BATCH PROOFS ARE STATISTICALLY HIDING

CHETHAN KAMATH

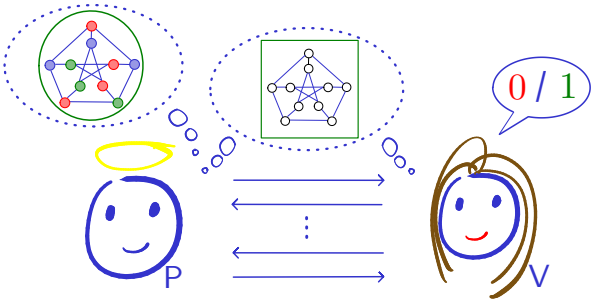



NIR BITANSKY OMER PANETH PRASHANT VASUDEVAN RON ROTHBLUM

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

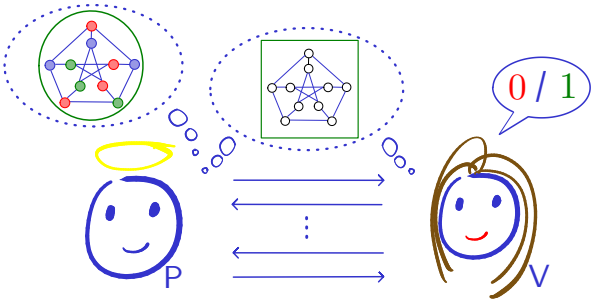
NUS National University of Singapore

TECHNION Israel Institute of Technology



INTERACTIVE PROTOCOLS

COMPLETENESS ◆ ◆◆ SOUNDNESS



INTERACTIVE PROTOCOLS

COMPLETENESS

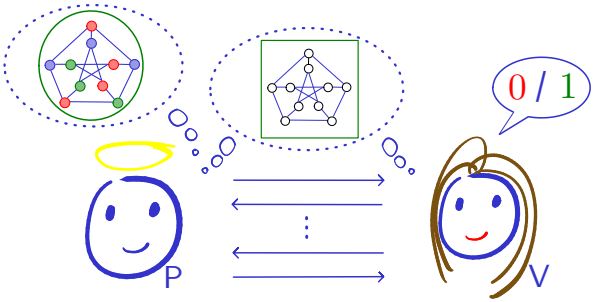
SOUNDNESS

SUCCINCTNESS

BATCHING

HIDING

WITNESS IND.



INTERACTIVE PROTOCOLS

COMPLETENESS ◆ ◆ SOUNDNESS

SUCCINCTNESS ◆ ⟶ ◆ HIDING

BATCHING WITNESS IND.

PLAN

- BACKGROUND
  - DEFINITIONS: BATCH PROOFS STAT. WITNESS INDISTINGUISHABILITY (SWI)
  - WHAT CAN BE BATCHED?

PLAN

- BACKGROUND
  - DEFINITIONS: BATCH PROOFS STAT. WITNESS INDISTINGUISHABILITY (SWI)
  - WHAT CAN BE BATCHED?
- MAIN RESULT
  - BATCH PROOFS $\Rightarrow$ SWI PROOFS
  - TECHNICAL OVERVIEW

PLAN

- BACKGROUND
  - DEFINITIONS: BATCH PROOFS STAT. WITNESS INDISTINGUISHABILITY (SWI)
  - WHAT CAN BE BATCHED?
- MAIN RESULT
  - BATCH PROOFS $\Rightarrow$ SWI PROOFS
  - TECHNICAL OVERVIEW
- MORE RESULTS
  - ONE-WAY FUNCTION + BATCH ARGUMENTS $\Rightarrow$ SZK ARGUMENTS
  - NON-INTERACTIVE (NI) BATCH ARGUMENTS $\Rightarrow$ NI SZK ARGUMENTS

PLAN

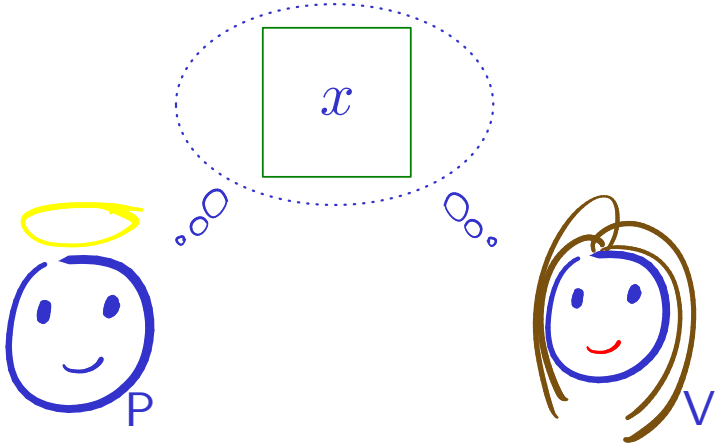
- BACKGROUND
  - DEFINITIONS: BATCH PROOFS STAT. WITNESS INDISTINGUISHABILITY (SWI)
  - WHAT CAN BE BATCHED?
- MAIN RESULT
  - BATCH PROOFS $\Rightarrow$ SWI PROOFS
  - TECHNICAL OVERVIEW
- MORE RESULTS
  - ONE-WAY FUNCTION + BATCH ARGUMENTS $\Rightarrow$ SZK ARGUMENTS
  - NON-INTERACTIVE (NI) BATCH ARGUMENTS $\Rightarrow$ NI SZK ARGUMENTS
- OPEN QUESTIONS

PLAN

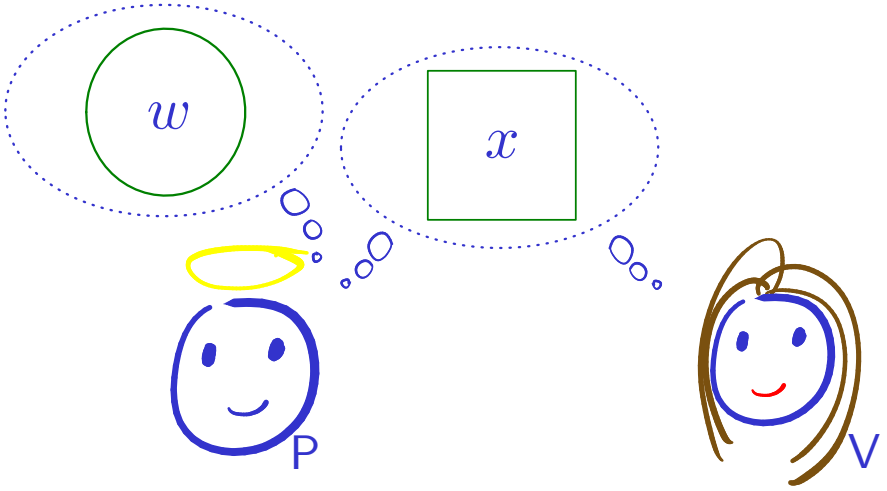
- BACKGROUND
  - DEFINITIONS: BATCH PROOFS STAT. WITNESS INDISTINGUISHABILITY (SWI)
  - WHAT CAN BE BATCHED?
- MAIN RESULT
  - BATCH PROOFS $\Rightarrow$ SWI PROOFS
  - TECHNICAL OVERVIEW
- MORE RESULTS
  - ONE-WAY FUNCTION + BATCH ARGUMENTS $\Rightarrow$ SZK ARGUMENTS
  - NON-INTERACTIVE (NI) BATCH ARGUMENTS $\Rightarrow$ NI SZK ARGUMENTS
- OPEN QUESTIONS

INTERACTIVE PROTOCOL FOR $\mathcal{L}$

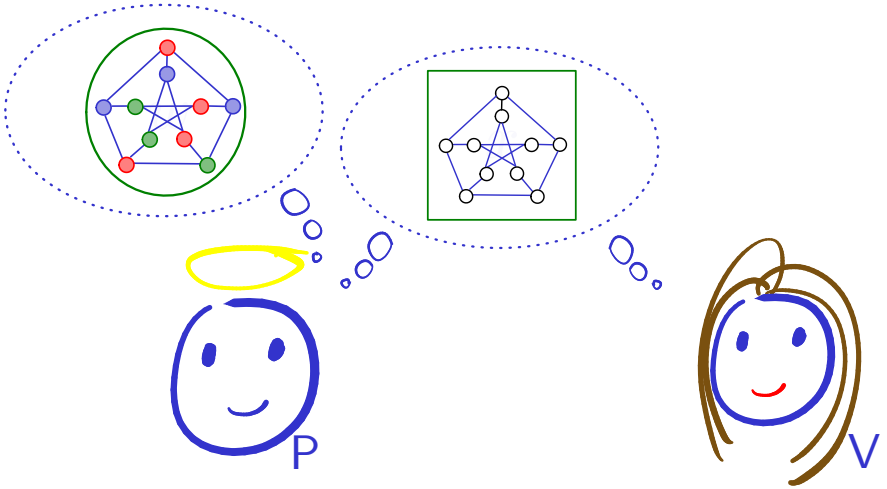
INTERACTIVE PROTOCOL FOR $\mathcal{L}$



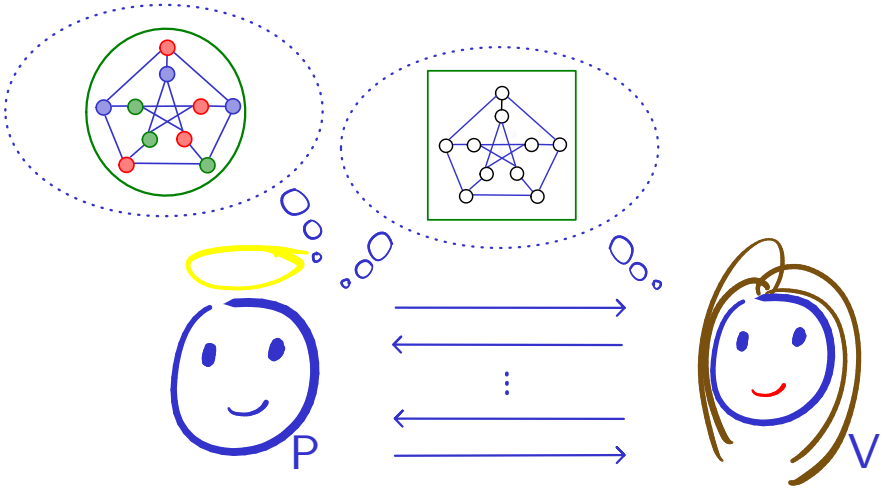
INTERACTIVE PROTOCOL FOR $\mathcal{L}$



INTERACTIVE PROTOCOL FOR $\mathcal{L}$ (E.G.: 3-COLORING)

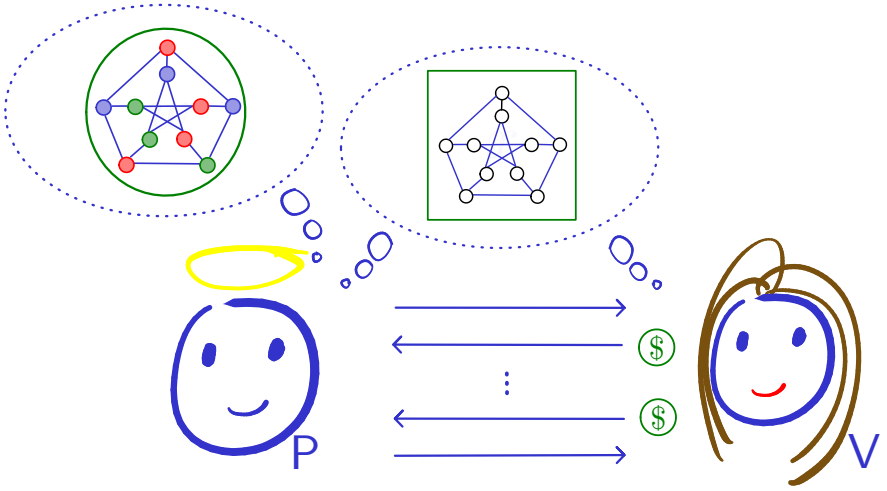


INTERACTIVE PROTOCOL FOR $\mathcal{L}$ (E.G.: 3-COLORING)



