Batch Proofs are Statistically Hiding

Prashant Nalin; Vasudevan

Based on work with:

Nir Bitansky  Chethan Kamath
Omer Paneth  Ron Rothblum
When Can You Batch Proofs?

Prashant Nalin Vasudevan

Based on work with:

Nir Bitansky Chethan Kamath
Omer Paneth Ron Rothblum
Batch Proofs for NP language \( L \)

\[
(x_1, \ldots, x_t) \\
(P, V) \\
(w_1, \ldots, w_t)
\]

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 LE U P
- some structured languages

How about SAT?
What We Show

Batch Proof \Rightarrow SWI^* Proof

for L
Witness Indistinguishability [FLS]

Theorem: For all witnesses $w_0, w_1$, $x \in L$, and PPT $V^*$:

1. Statistical WI:
   - $P(w_0) \xrightarrow{\text{look same to}} V^*$
   - $P(w_1) \xrightarrow{\text{look same to}} V^*$
   - $\forall PPT V^*, x \in L, \text{valid witnesses } w_0, w_1:
     \text{View}_{V^*}(w_0) \approx \text{View}_{V^*}(w_1)$
   - WI error

2. Honest-Verifier SWI:
   - Above holds only for honest verifier $V$
What We Show

Batch Proof for $L$ $\Rightarrow$ HVSWI Proof for $L$ $\Rightarrow$ SWI Proof for $L$

non-uniform prover
\(1/\text{poly}\) - SWI error
[GSV]

if public-coin
non-uniform prover
\(1/\text{poly}\) - SWI error
What We Show

$L$ does not have $\text{SWI}^* \implies L$ does not have $\text{Batch Proof}$
Which languages in NP have SWI Proofs?

- UP, vacuously
- SZK \& NP
- Some combinations thereof

How about SAT?
Interactive Batch Arguments

\[(x_1, \ldots, x_t)\]

\[P \quad V\]

\[(w_1, \ldots, w_t)\]

\[\iff\]

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

$r$ rounds

$\Rightarrow$

HVSWI Args. for NP

$(r+1)$ rounds

non-uniform prover

$\forall \text{poly WI error}$

$\Rightarrow$

OWF [GMW]

[FLS]

SZK Args. for NP

$O(r)$ rounds

non-uniform prover

$\forall \text{poly 2K error}$
What We Show

$O(1)$-round Batch Arguments for NP + OWF $\Rightarrow$ $O(1)$-round SZK Arguments for NP

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

If OWF $\Rightarrow$ $O(1)$-round Batch Arguments for NP

Then OWF $\Rightarrow$ $O(1)$-round SZK Arguments for NP
Non-Interactive Batch Arguments

\[(x_1, \ldots, x_t)\]

\[\text{CRS} \]

\[P \rightarrow V\]

\[(w_1, \ldots, w_t)\]

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 \( \text{NP} \)?

- LWE \([\text{CJJ}]\)
- Bilinear maps \([\text{WW}]\)
- DDH \([\text{BKM, HJKS, CGJJZ}]\)

What assumptions are necessary for non-interactive Batch Args. for \( \text{NP} \)?
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-uniform prover

\frac{\text{poly}}{\text{WI error}}

\uparrow

\non-uniform prover

\text{negl. ZK error}
Batch Proofs to WI

Simplest case: $L$ has Batch "NP" proof

$\begin{array}{c}
\frac{P}{(w_1, \ldots, w_t)} \\
\overline{(x_1, \ldots, x_t)} \\
\end{array}$

$\Pi \leftarrow f((x_1, w_1), \ldots, (x_t, w_t))$  $\Pi$  Accepts $\Pi$ iff

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

Want: SWI proof for $L$
Approach: $T_j$ cannot remember all of the $w_i$'s.

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

$P(u) \times \nabla$

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

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

View

$\{x_i, j, T_j\}$

Run Batch Verifier with instance $(x_1, \ldots, x, \ldots x_t)$ proof $T_j$
\[ \text{\underline{WI?}} \]

\[ \text{TI} \leftarrow f ( (x_i, w_i), \ldots, (x, w), \ldots, (x_t, w_t)) \]

- Fix \( x \in L \), witnesses \( w^0, w^1 \)
- Can we pick \((x_i, w_i)\)'s so that \( \text{TI} \) 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]:

A function \( g : \{0, 1\}^t \rightarrow \{0, 1\}^{p \cdot t} \) \((p < 1)\)

\((j, g(b_1, \ldots, b_{j-1}, 0, b_{j+1}, \ldots, b_t)) \sim_{\sqrt{p}} (j, g(b_1, \ldots, 1, \ldots, b_t))\)

where \( j \leftarrow [t] \)

\( b_i \leftarrow \{0, 1\} \)
Fix \((x, w^0, w^1)\)

Set \(x_j = x, w_j \leftarrow \{w^0, w^1\}, j \leftarrow [t]\)

\[\prod_b = f((x_1, w_1), \ldots, (x, w^b), \ldots, (x_t, w_t))\]

Compiled Lemma with \(g(b_1, \ldots, b_t) = f((x, w^{b_1}), \ldots, (x, w^{b_t}))\)

\[\Rightarrow (j, \prod_0) \approx (j, \prod_1)\]
Fix distribution $D$ over $(x, w_0, w_1)$

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

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

$$\Pi_b = \mathcal{f}((x_i, w_i), \ldots, (x_i, w^b_i), \ldots, (x_t, w_t))$$

Comp. Lemma with $g(b_1, \ldots, b_t) = \mathcal{f}((x_i, w^b_i), \ldots, (x_t, w^b_t))$

$$\Rightarrow (x, \{x_i\}, j, \Pi_0) \sim (x, \{x_i\}, j, \Pi_1) \quad \text{Distributional WI}$$
Have: A distribution over \((x, w_0, w_1)\):
   \[ \exists \text{distrib. over } (x_i, w_i)'s: \]
   proof is WI

Want: \[ \exists \text{distrib. over } (x_i, w_i)'s: \]
   A tuple \((x, w_0, w_1)\):
   proof is WI

\[ \text{Min max!} \]
Dist: $WI \rightarrow WI$

Two-Player Zero-Sum Game

$P_1$ picks $(x, w^0, w')$

$P_2$ picks $\{ (x_i, w_i^0, w_i') \}$

Payoff $= \| (x, \{x_i, j, T_i\}) - (x, \{x_i^0, j, T_i^0\}) \|_1$

Dist: $WI$

A mixed strat of $P_1$

$\exists$ mixed strat of $P_2$:

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

WI

A mixed strat of $P_2$

$\exists$ mixed strat of $P_2$:

$E[\text{payoff}] < \text{small}$
Have: A distribution over \((x, w_0, w_1)\):

\[ \exists \text{ distribution over } (x_i, w_i)\]'s:

proof is WI

Want: \( \exists \text{ distribution over } (x_i, w_i)\)'s:

A tuple \((x, w_0, w_1)\):

proof is WI

\[ \text{Min max!} \]

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.

\[ P \xrightarrow{a} V(r) \]

\[ P' \xrightarrow{a} V' \]

\[ (P, V) \text{ is HVSWI} \quad \text{iff} \quad (P', V') \text{ is HVSWI} \]
Questions

1. Is \( NP \leq SWI \)?
   - 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.
- $R(x_1, \ldots, x_t) = y \in L$ if $\forall i \in [t]: x_i \in L$
- $|y| \ll t$

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

Compare : $L$ has Batch $\Rightarrow L \in \text{SWI}^*$

Proof