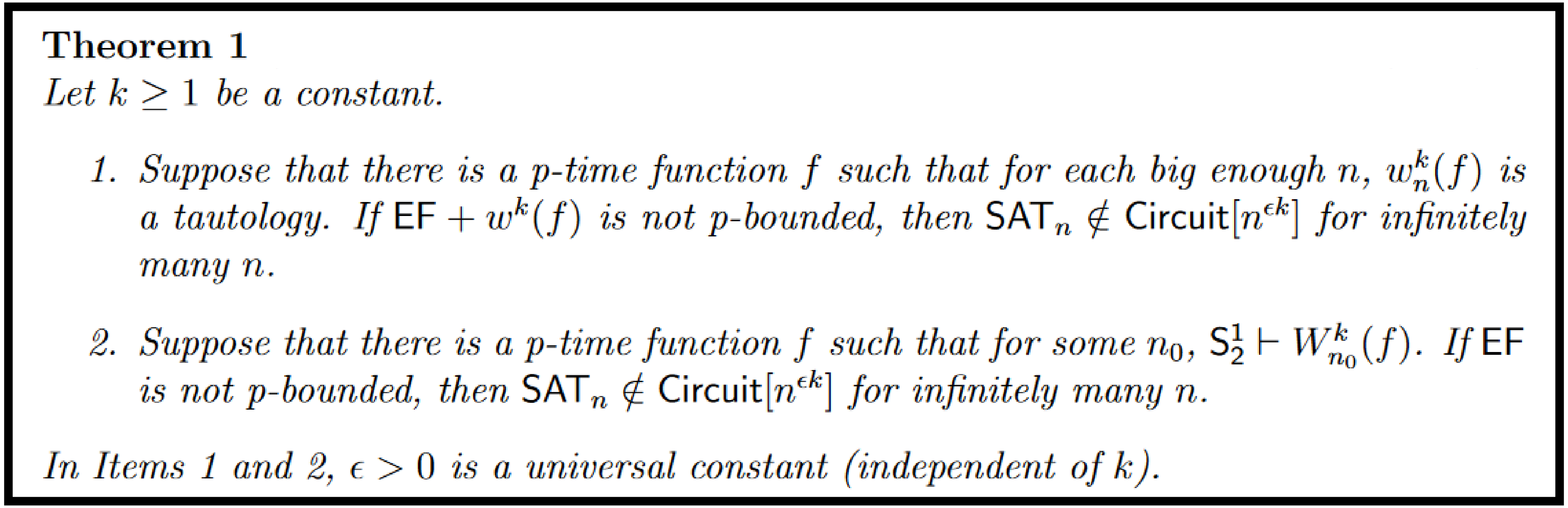
2. *Suppose that there is a p-time function f such that for some n_0, $\mathsf{S}^1_2 \vdash W^k_{n_0}(f)$. If EF is not p-bounded, then $\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{\epsilon k}]$ for infinitely many n.*

In Items 1 and 2, $\epsilon > 0$ is a universal constant (independent of k).

Open problem: $w^k_n(f) \in \mathsf{TAUT}$?

For each p-time f some circuit looks like it solves SAT?

Circuit complexity ⇐ proof complexity & witnessing of P≠NP



Theorem 1

Let $k \geq 1$ be a constant.

1. *Suppose that there is a p-time function f such that for each big enough n, $w^k_n(f)$ is a tautology. If $\mathsf{EF} + w^k(f)$ is not p-bounded, then $\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{\epsilon k}]$ for infinitely many n.*
2. *Suppose that there is a p-time function f such that for some n_0, $\mathsf{S}^1_2 \vdash W^k_{n_0}(f)$. If EF is not p-bounded, then $\mathsf{SAT}_n \notin \mathsf{Circuit}[n^{\epsilon k}]$ for infinitely many n.*

In Items 1 and 2, $\epsilon > 0$ is a universal constant (independent of k).