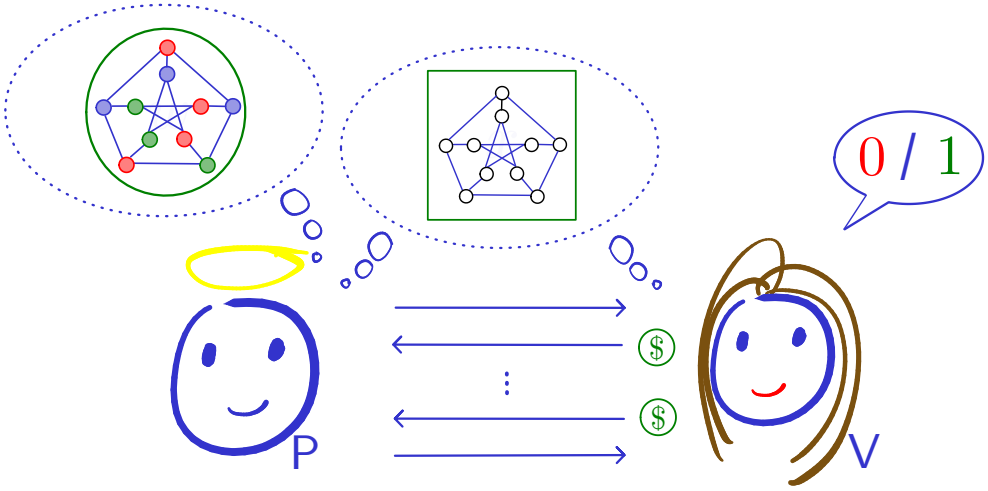
(PUBLIC-COIN)

INTERACTIVE PROTOCOL FOR $\mathcal{L}$ (E.G.: 3-COLORING)



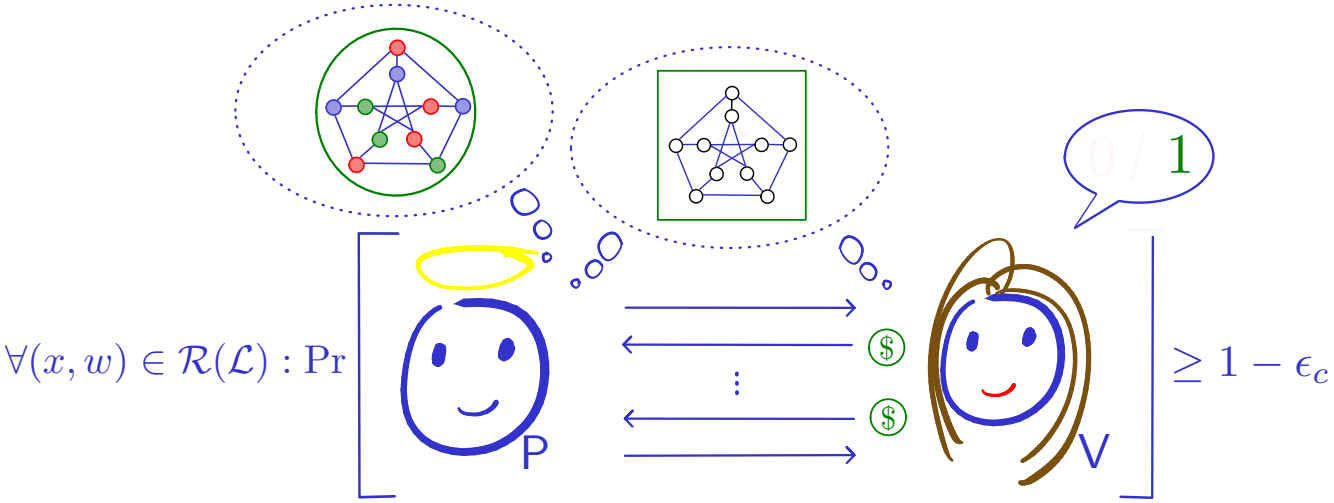
(PUBLIC-COIN)

INTERACTIVE PROTOCOL FOR $\mathcal{L}$ (E.G.: 3-COLORING)



(PUBLIC-COIN)

INTERACTIVE PROTOCOL FOR $\mathcal{L}$ (E.G.: 3-COLORING)



$$\forall (x, w) \in \mathcal{R}(\mathcal{L}) : \Pr[\ \langle P, V \rangle(x) = 1\ ] \geq 1 - \epsilon_c$$

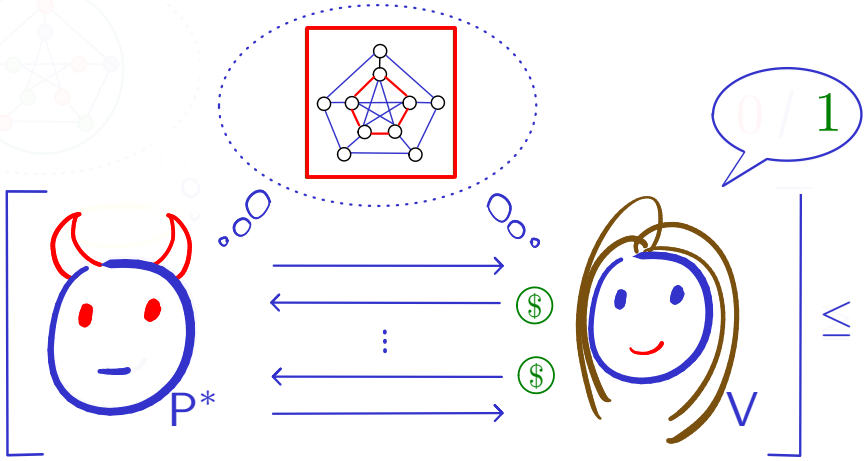
◆ REQUIREMENTS

◆ COMPLETENESS

HONEST P CONVINCES V OF TRUE STATEMENTS

(PUBLIC-COIN)

INTERACTIVE PROTOCOL FOR $\mathcal{L}$ (E.G.: 3-COLORING)



$$\forall x \notin \mathcal{L} : \Pr\left[\text{P}^* \leftrightarrows \text{V}\right] \leq \epsilon_s$$

REQUIREMENTS

COMPLETENESS

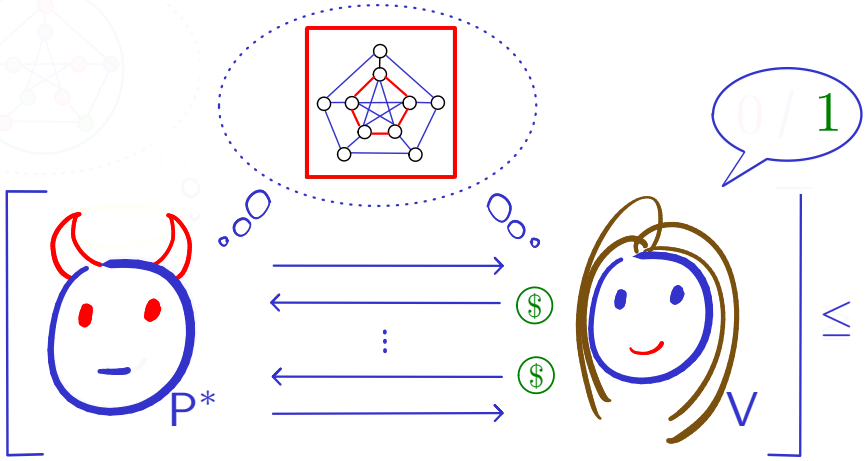
HONEST P CONVINCES V OF TRUE STATEMENTS

SOUNDNESS

MALICIOUS P* CANNOT CONVINCE V OF FALSE STATEMENTS

(PUBLIC-COIN)

INTERACTIVE PROTOCOL FOR $\mathcal{L}$ (E.G.: 3-COLORING)



$$\forall x \notin \mathcal{L} : \Pr[\langle P^*, V \rangle(x) = 1] \leq \epsilon_s$$

REQUIREMENTS

COMPLETENESS

HONEST P CONVINCES V OF TRUE STATEMENTS

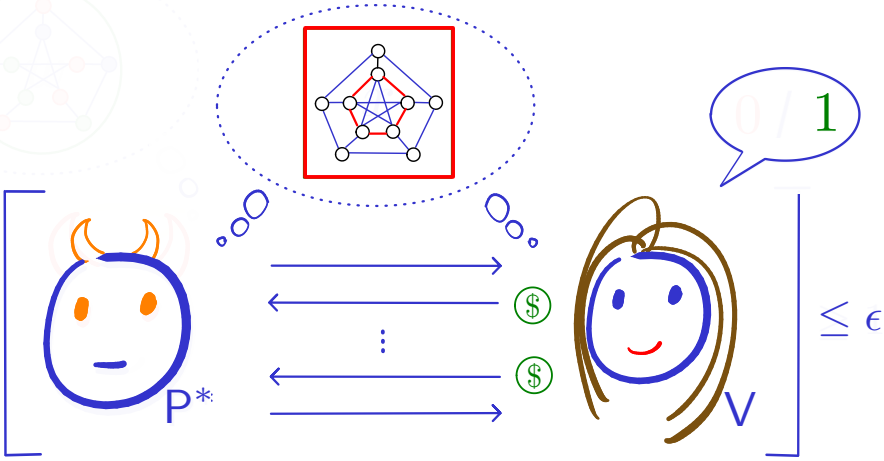
SOUNDNESS

MALICIOUS P* CANNOT CONVINCE V OF FALSE STATEMENTS

UNBOUNDED
STATISTICAL SOUNDNESS = PROOF

(PUBLIC-COIN)

INTERACTIVE PROTOCOL FOR $\mathcal{L}$ (E.G.: 3-COLORING)



$$\forall x \notin \mathcal{L} : \Pr\left[\; P^* \;\$\; \vdots \;\$\; V \;\right] \leq \epsilon_s$$

REQUIREMENTS

COMPLETENESS

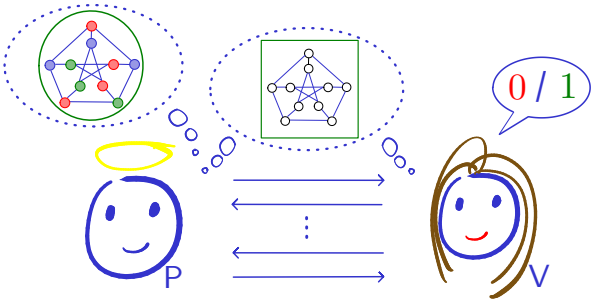
HONEST P CONVINCES V OF TRUE STATEMENTS

SOUNDNESS

MALICIOUS P* CANNOT CONVINCE V OF FALSE STATEMENTS

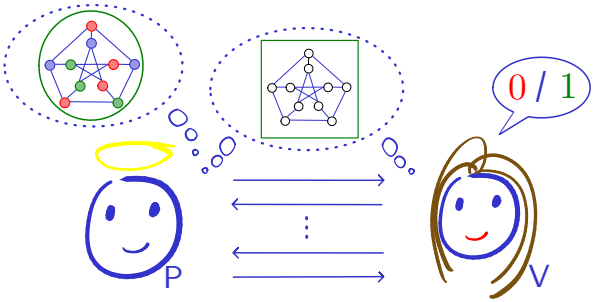
- UNBOUNDED
  STATISTICAL SOUNDNESS = PROOF
- BOUNDED
  COMPUTATIONAL SOUNDNESS=ARGUMENT

...



