Batch Proofs are Statistically Hiding

Prashant Nalini Vasudevan

Based on work with: Nir Bitansky, Chethan Kamath, Omer Paneth, Ron Rothblum

When Can You Batch Proofs?

Prashant Nalini Vasudevan

Based on work with:

Nir Bitansky   Chethan Kamath

Omer Paneth   Ron Rothblum

Batch Proofs for NP language L

$(x_1, \ldots, x_t)$

P $\qquad\qquad$ V

$(w_1, \ldots, w_t)$

Proof that

$\forall i \in [t] : x_i \in L$

$t \gg |w_i|$

Efficiency: P, V poly-time

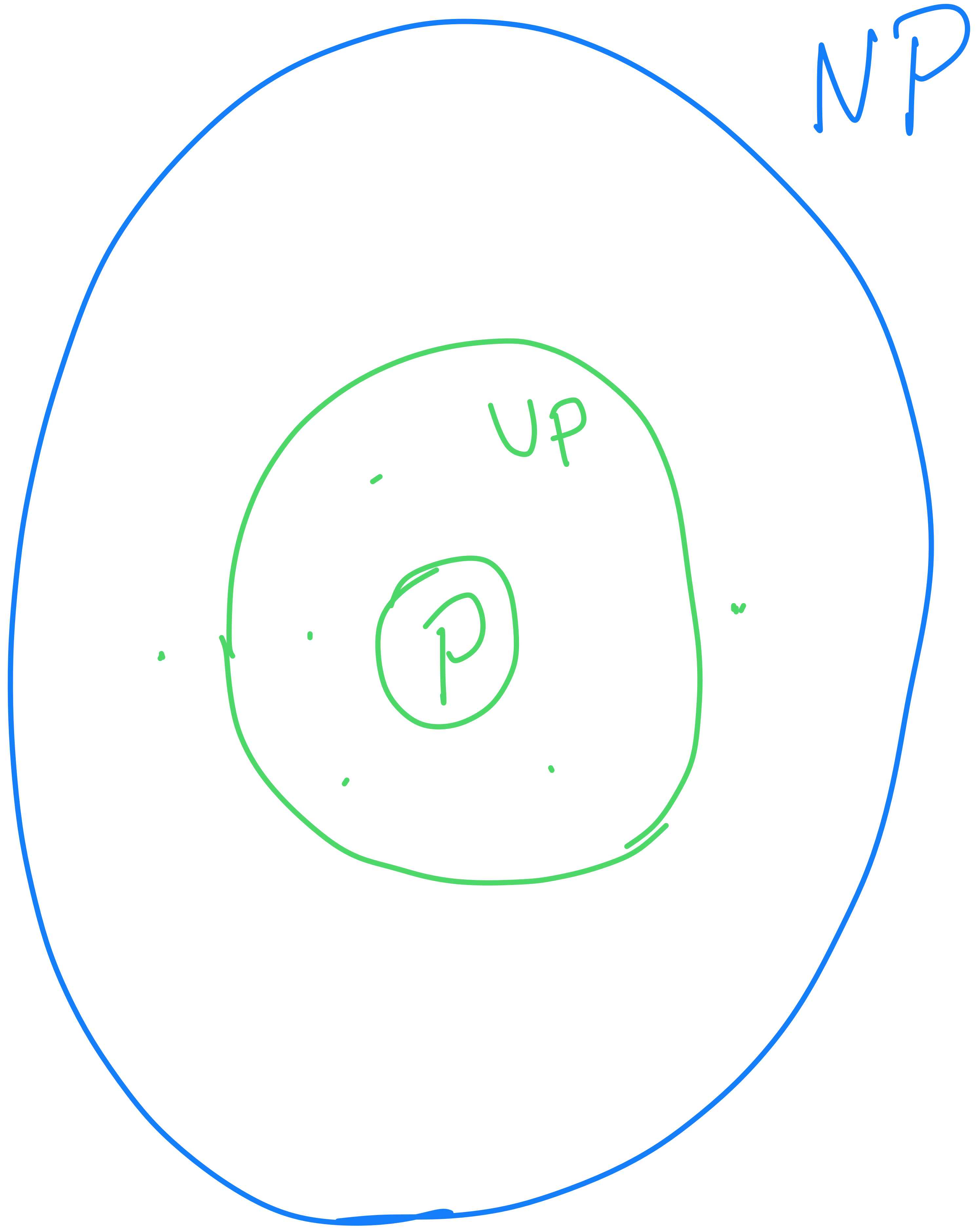
Succinctness:

Total Communication $< t^{1-\epsilon}$ bits

Soundness: Statistical

Which languages in NP have Batch Proofs?