Open problem: $w^k_n(f) \in \mathsf{TAUT}$?

$$\forall k \exists f, w^k_n(f) \in \mathsf{TAUT} \quad \Rightarrow \quad \mathsf{NEXP} \not\subseteq \mathsf{P/poly}$$

Nonuniform witnessing

$$\alpha_n^s := \big(\mathsf{SAT}_n(x,y) \to \mathsf{SAT}_n(x,B(x))\big) \vee \Big(\bigvee_{z\in A} C(z) \neq \mathsf{SAT}_n(z)\Big)$$

Nonuniform witnessing

fixed p-size circuit

$$\alpha_n^s := \big(\mathsf{SAT}_n(x,y) \rightarrow \mathsf{SAT}_n(x,B(x))\big) \vee \big(\bigvee_{z\in A} C(z) \neq \mathsf{SAT}_n(z)\big)$$

fixed p-size set

Nonuniform witnessing

fixed p-size circuit

$$\boxed{\alpha_n^s := \big(\mathsf{SAT}_n(x,y) \to \mathsf{SAT}_n(x, B(x))\big) \vee \Big(\bigvee_{z \in A} C(z) \neq \mathsf{SAT}_n(z)\Big)}$$

fixed p-size set

$\exists\ poly(s)\text{-size } A \qquad \mathsf{SAT}_n \notin \mathsf{Circuit}[s^3] \quad \Rightarrow \quad \forall s\text{-size } C, \bigvee_{x \in A} C(x) \neq \mathsf{SAT}_n(x)$

anti-checkers

Nonuniform witnessing

fixed p-size circuit

$$\alpha_n^s := \big(\mathsf{SAT}_n(x,y) \rightarrow \mathsf{SAT}_n(x, B(x))\big) \vee \Big(\bigvee_{z \in A} C(z) \neq \mathsf{SAT}_n(z)\Big)$$

fixed p-size set

$\exists\ s^3$-size B' $\quad \mathsf{SAT}_n \in \mathsf{Circuit}[s^3] \Leftrightarrow \forall x \in \{0,1\}^n, B'(x) = \mathsf{SAT}_n(x)$

$\exists\ poly(s)$-size A $\quad \mathsf{SAT}_n \notin \mathsf{Circuit}[s^3] \quad \Rightarrow \quad \forall s\text{-size } C, \bigvee_{x \in A} C(x) \neq \mathsf{SAT}_n(x)$

anti-checkers

Nonuniform witnessing

fixed p-size circuit

$$\alpha_n^s := (\mathsf{SAT}_n(x,y) \rightarrow \mathsf{SAT}_n(x,B(x))) \vee \Big(\bigvee_{z\in A} C(z) \neq \mathsf{SAT}_n(z)\Big)$$

fixed p-size set

$\exists\ s^3$-size B' $\qquad \mathsf{SAT}_n \in \mathsf{Circuit}[s^3] \Leftrightarrow \forall x \in \{0,1\}^n, B'(x) = \mathsf{SAT}_n(x)$

$\exists\ poly(s)$-size A $\qquad \mathsf{SAT}_n \notin \mathsf{Circuit}[s^3] \quad \Rightarrow \quad \forall s\text{-size } C, \bigvee_{x\in A} C(x) \neq \mathsf{SAT}_n(x)$ $\qquad$ anti-checkers

Theorem 2 (Circuit complexity from nonuniform proof complexity)**.**
Let $k \geq 3$ be a constant. If there are tautologies without p-size EF*-derivations from substitutional instances of tautologies $\alpha_n^{n^k}$, then* $\mathsf{SAT}_n \notin \mathsf{Circuit}[n^k]$ *for infinitely many n.*