INTERACTIVE PROTOCOLS

- COMPLETENESS
- SOUNDNESS



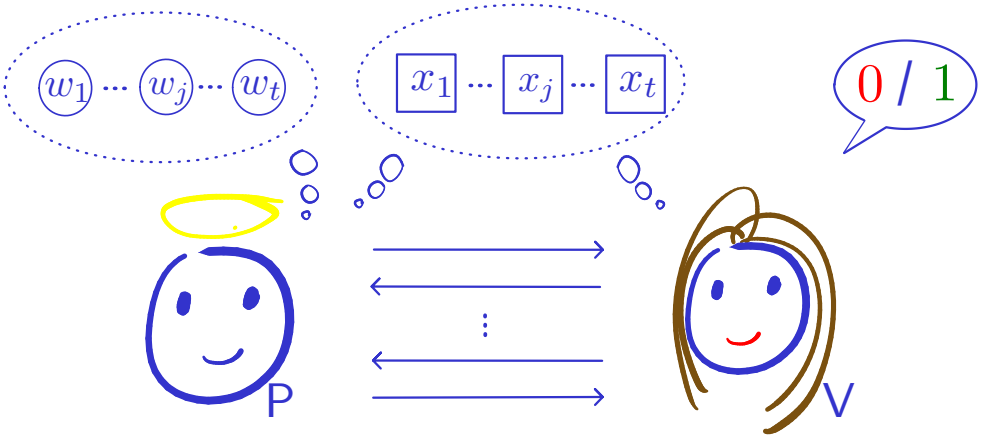
INTERACTIVE PROTOCOLS

- COMPLETENESS
- SOUNDNESS
- SUCCINCTNESS
  "CAN WE REDUCE COMMUNICATION?"
- HIDING
  "CAN WE HIDE THE WITNESS?"

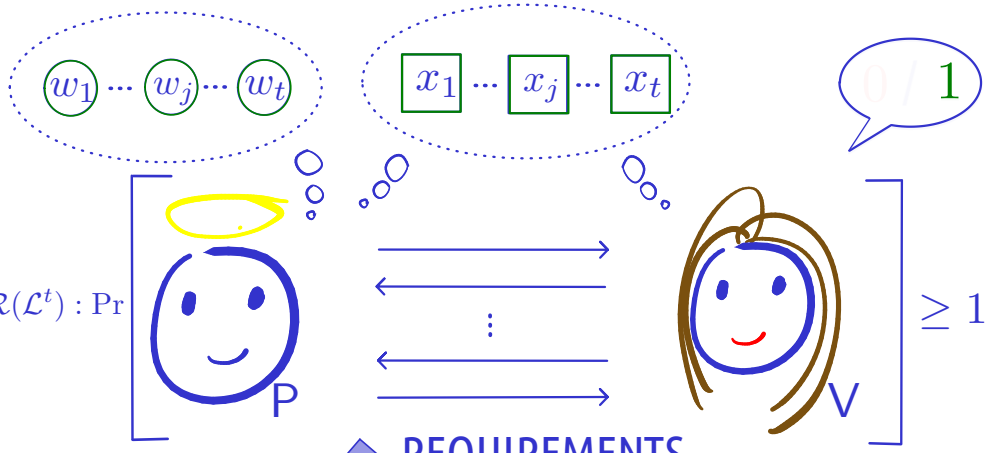
BATCH PROTOCOL FOR $\mathcal{L}^t$

BATCH PROTOCOL FOR $\mathcal{L}^t := \{x_1, \ldots, x_t : x_1 \in \mathcal{L} \wedge \cdots \wedge x_t \in \mathcal{L}\}$

BATCH PROTOCOL FOR $\mathcal{L}^t := \{x_1, \ldots, x_t : x_1 \in \mathcal{L} \wedge \cdots \wedge x_t \in \mathcal{L}\}$



BATCH PROTOCOL FOR $\mathcal{L}^t := \{x_1, \ldots, x_t : x_1 \in \mathcal{L} \wedge \cdots \wedge x_t \in \mathcal{L}\}$



$\forall (x_1, w_1), \cdots, (x_t, w_t) \in \mathcal{R}(\mathcal{L}^t) : \Pr[\ \ ] \geq 1 - \epsilon_c$

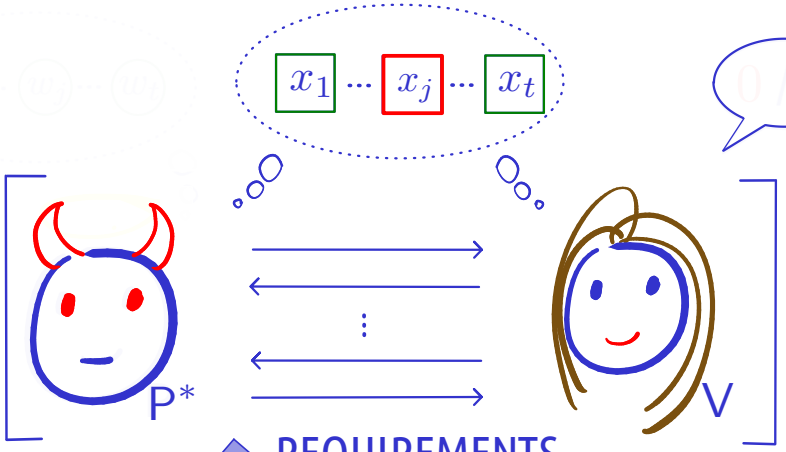
REQUIREMENTS

COMPLETENESS

HONEST P CONVINCES V IF ALL STATEMENTS TRUE

BATCH PROTOCOL FOR $\mathcal{L}^t := \{x_1, \ldots, x_t : x_1 \in \mathcal{L} \wedge \cdots \wedge x_t \in \mathcal{L}\}$

$\forall x_1, \ldots, x_t$ s.t. $\exists x_j \notin \mathcal{L} : \Pr$



$\leq \epsilon_s$

REQUIREMENTS

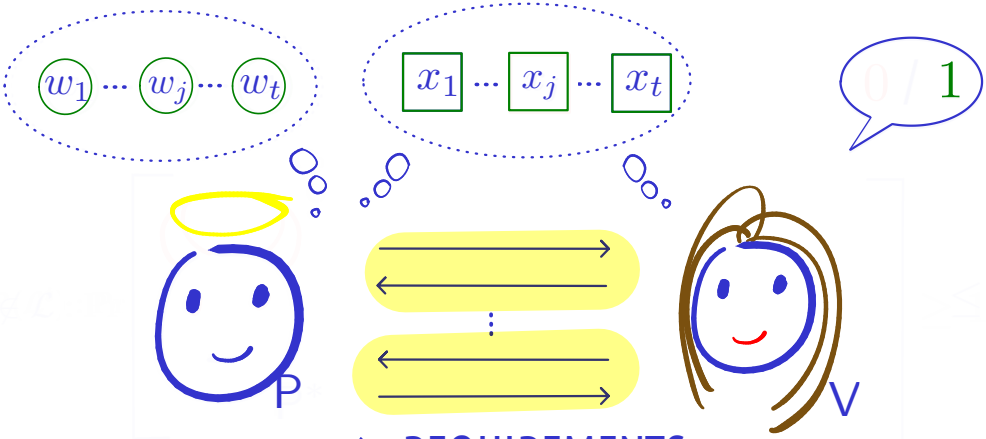
COMPLETENESS

HONEST P CONVINCES V IF ALL STATEMENTS TRUE

SOUNDNESS

MALICIOUS P* CANNOT CONVINCE V IF THERE EXISTS A FALSE STATEMENT

BATCH PROTOCOL FOR $\mathcal{L}^t := \{x_1, \ldots, x_t : x_1 \in \mathcal{L} \wedge \cdots \wedge x_t \in \mathcal{L}\}$



REQUIREMENTS

COMPLETENESS

HONEST P CONVINCES V IF ALL STATEMENTS TRUE

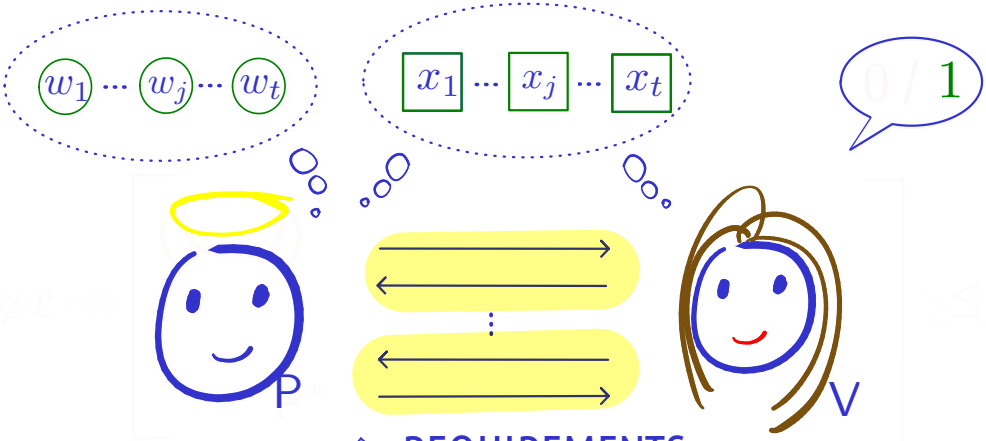
SOUNDNESS

MALICIOUS P* CANNOT CONVINCE V IF THERE EXISTS A FALSE STATEMENT

SUCCINCTNESS

COMPRESSING WITH RATE ρ IF COMMUNICATION $\leq \rho \cdot t$ (E.G: ASSUME $|w| \ll t$ AND $\rho = t^{-1/2}$)

BATCH PROTOCOL FOR $\mathcal{L}^t := \{x_1, \ldots, x_t : x_1 \in \mathcal{L} \wedge \cdots \wedge x_t \in \mathcal{L}\}$



REQUIREMENTS

COMPLETENESS

HONEST P CONVINCES V IF ALL STATEMENTS TRUE

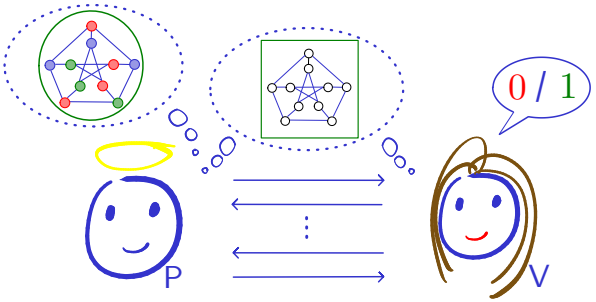
SOUNDNESS

MALICIOUS P* CANNOT CONVINCE V IF THERE EXISTS A FALSE STATEMENT

SUCCINCTNESS

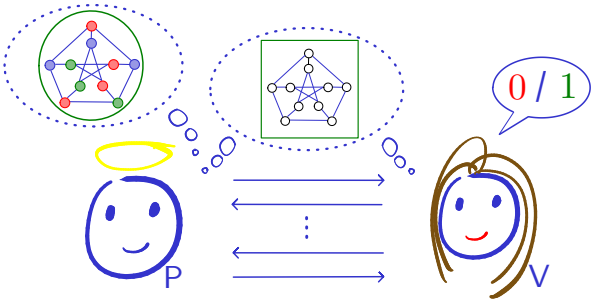
COMPRESSING WITH RATE ρ IF COMMUNICATION $\leq \rho \cdot t$ (E.G: ASSUME $|w| \ll t$ AND $\rho = t^{-1/2}$)

TRIVIAL IF P UNBOUNDED VIA IP=PSPACE



INTERACTIVE PROTOCOLS

- COMPLETENESS
- SOUNDNESS
- SUCCINCTNESS
  - "CAN WE REDUCE COMMUNICATION?"
- HIDING
  - "CAN WE HIDE WITNESS?"