- [RRRRR...] all $L \in UP$
- Some structured languages



How about SAT?

What We Show

Batch Proof for L $\Longrightarrow$ SWI* Proof for L

Witness Indistinguishability [FLS]

$x \in L$, witnesses w_0, w_1

$P(w_0) \rightleftarrows V^*$

$\downarrow$

look same to V^*

$\uparrow$

$P(w_1) \rightleftarrows V^*$

Trivial to get if P is inefficient

Statistical WI:

$\forall$ PPT V^*, $x \in L$, valid witnesses w_0, w_1:

$$\mathrm{View}_{V^*}(w_0) \approx_{\varepsilon} \mathrm{View}_{V^*}(w_1)$$

WI error

Honest-Verifier SWI:

Above holds only for honest verifier V

What We Show

Batch Proof for L $\Rightarrow$ HVSWI Proof for L $\xRightarrow[\text{[GSV]}]{\text{if public-coin}}$ SWI Proof for L

non-uniform prover

$1/\text{poly}$-SWI error

non-uniform prover

$1/\text{poly}$-SWI error

What We Show

L does not have SWI* Proof $\Rightarrow$ L does not have Batch Proof

Which languages in NP have SWI Proofs?

- UP, vacuously
- $SZK \cap NP$
- some combinations thereof

$\boxed{\text{How about SAT?}}$

Interactive Batch Arguments

$(x_1, \ldots, x_t)$

P $\qquad\qquad$ V

$(w_1, \ldots, w_t)$

Proof that

$\forall i \in [t] : x_i \in L$

Efficiency: P, V poly-time

Succinctness:

Total Communication $< t^{1-\epsilon}$ bits

Soundness: Computational

What assumptions are sufficient to get Batch Arguments for NP?

[Killian] Collision-Resistant Hash Functions

[BKP, KNY] Multicollision-Resistant Hash Functions

What assumptions are **necessary** for Batch Arguments for NP?

What We Show

Batch Arguments for NP $\Rightarrow$ HVSWI Args. for NP $\xRightarrow{+\text{OWF}}$ SZK Args. for NP

[GMW]

[FLS]

r rounds

(r+1) rounds

non-uniform prover

1/poly WI error

O(r) rounds

non-uniform prover

1/poly ZK error

What We Show

O(1)-round Batch Arguments for NP + OWF ⇒ O(1)-round SZK Arguments for NP

only known from O(1)-round Statistically Hiding Commitments

If OWF ⇒ O(1)-round Batch Arguments for NP

Then OWF ⇒ O(1)-round SZK Arguments for NP

Non-Interactive Batch Arguments

$(x_1, \ldots, x_t)$

$\boxed{CRS}$

$$P \longrightarrow V$$

$(w_1, \ldots, w_t)$

Proof that

$\forall i \in [t] : x_i \in L$

Efficiency: P, V poly-time

Succinctness:

Total Communication $< t^{1-\epsilon}$ bits

Soundness: Computational

Adaptive

What assumptions are sufficient for non-interactive Batch Args. for NP?

- LWE [CJJ]
- Bilinear maps [WW]
- DDH [BKM, HJKS, CGJJZ]

$\boxed{\text{What assumptions are } \underline{\text{necessary}} \text{ for non-interactive Batch Args. for NP?}}$

What We Show

Non-interactive Batch Argument for NP $\Rightarrow$ Non-Interactive SWI Argument for NP $\Rightarrow$ Non-Interactive SZK Argument for NP

$\Downarrow$

Lossy PKE

Non-Interactive SWI Argument for NP:

non-uniform prover

1/poly WI error

Non-Interactive SZK Argument for NP:

non-uniform prover

negl. ZK error

Batch Proofs to WI

Simplest case: L has Batch "NP" proof

$$\underline{P} \qquad (x_1, \dots, x_t) \qquad \underline{V}$$

$(w_1, \dots, w_t)$

$$\Pi \leftarrow f\big((x_1, w_1), \dots, (x_t, w_t)\big) \xrightarrow{\Pi} \text{Accepts } \Pi \text{ iff.}$$

$$\forall i \in [t] : x_i \in L$$

- poly-time
- deterministic
- $\underline{|\Pi| = t^{1-\epsilon}}$

$\boxed{\underline{\text{Want}}: \text{SWI proof for } L}$

<u>Approach:</u> π cannot remember all of the w_i's

Given (x, w), hide it among the inputs to f

$\underline{P(w)}$ $\qquad\qquad$ x $\qquad\qquad$ $\underline{V}$

Pick $(x_i, w_i) \in R_L$, $j \leftarrow [t]$

$\pi \leftarrow f((x_1, w_1), \ldots, (x, w), \ldots, (x_t, w_t))$

j^{th} location

View$_V$

$\boxed{\{x_i\}, j, \pi}$ $\longrightarrow$ Run Batch Verifier with instance $(x_1, \ldots, x, \ldots x_t)$ proof π