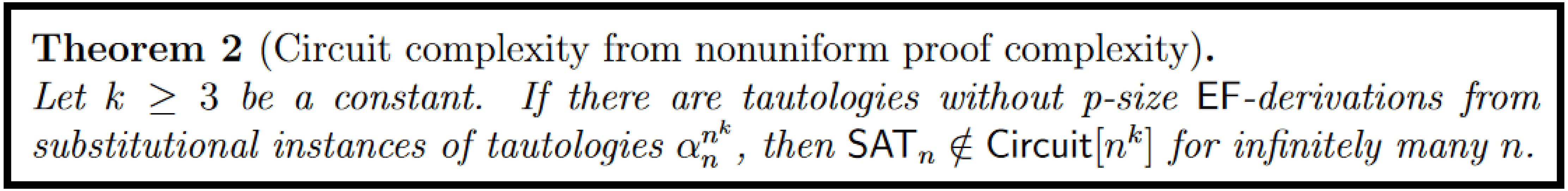
Nonuniform witnessing

fixed p-size circuit

$$\alpha_n^s := \left(\mathsf{SAT}_n(x,y) \to \mathsf{SAT}_n(x, B(x))\right) \vee \Big(\bigvee_{z \in A} C(z) \neq \mathsf{SAT}_n(z) \Big)$$

fixed p-size set

Open problem: Feasible MinMax?



Theorem 2 (Circuit complexity from nonuniform proof complexity)**.** *Let $k \geq 3$ be a constant. If there are tautologies without p-size* EF*-derivations from substitutional instances of tautologies $\alpha_n^{n^k}$, then $\mathsf{SAT}_n \notin \mathsf{Circuit}[n^k]$ for infinitely many n.*

Collapsing Impagliazzo’s worlds

OWF ⇐ P≠NP

Proof complexity collapse from "OWF $\Leftarrow$ P$\neq$NP" & hardness of E

Theorem

$S^1_2 \vdash$ **E** hard on average for subexponential-size circuits

&

$S^1_2 \vdash$ OWF $\Leftarrow$ P$\neq$NP

$\Longrightarrow$

EF not p-bounded $\Rightarrow$ P$\neq$NP

Proof complexity collapse from “OWF $\Leftarrow$ P$\neq$NP” & hardness of E

Theorem

$S^1_2 \vdash$ **E** hard on average for subexponential-size circuits

&

$S^1_2 \vdash$ OWF $\Leftarrow$ P$\neq$NP

$$\Longrightarrow$$

EF not p-bounded $\Rightarrow$ P$\neq$NP

- No need for the **provability** of “E is hard” if EF replaced by EF+“**E** is hard”

Proof complexity collapse from “OWF $\Leftarrow$ P$\neq$NP” & hardness of E

Theorem

$S^1_2 \vdash$ **E** hard on average for subexponential-size circuits

&

$S^1_2 \vdash$ OWF $\Leftarrow$ P$\neq$NP

$$\Longrightarrow$$

EF not p-bounded $\Rightarrow$ P$\neq$NP

- No need for the **provability** of “E is hard” if EF replaced by EF+“**E** is hard”
- Generalizes to stronger systems, e.g. **ZFC**

Proof complexity collapse from “OWF ⇐ P≠NP” & hardness of E

Theorem

$S^1_2 \vdash$ **E** hard on average for subexponential-size circuits

&

$S^1_2 \vdash$ OWF ⇐ P≠NP

$$\Longrightarrow$$

EF not p-bounded ⇒ P≠NP

- No need for the **provability** of “E is hard” if EF replaced by EF+“**E** is hard”
- Generalizes to stronger systems, e.g. **ZFC**
- Requires **p-time reductions** witnessing that OWF ⇐ P≠NP

Proof

$$h \text{ is one-way} \Rightarrow \text{“}h(x) = h(\overset{\text{random}}{\overset{\Downarrow}{a}})\text{”} \text{ is a hard } \mathsf{SAT}\text{-instance}$$