INTERACTIVE PROTOCOLS

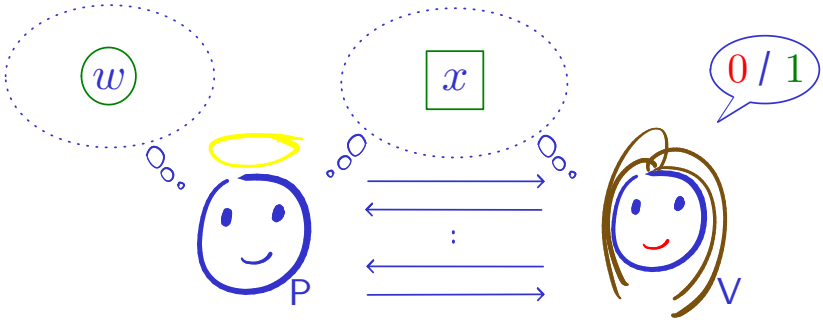
- COMPLETENESS
- SOUNDNESS
- SUCCINCTNESS

"CAN WE REDUCE COMMUNICATION?"

- HIDING

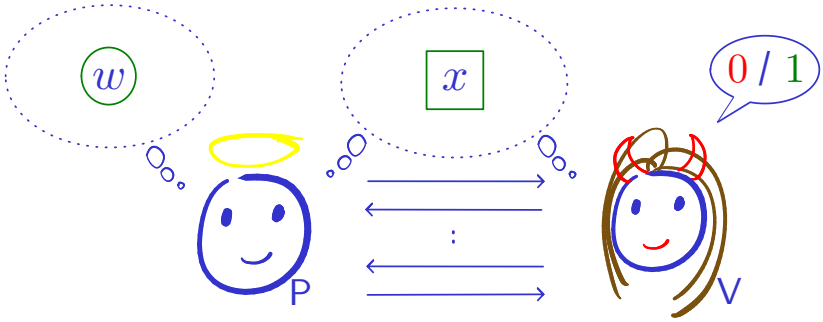
"CAN WE HIDE THE WITNESS?"

WITNESS INDISTINGUISHABILITY [FLS90]



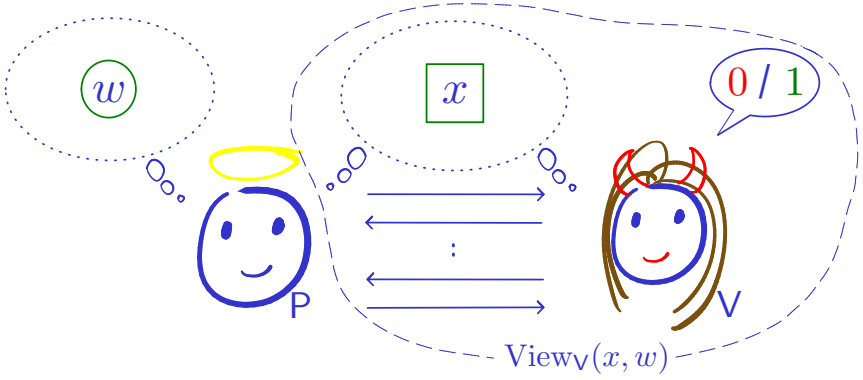
(HONEST-VERIFIER)

WITNESS INDISTINGUISHABILITY [FLS90]



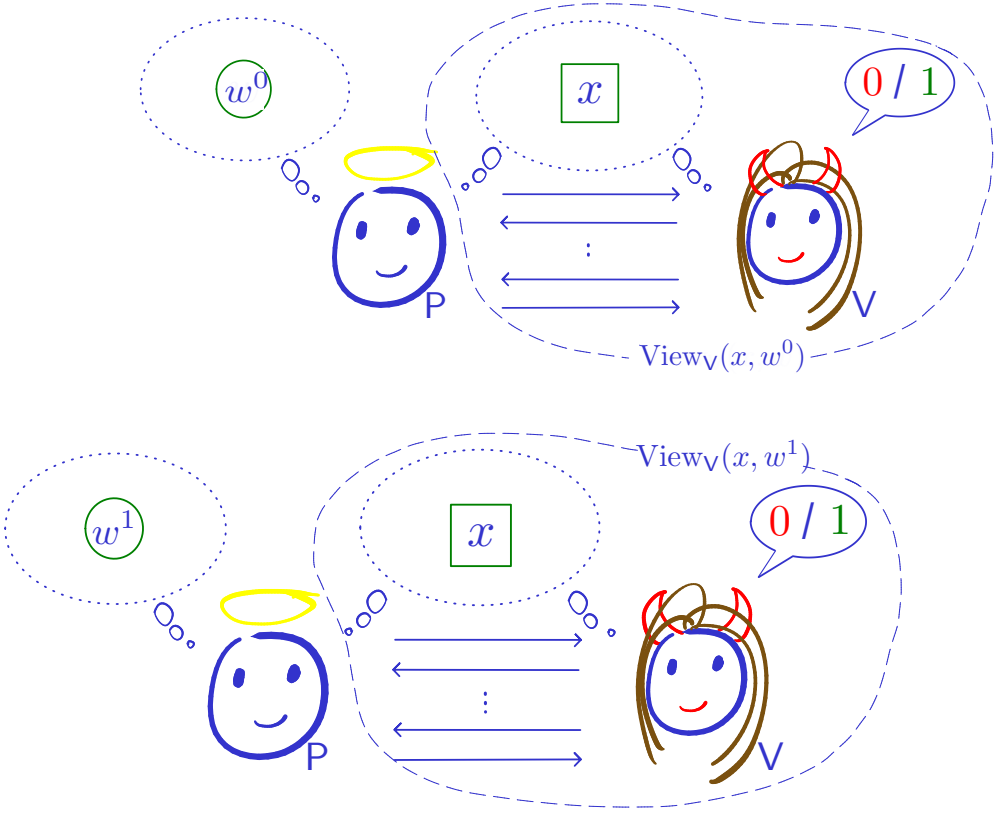
(HONEST-VERIFIER)

WITNESS INDISTINGUISHABILITY [FLS90]



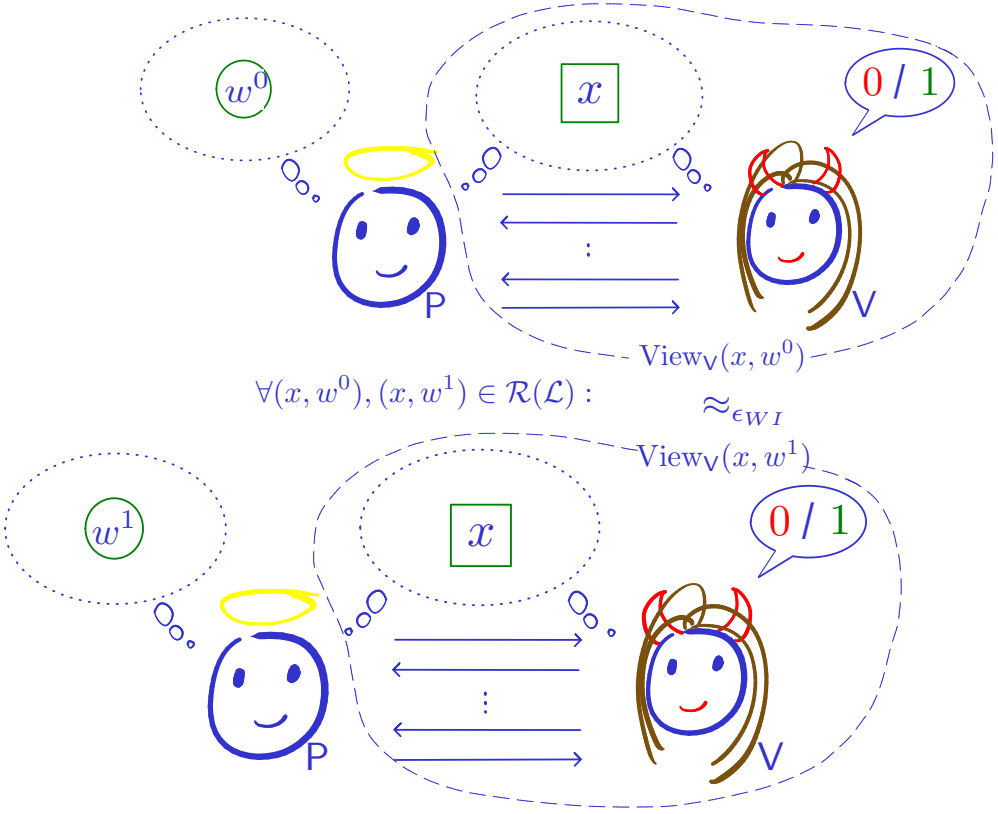
(HONEST-VERIFIER)

WITNESS INDISTINGUISHABILITY [FLS90]

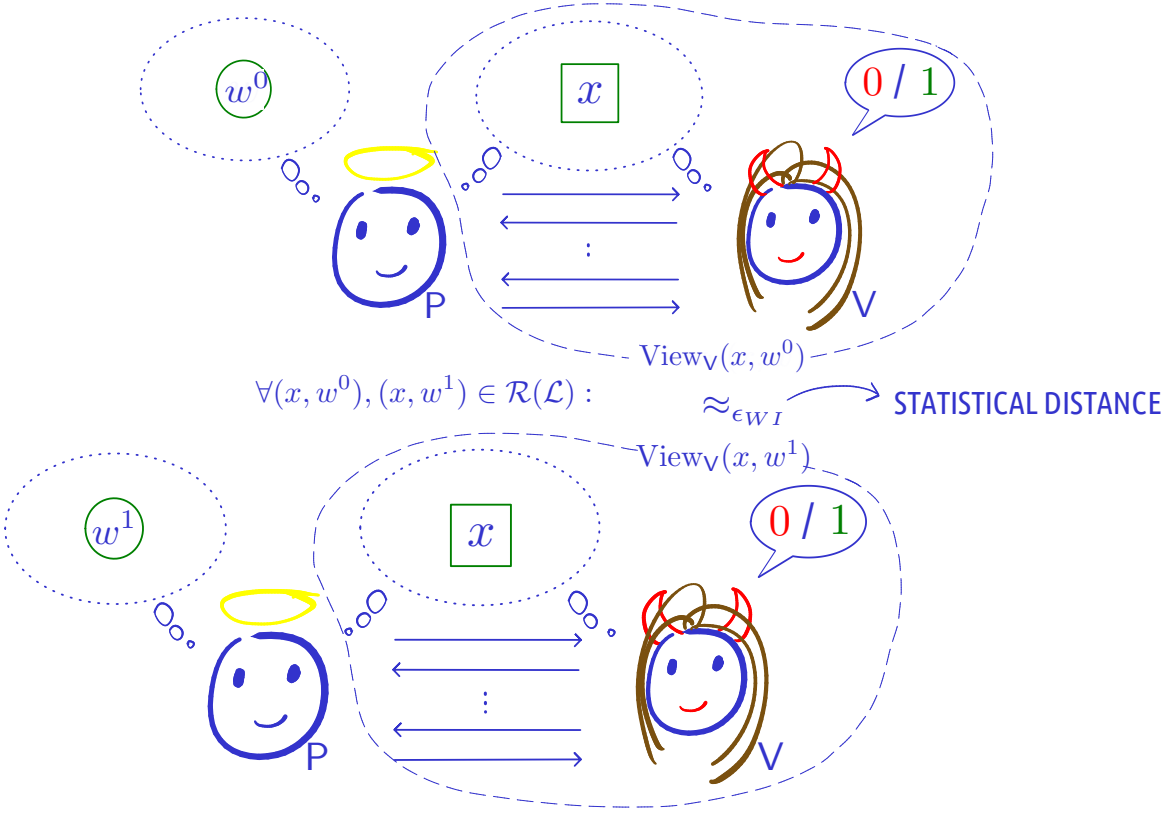


(HONEST-VERIFIER)