WI?

$$\Pi \leftarrow f\left((x_1, w_1), \ldots, (x, w), \ldots, (x_t, w_t)\right)$$

- Fix $x \in L$, witnesses w^0, w^1
- Can we pick (x_i, w_i)'s so that Π looks same for $w = w^0$, and $w = w^1$?

Yes! Set $x_i = x$, $w_i \leftarrow \{w^0, w^1\}$

Compression Lemma [Drucker, Dell]:

$\forall$ function $g : \{0,1\}^t \to \{0,1\}^{\rho \cdot t}$ $(\rho < 1)$

$$(j, g(b_1, \ldots, b_{j-1}, 0, b_{j+1}, \ldots, b_t)) \approx_{\sqrt{\rho}} (j, g(b_1, \ldots, 1, \ldots, b_t))$$

where $j \leftarrow [t]$

$b_i \leftarrow \{0,1\}$

Fix (x, w^0, w^1)

Set $x_i := x$, $w_i \leftarrow \{w^0, w^1\}$, $j \leftarrow [t]$

j th location

$$\Pi_b = f\left((x_1, w_1), \ldots, \underset{\downarrow}{(x, w^b)}, \ldots, (x_t, w_t)\right)$$

Comp. Lemma with $g(b_1, \ldots, b_t) = f\left((x, w^{b_1}), \ldots, (x, w^{b_t})\right)$

$$\Rightarrow \quad (j, \Pi_0) \approx (j, \Pi_1)$$

Fix distribution D over (x, w_0, w_1)

$$(x, w^0, w^1) \leftarrow D$$

Sample $(x_i, w_i^0, w_i^1) \leftarrow D$, $w_i \leftarrow \{w_i^0, w_i^1\}$, $j \leftarrow [t]$

$$\Pi_b = f\left((x_1, w_1), \ldots, (x, w^b), \ldots, (x_t, w_t)\right)$$

Comp. Lemma with $g(b_1, \ldots, b_t) = f\left((x_1, w_1^{b_1}), \ldots, (x_t, w_t^{b_t})\right)$

$$\Rightarrow \quad (x, \{x_i\}, j, \Pi_0) \approx (x, \{x_i\}, j, \Pi_1)$$

Distributional WI

Have: $\forall$ distribution over (x, w_0, w_1):

$\exists$ distrib. over (x_i, w_i)'s:

proof is WI

Minmax!

Want: $\exists$ distrib. over (x_i, w_i)'s:

$\forall$ tuple (x, w_0, w_1):

proof is WI

Dist. WI $\to$ WI

Two-Player Zero-Sum Game :

P1 picks (x, w^0, w^1)

P2 picks $\{(x_i, w_i^0, w_i^1)\}$

$\text{Payoff} = \|(x, \{x_i\}, j, \Pi_0) - (x, \{x_i\}, j, \Pi_1)\|_1$

Dist. WI

$\forall$ mixed strat. of P1

$\exists$ mixed strat. of P2 :

$E[\text{payoff}] < \text{small}$

$\xLeftrightarrow{\text{Minmax}}$

WI

$\exists$ mixed strat. of P2

$\forall$ pure strat. of P1 :

$E[\text{payoff}] < \text{small}$

<u>Have:</u> $\forall$ distribution over (x, w_0, w_1):

$\exists$ distrib. over (x_i, w_i)'s:

proof is WI

Minmax!