E hard on average for subexponential-size circuits

$$\Longrightarrow$$

$$\exists \text{ p-time } f \text{ s.t. } \forall C \in \mathsf{Circuit}[n^k]$$

$$\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))$$

Proof

$\mathsf{S}^1_2 \vdash$

$$h \text{ is one-way} \Rightarrow \text{“}h(x) = h(\overset{\substack{\text{random}\\ \Downarrow}}{a})\text{”} \text{ is a hard } \mathsf{SAT}\text{-instance}$$

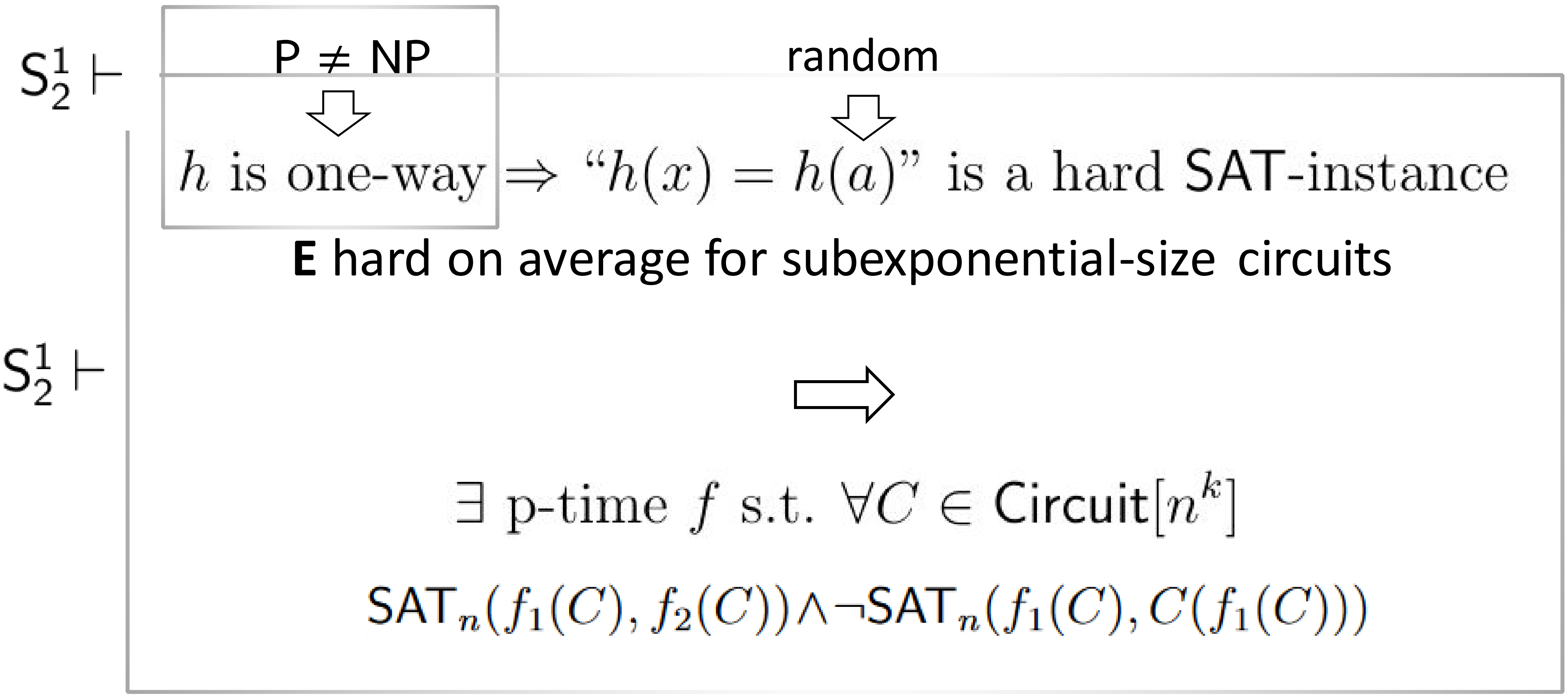
E hard on average for subexponential-size circuits