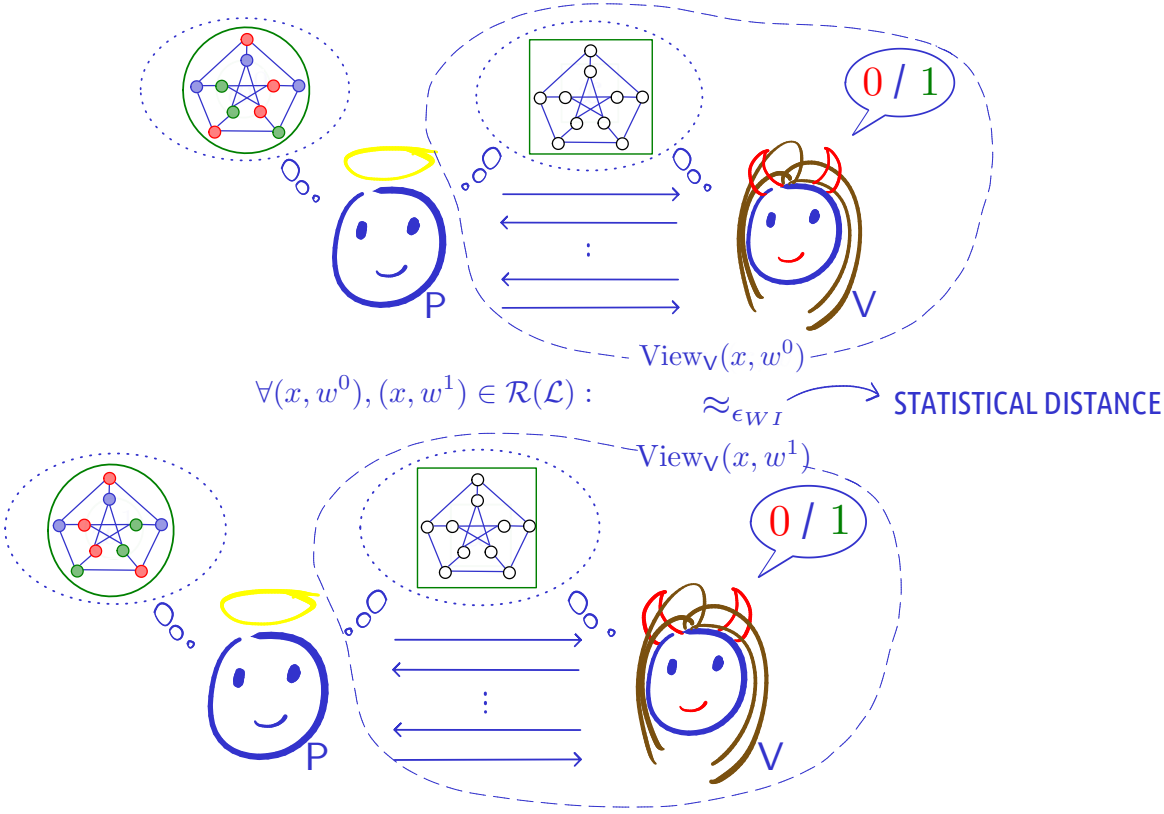
WITNESS INDISTINGUISHABILITY [FLS90]



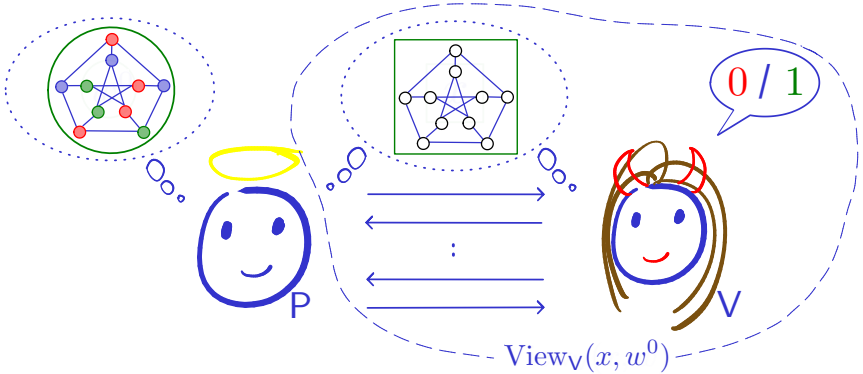
(HONEST-VERIFIER) STATISTICAL WITNESS INDISTINGUISHABILITY [FLS90]



(HONEST-VERIFIER) STATISTICAL WITNESS INDISTINGUISHABILITY [FLS90]



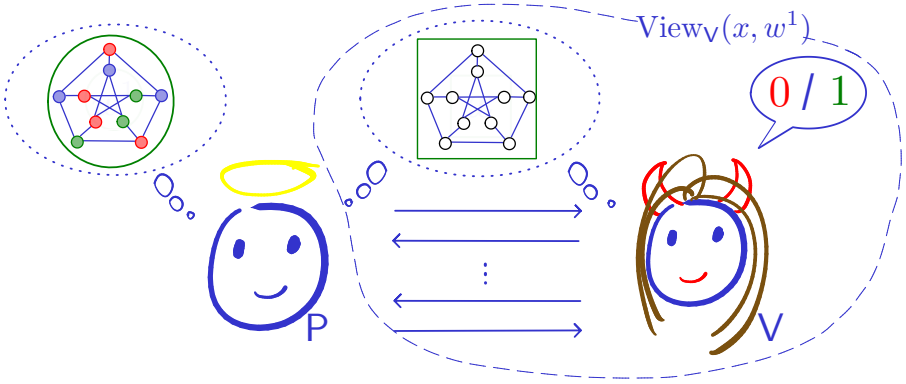
(HONEST-VERIFIER) STATISTICAL WITNESS INDISTINGUISHABILITY [FLS90]



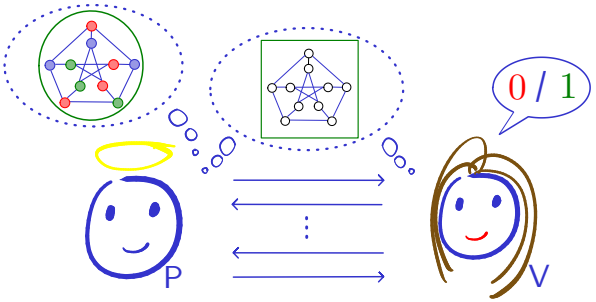
$\text{View}_V(x, w^0)$

$\forall (x, w^0), (x, w^1) \in \mathcal{R}(\mathcal{L}) :$ $\approx_{\epsilon_{WI}}$ STATISTICAL DISTANCE

$\text{View}_V(x, w^1)$



TRIVIAL IF P UNBOUNDED

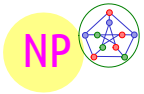


INTERACTIVE PROTOCOLS

- COMPLETENESS
- SOUNDNESS

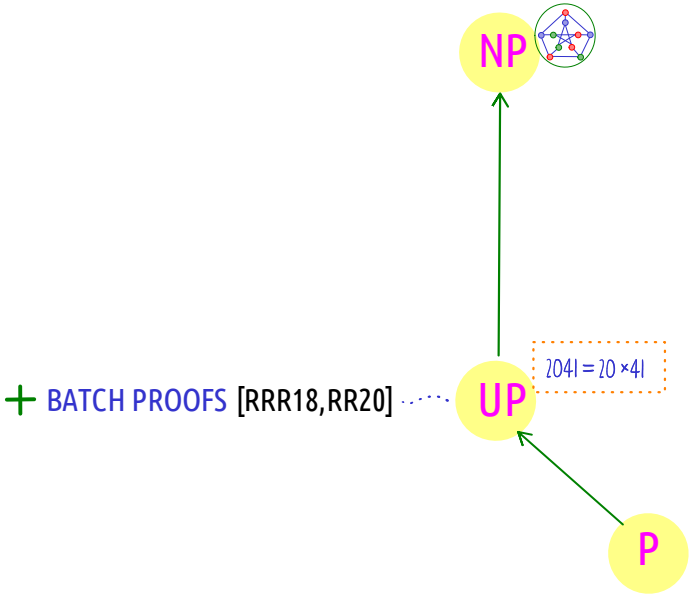
- SUCCINCTNESS
  - BATCHING
- HIDING
  - SWI

WHAT CAN BE BATCHED?



WHAT CAN BE BATCHED?

- PRIOR WORKS



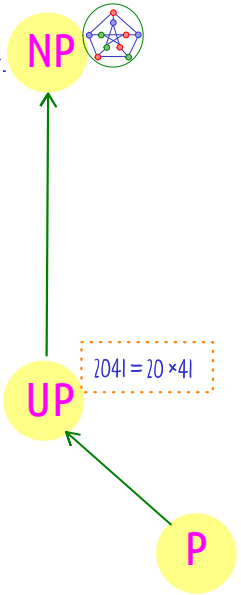
WHAT CAN BE BATCHED?

- PRIOR WORKS

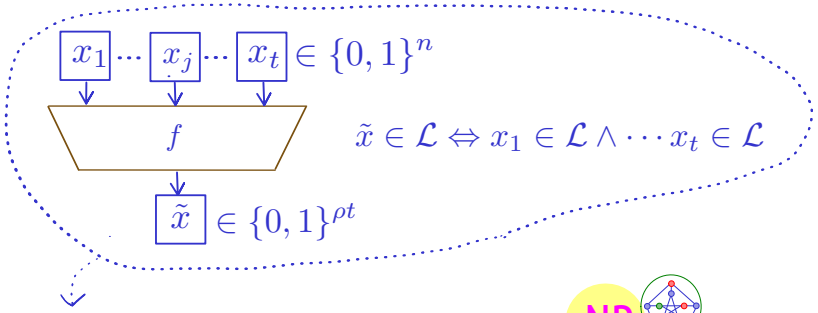
? BATCH PROOFS NOT KNOWN (WHEN HONEST PROVER IS EFFICIENT)

\+ NON-INTERACTIVE BATCH ARGUMENTS FROM STANDARD ASSUMPTIONS [CJJ22, WW22, HJKS22]

\+ BATCH PROOFS [RRR18, RR20]



WHAT CAN BE BATCHED?