<u>Want:</u> $\exists$ distrib. over (x_i, w_i)'s:

$\forall$ tuple (x, w_0, w_1):

proof is WI

Sparse minmax

[Lipton-Young]

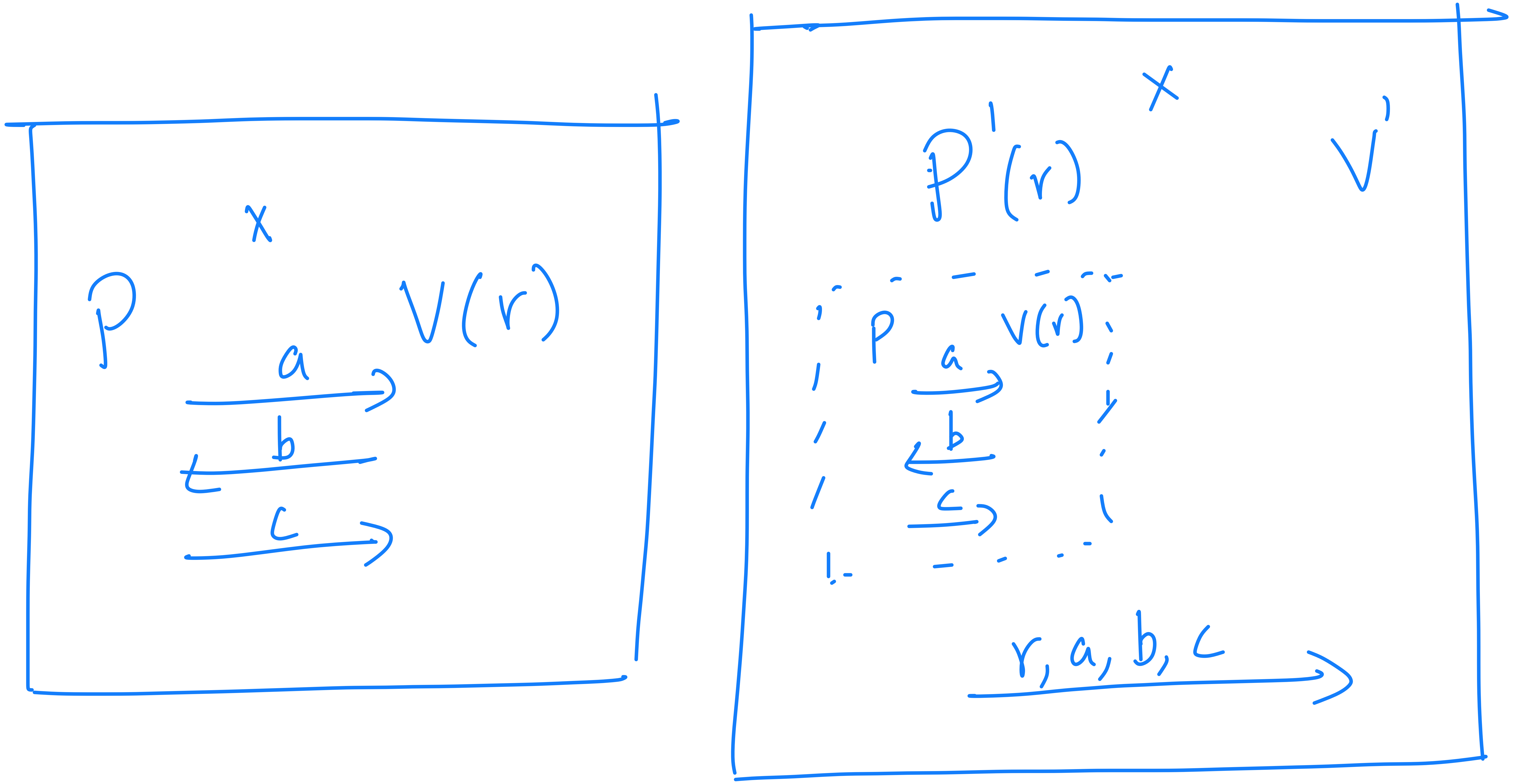
gives efficient

non-uniform

sampleability

Handling More Rounds

Identical approach - insert (x,w) at a random location and use batch proof



(P,V) is HVSWI

iff

(P',V') is HVSWI

Questions

1. Is $NP \subseteq SWI$?
   - General study of SWI
2. Remove caveats in our constructions
   - Make prover uniform
   - Get negligible SWI error
3. Show stronger bounds for non-interactive Batch Proofs
   - Can these exist for UP?
   - even with unbounded provers?
4. Batch Proofs for classes other than UP?

Instance Compression [HN, BDFH]

AND-Compression of L : poly-time R s.t.

- $R(x_1, \dots, x_t) = y \in L$ iff $\forall i \in [t] : x_i \in L$
- $|y| \ll t$

[FS, Drucker] L has AND-Comp. $\Rightarrow L \in SZK^*$

Compare : L has Batch Proof $\Rightarrow L \in SWI^*$