$$\Longrightarrow$$

$$\exists \text{ p-time } f \text{ s.t. } \forall C \in \mathsf{Circuit}[n^k]$$

$$\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))$$

Proof



$\mathsf{S}^1_2 \vdash$

P ≠ NP

random

h is one-way $\Rightarrow$ "$h(x) = h(a)$" is a hard SAT-instance

E hard on average for subexponential-size circuits

$\mathsf{S}^1_2 \vdash$

$\Longrightarrow$

$\exists$ p-time f s.t. $\forall C \in \mathsf{Circuit}[n^k]$

$\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))$

Proof

$\mathsf{S}^1_2 \vdash$ P ≠ NP random

⇓ ⇓

h is one-way $\Rightarrow$ "$h(x) = h(a)$" is a hard SAT-instance

E hard on average for subexponential-size circuits

$\mathsf{S}^1_2 \vdash$

$\Longrightarrow$

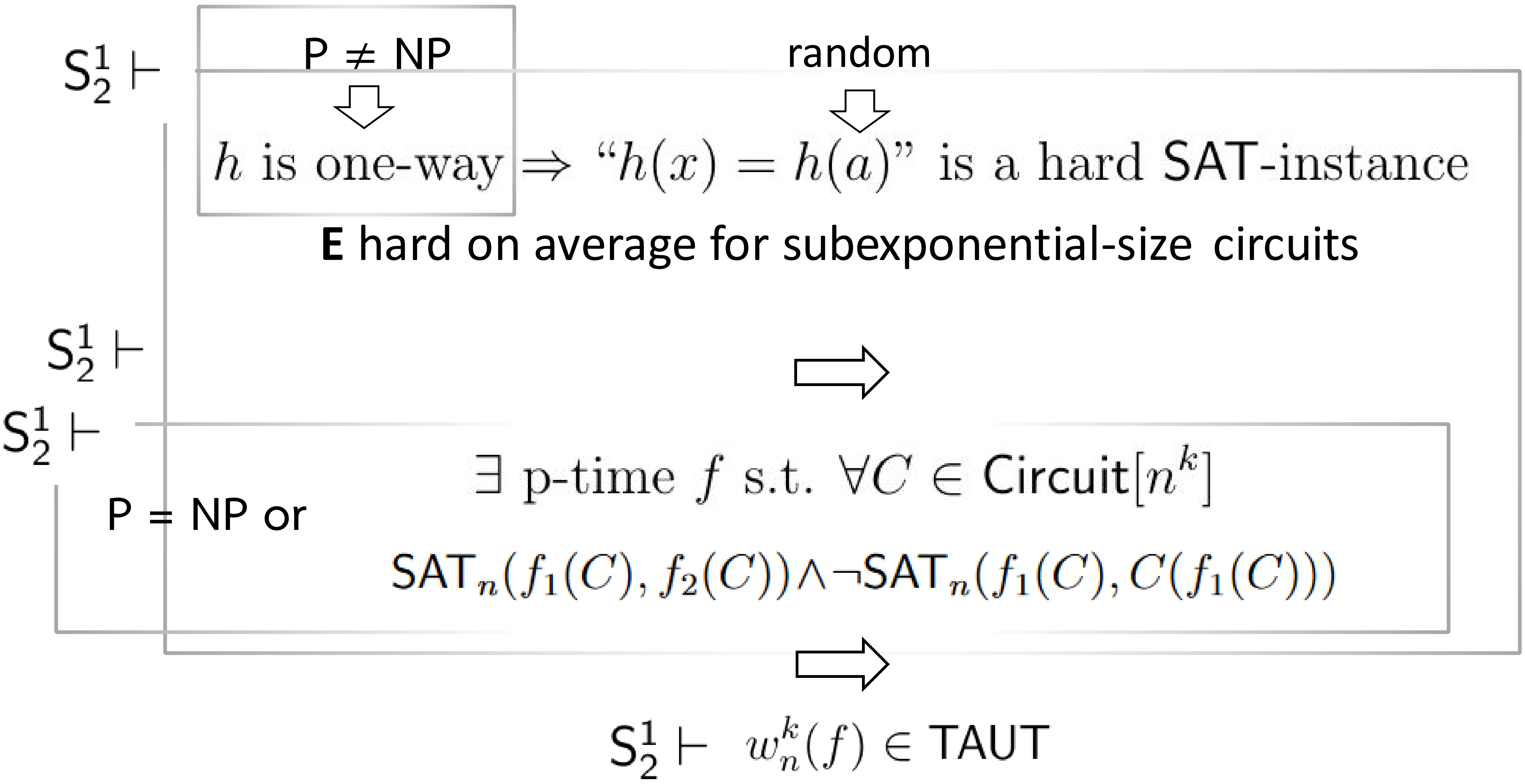
$\mathsf{S}^1_2 \vdash$

P = NP or

$\exists$ p-time f s.t. $\forall C \in \mathsf{Circuit}[n^k]$

$\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))$

Proof



$\mathsf{S}^1_2 \vdash$

P ≠ NP

random

h is one-way $\Rightarrow$ "$h(x) = h(a)$" is a hard SAT-instance

E hard on average for subexponential-size circuits