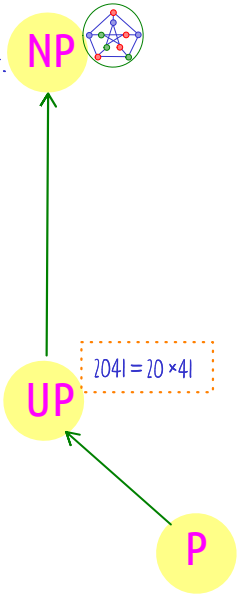
PRIOR WORKS

− INSTANCE COMPRESSION UNLIKELY [D15]

? BATCH PROOFS NOT KNOWN (WHEN HONEST PROVER IS EFFICIENT)

\+ NON-INTERACTIVE BATCH ARGUMENTS FROM STANDARD ASSUMPTIONS [CJJ22,WW22,HJKS22]

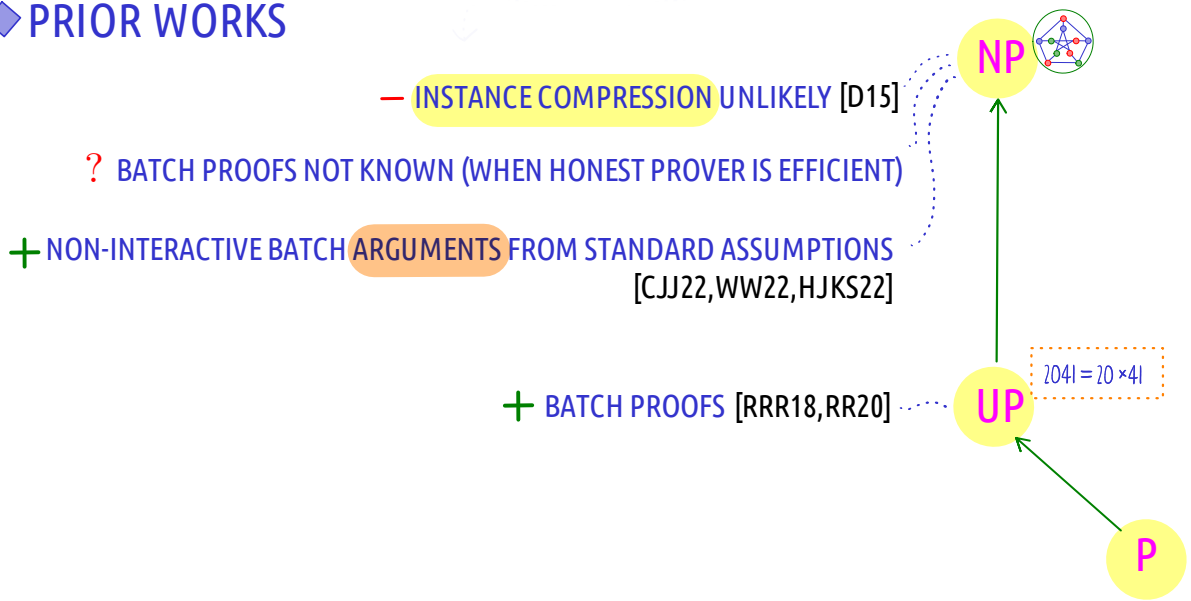
\+ BATCH PROOFS [RRR18,RR20]



WHAT CAN BE BATCHED?

- THIS WORK: WHAT HAPPENS WHEN BATCHING IS POSSIBLE?

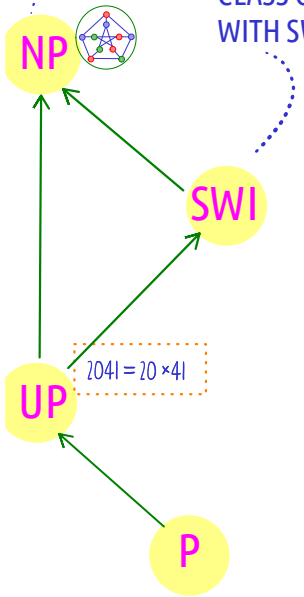
- PRIOR WORKS



WHAT CAN BE BATCHED?

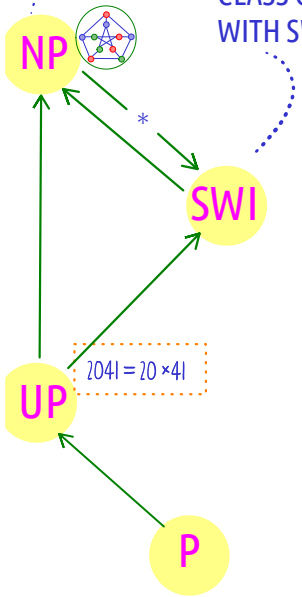
- THIS WORK: WHAT HAPPENS WHEN BATCHING IS POSSIBLE?
  - + BATCH PROOF FOR NP IMPLIES SWI PROOF FOR NP

- PRIOR WORKS
  - − INSTANCE COMPRESSION UNLIKELY [D15]
  - ? BATCH PROOFS NOT KNOWN (WHEN HONEST PROVER IS EFFICIENT)
  - + NON-INTERACTIVE BATCH ARGUMENTS FROM STANDARD ASSUMPTIONS [CJJ22, WW22, HJKS22]
  - + BATCH PROOFS [RRR18, RR20]



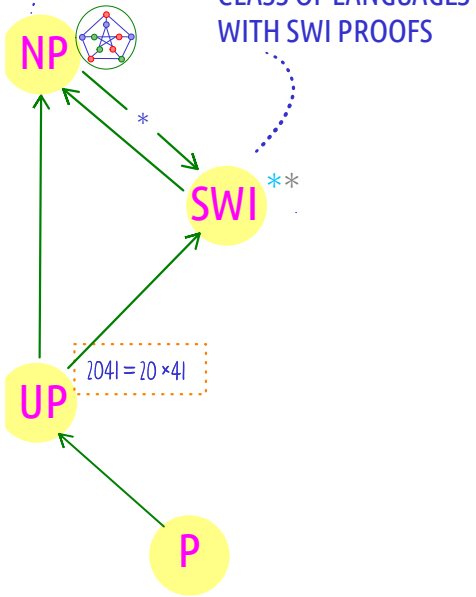
WHAT CAN BE BATCHED?

- THIS WORK: WHAT HAPPENS WHEN BATCHING IS POSSIBLE?
  - + BATCH PROOF FOR NP IMPLIES SWI PROOF FOR NP
  - − *
- PRIOR WORKS
  - − INSTANCE COMPRESSION UNLIKELY [D15]
  - ? BATCH PROOFS NOT KNOWN (WHEN HONEST PROVER IS EFFICIENT)
  - + NON-INTERACTIVE BATCH ARGUMENTS FROM STANDARD ASSUMPTIONS [CJJ22,WW22,HJKS22]
  - + BATCH PROOFS [RRR18,RR20]



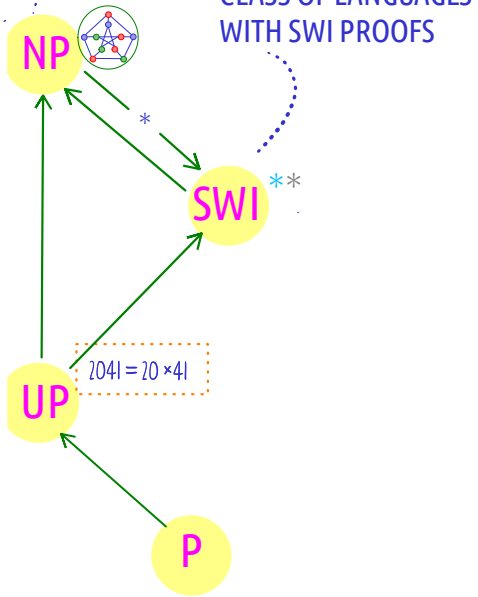
WHAT CAN BE BATCHED?

- THIS WORK: WHAT HAPPENS WHEN BATCHING IS POSSIBLE?
  - ± BATCH PROOF FOR NP IMPLIES SWI PROOF** FOR NP
- PRIOR WORKS
  - − INSTANCE COMPRESSION UNLIKELY [D15]
  - ? BATCH PROOFS NOT KNOWN (WHEN HONEST PROVER IS EFFICIENT)
  - + NON-INTERACTIVE BATCH ARGUMENTS FROM STANDARD ASSUMPTIONS [CJJ22,WW22,HJKS22]
  - + BATCH PROOFS [RRR18,RR20]



WHAT CAN BE BATCHED?

- THIS WORK: WHAT HAPPENS WHEN BATCHING IS POSSIBLE?
  - + BATCH PROOF FOR NP IMPLIES SWI PROOF** FOR NP
  - − *
  - + (NI) BATCH ARGUMENT FOR NP IMPLIES (NI) SWI ARGUMENT** FOR NP
- PRIOR WORKS
  - − INSTANCE COMPRESSION UNLIKELY [D15]
  - ? BATCH PROOFS NOT KNOWN (WHEN HONEST PROVER IS EFFICIENT)
  - + NON-INTERACTIVE BATCH ARGUMENTS FROM STANDARD ASSUMPTIONS [CJJ22,WW22,HJKS22]
  - + BATCH PROOFS [RRR18,RR20]



PLAN

- BACKGROUND
  - DEFINITIONS: BATCH PROOFS STAT. WITNESS INDISTINGUISHABILITY (SWI)
  - WHAT CAN BE BATCHED?
- **MAIN RESULT**
  - **BATCH PROOFS $\Rightarrow$ SWI PROOFS**
  - **TECHNICAL OVERVIEW**
- MORE RESULTS
  - ONE-WAY FUNCTION + BATCH ARGUMENTS $\Rightarrow$ SZK ARGUMENTS
  - NON-INTERACTIVE (NI) BATCH ARGUMENTS $\Rightarrow$ NI SZK ARGUMENTS
- OPEN QUESTIONS

BATCH PROOFS $\Rightarrow$ SWI PROOFS

- *MAIN THEOREM.*

(PUBLIC-COIN) BATCH PROOF FOR $\mathcal{L}^t$ WITH COMPRESSION RATE ρ

$\Downarrow$

(PUBLIC-COIN) HV-SWI PROOF** FOR $\mathcal{L}$

BATCH PROOFS $\Rightarrow$ SWI PROOFS

MAIN THEOREM.

(PUBLIC-COIN) BATCH PROOF FOR $\mathcal{L}^t$ WITH COMPRESSION RATE ρ

$\Downarrow$

(PUBLIC-COIN) HV-SWI PROOF** FOR $\mathcal{L}$

- NEGLIGIBLE SOUNDNESS ERROR
- WI ERROR $\epsilon_{WI} \approx \sqrt{\rho}$: CAN BE INVERSE-POLYNOMIAL $(*)$
- PROVER IS NON-UNIFORM $(*)$

BATCH PROOFS $\Rightarrow$ SWI PROOFS

MAIN THEOREM.