$\mathsf{S}^1_2 \vdash$

$\Longrightarrow$

$\mathsf{S}^1_2 \vdash$

P = NP or

$$\exists \text{ p-time } f \text{ s.t. } \forall C \in \mathsf{Circuit}[n^k]$$

$$\mathsf{SAT}_n(f_1(C), f_2(C)) \wedge \neg \mathsf{SAT}_n(f_1(C), C(f_1(C)))$$

$\Longrightarrow$

$\mathsf{S}^1_2 \vdash \ w^k_n(f) \in \mathsf{TAUT}$

Learning or Crypto

Theorem

$S^1_2 \vdash$ **E** hard on average for subexponential-size circuits

&

$S^1_2 \vdash$ OWF $\Leftarrow$ P$\neq$NP

$$\Longrightarrow$$

EF not p-bounded $\Rightarrow$ P$\neq$NP

- Can replace "OWF $\Leftarrow$ P$\neq$NP" by "**Learning or Crypto**"
  if EF lower bounds replaced by EF lower bounds for tautologies
  expressing circuit lower bounds

Learning or Crypto

Theorem

$S^1_2 \vdash$ **E** hard on average for subexponential-size circuits

&

$S^1_2 \vdash$ **OWF or Learning P/poly**

$$\Longrightarrow$$

EF $\nvdash$ circuit lower bound $\Rightarrow$ P$\neq$NP

- Can replace “OWF $\Leftarrow$ P$\neq$NP” by “**Learning or Crypto**”
  if EF lower bounds replaced by EF lower bounds for tautologies expressing circuit lower bounds