(PUBLIC-COIN) BATCH PROOF FOR $\mathcal{L}^t$ WITH COMPRESSION RATE ρ

$\Downarrow$

(PUBLIC-COIN) HV-SWI PROOF** FOR $\mathcal{L}$

$\Downarrow$ [GSV98]

SWI PROOF** FOR $\mathcal{L}$

- NEGLIGIBLE SOUNDNESS ERROR
- WI ERROR $\epsilon_{WI} \approx \sqrt{\rho}$: CAN BE INVERSE-POLYNOMIAL $(*)$
- PROVER IS NON-UNIFORM $(*)$

BATCH PROOFS $\Rightarrow$ SWI PROOFS

- *MAIN THEOREM.*

  (PUBLIC-COIN) BATCH PROOF FOR $\mathcal{L}^t$ WITH COMPRESSION RATE ρ

  $\Downarrow$

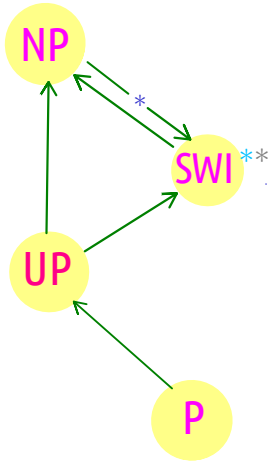
  (PUBLIC-COIN) HV-SWI PROOF** FOR $\mathcal{L}$

  $\Downarrow$ [GSV98]

  SWI PROOF** FOR $\mathcal{L}$

  - NEGLIGIBLE SOUNDNESS ERROR
  - WI ERROR $\epsilon_{WI} \approx \sqrt{\rho}$: CAN BE INVERSE-POLYNOMIAL $(*)$
  - PROVER IS NON-UNIFORM $(*)$

– *COROLLARY.* IF NP DOESN'T HAVE HV-SWI PROOFS**
THEN IT DOESN'T HAVE BATCH PROOFS



BATCH PROOFS $\Rightarrow$ SWI PROOFS

- *MAIN THEOREM.*

  (PUBLIC-COIN) BATCH PROOF FOR $\mathcal{L}^t$ WITH COMPRESSION RATE ρ

  $\Downarrow$

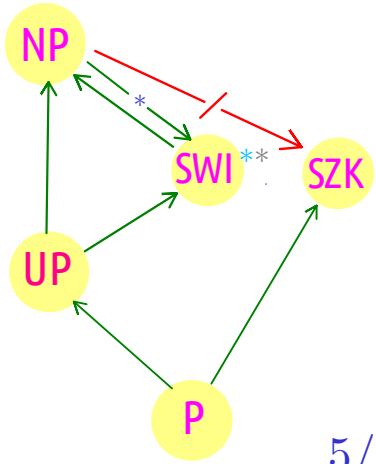
  (PUBLIC-COIN) HV-SWI PROOF** FOR $\mathcal{L}$

  $\Downarrow$ [GSV98]

  SWI PROOF** FOR $\mathcal{L}$

  - NEGLIGIBLE SOUNDNESS ERROR
  - WI ERROR $\epsilon_{WI} \approx \sqrt{\rho}$: CAN BE INVERSE-POLYNOMIAL $(*)$
  - PROVER IS NON-UNIFORM $(*)$

- *COROLLARY.* IF NP DOESN'T HAVE HV-SWI PROOFS** THEN IT DOESN'T HAVE BATCH PROOFS
  - $\mathbf{NP} \subseteq \mathbf{SZK} \Rightarrow$ POLYNOMIAL HIERARCHY COLLAPSES [F89,AH91]
  - SWI SHOULD NOT BE MUCH MORE POWERFUL THAN SZK



BATCH PROTOCOL $\mapsto$ SWI PROTOCOL

$\Pi = (\mathsf{P}, \mathsf{V})$ $\quad$ $\Pi' = (\mathsf{P}', \mathsf{V}')$

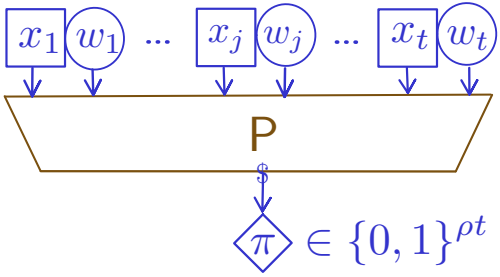
BATCH PROTOCOL $\Pi = (\mathsf{P}, \mathsf{V})$ $\mapsto$ SWI PROTOCOL $\Pi' = (\mathsf{P}', \mathsf{V}')$

- SIMPLIFYING ASSUMPTION: Π IS NON-INTERACTIVE $\Rightarrow$ P RANDOMISED FN.

BATCH PROTOCOL $\mapsto$ SWI PROTOCOL

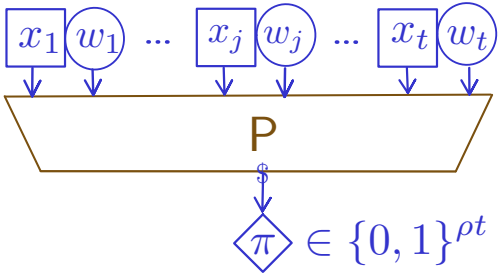
$\Pi = (\mathsf{P}, \mathsf{V})$ $\qquad$ $\Pi' = (\mathsf{P}', \mathsf{V}')$

- SIMPLIFYING ASSUMPTION: Π IS NON-INTERACTIVE $\Rightarrow$ P RANDOMISED FN.



BATCH PROTOCOL $\Pi = (\mathsf{P}, \mathsf{V})$ $\mapsto$ SWI PROTOCOL $\Pi' = (\mathsf{P}', \mathsf{V}')$

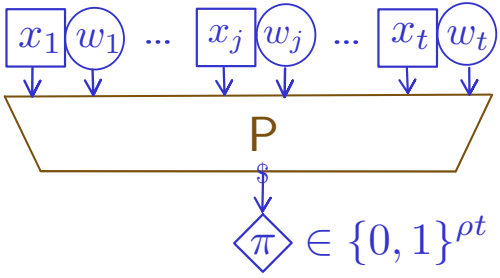
- SIMPLIFYING ASSUMPTION: Π IS NON-INTERACTIVE $\Rightarrow$ P RANDOMISED FN.
  - FOR INTERACTIVE Π, FIX V'S RANDOM COINS $\$$



BATCH PROTOCOL $\mapsto$ SWI PROTOCOL

$\Pi = (\mathsf{P}, \mathsf{V})$ $\qquad$ $\Pi' = (\mathsf{P}', \mathsf{V}')$

- SIMPLIFYING ASSUMPTION: Π IS NON-INTERACTIVE $\Rightarrow$ P RANDOMISED FN.
  - FOR INTERACTIVE Π, FIX V'S RANDOM COINS $\$$



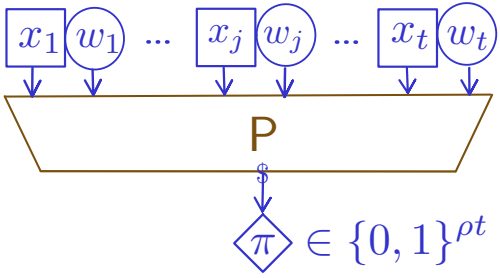
INTUITION

$\blacklozenge \mapsto \blacklozenge$

P IS COMPRESSING $\Rightarrow$ LOSES INFORMATION ABOUT INPUT $\mapsto$ SWI OF Π'

BATCH PROTOCOL $\Pi = (\mathsf{P}, \mathsf{V})$ $\mapsto$ SWI PROTOCOL $\Pi' = (\mathsf{P}', \mathsf{V}')$

- SIMPLIFYING ASSUMPTION: Π IS NON-INTERACTIVE $\Rightarrow$ P RANDOMISED FN.
  - FOR INTERACTIVE Π, FIX V'S RANDOM COINS $\$$



INTUITION

P IS COMPRESSING $\Rightarrow$ LOSES INFORMATION ABOUT INPUT $\mapsto$ SWI OF Π'

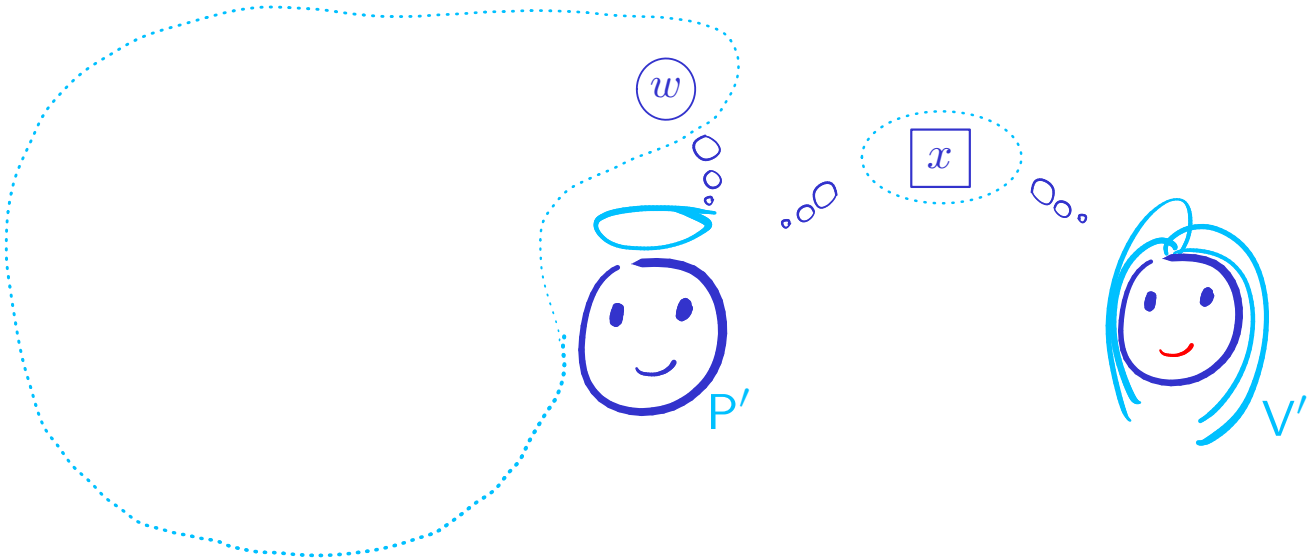
Π COMPLETE AND SOUND $\Rightarrow$ Π' COMPLETE AND SOUND

BATCH PROTOCOL $\mapsto$ SWI PROTOCOL...

$\Pi = (\mathsf{P}, \mathsf{V})$ $\quad$ $\Pi' = (\mathsf{P}', \mathsf{V}')$

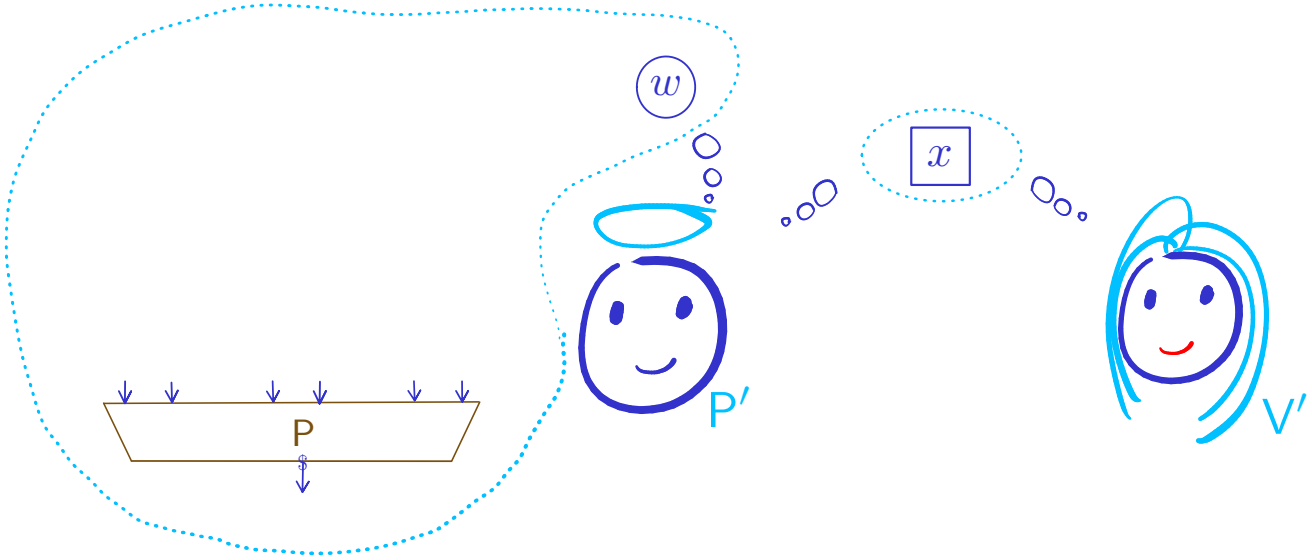
BATCH PROTOCOL $\mapsto$ SWI PROTOCOL...