Automatability or OWF

Theorem

$S^1_2 \vdash$ **E** hard on average for subexponential-size circuits

&

$S^1_2 \vdash$ **OWF or EF automatable**

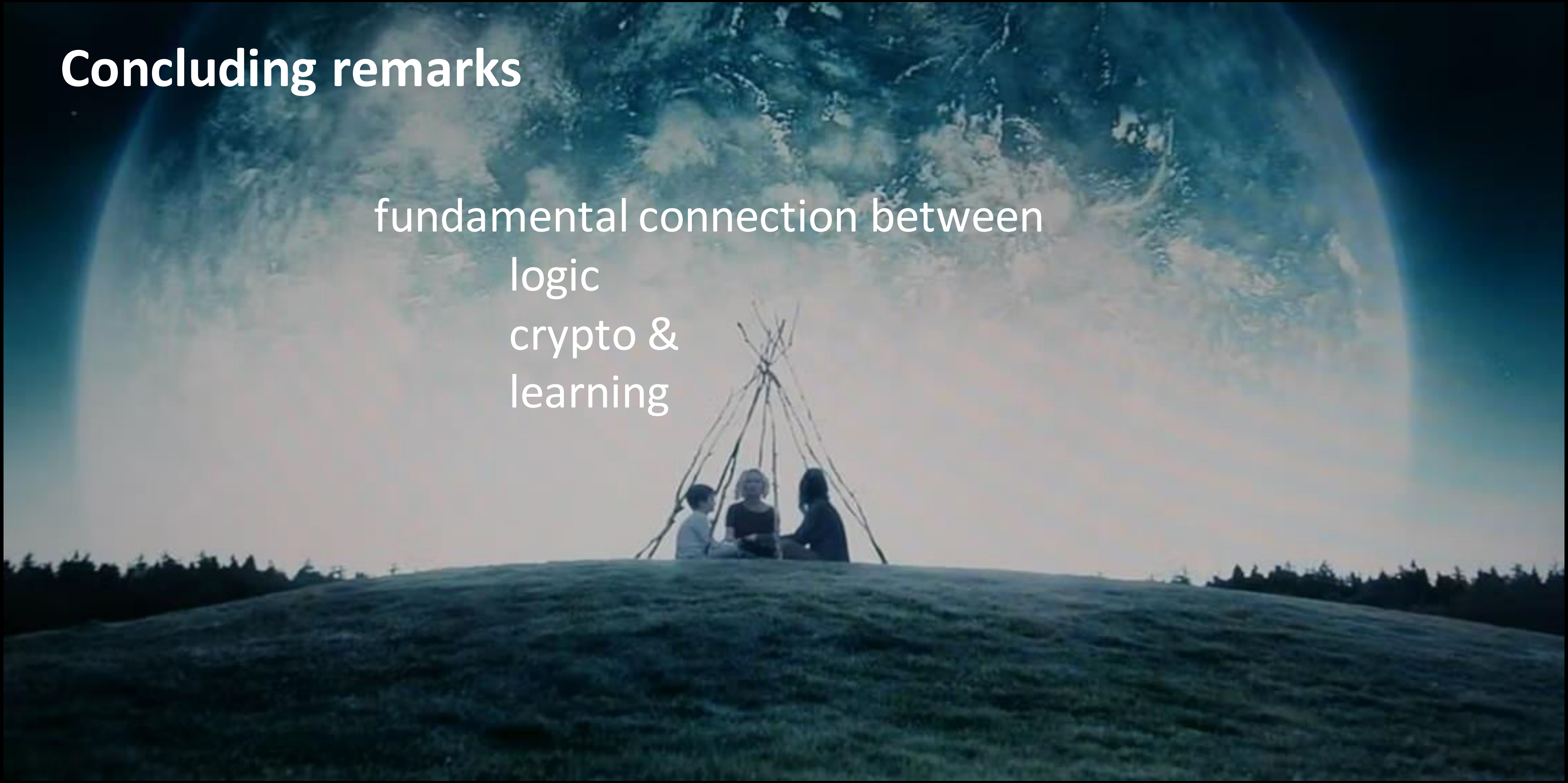
⇨

EF $\nvdash$ circuit lower bound $\Rightarrow$ P$\neq$NP

- Can replace “OWF $\Leftarrow$ P$\neq$NP” by “**Automatability or OWF**”
  if EF lower bounds replaced by EF lower bounds for tautologies expressing circuit lower bounds

Concluding remarks

Concluding remarks

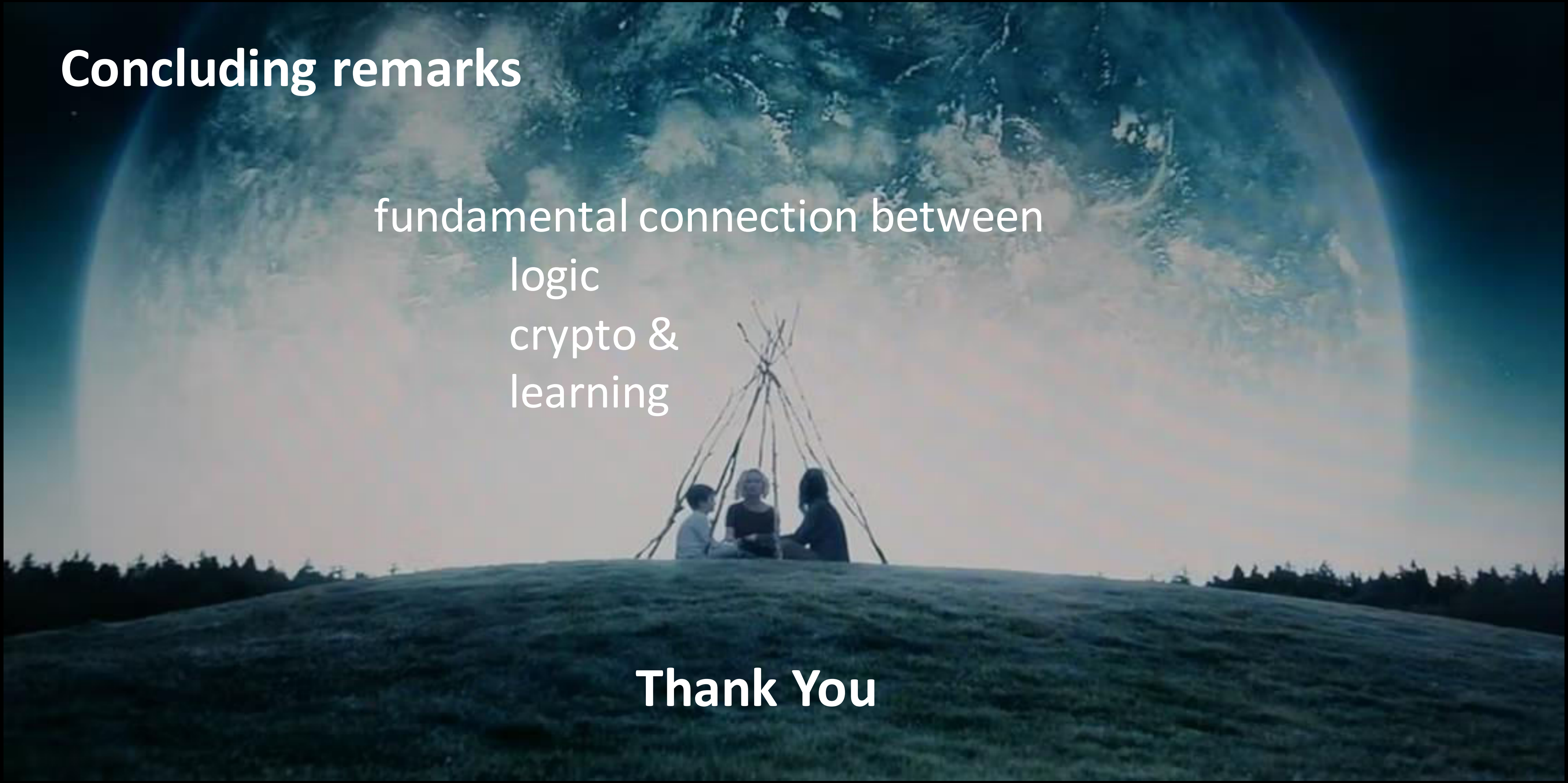


fundamental connection between

logic

crypto &

learning



Concluding remarks

fundamental connection between

logic
crypto &
learning

Thank You