$\Pi = (\mathsf{P}, \mathsf{V})$ $\Pi' = (\mathsf{P}', \mathsf{V}')$



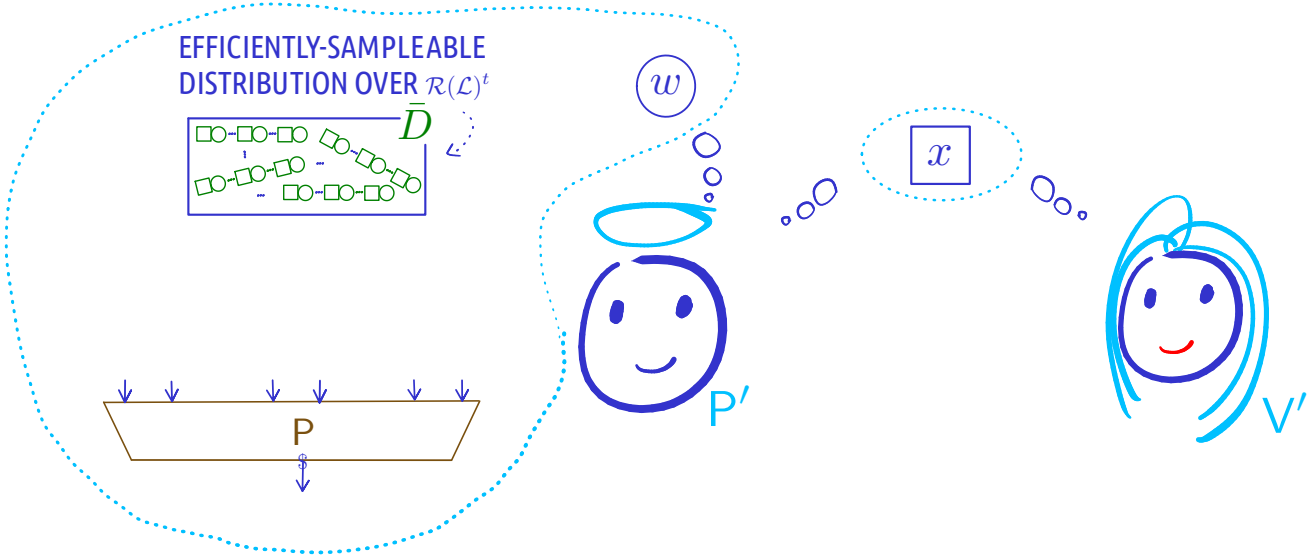
BATCH PROTOCOL $\mapsto$ SWI PROTOCOL...

$\Pi = (\mathsf{P}, \mathsf{V})$ $\Pi' = (\mathsf{P}', \mathsf{V}')$



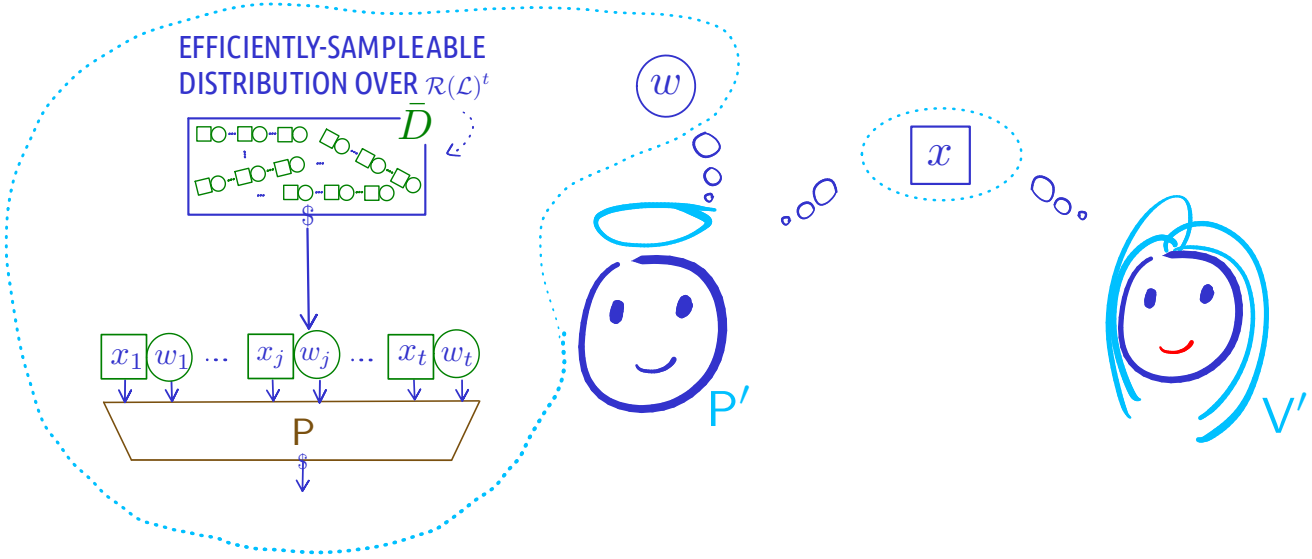
BATCH PROTOCOL $\mapsto$ SWI PROTOCOL...

$\Pi = (\mathsf{P}, \mathsf{V})$ $\quad$ $\Pi' = (\mathsf{P}', \mathsf{V}')$



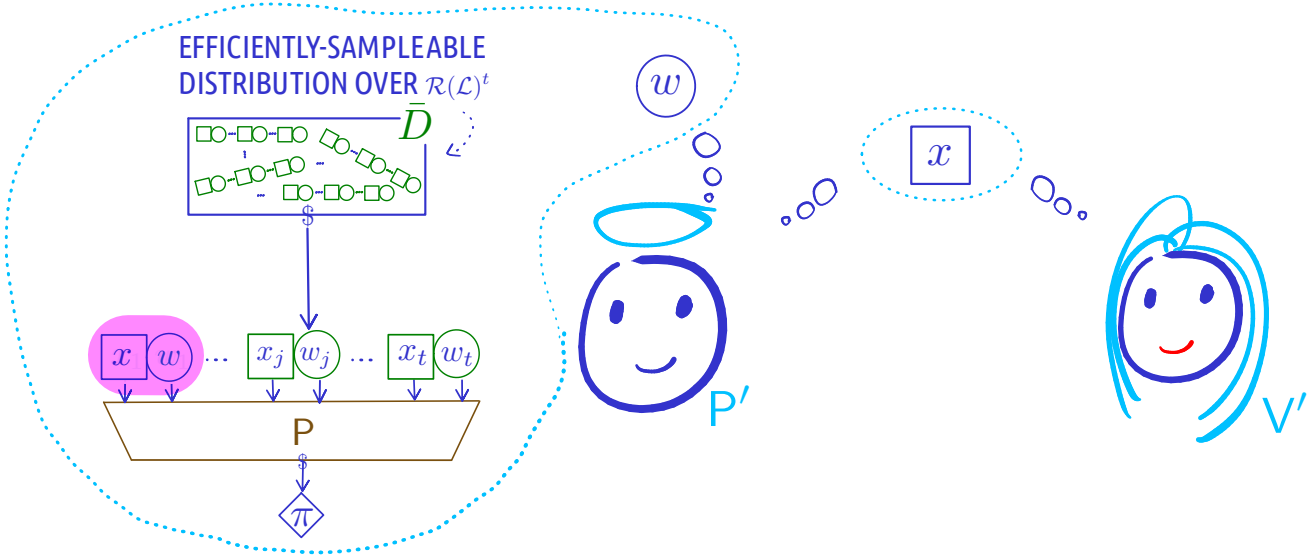
BATCH PROTOCOL $\mapsto$ SWI PROTOCOL...

$\Pi = (\mathsf{P}, \mathsf{V})$ $\quad$ $\Pi' = (\mathsf{P}', \mathsf{V}')$



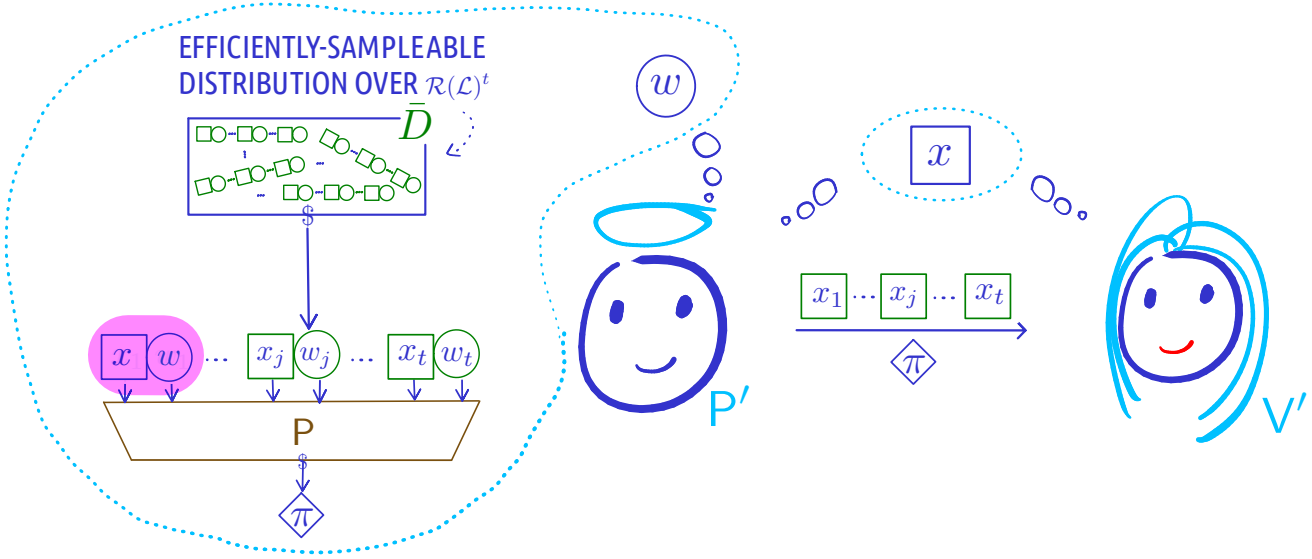
BATCH PROTOCOL $\Pi = (\mathsf{P}, \mathsf{V})$ $\mapsto$ SWI PROTOCOL... $\Pi' = (\mathsf{P}', \mathsf{V}')$

- FIRST ATTEMPT: EMBED GIVEN INSTANCE+WITNESS AT 1-st LOCATION



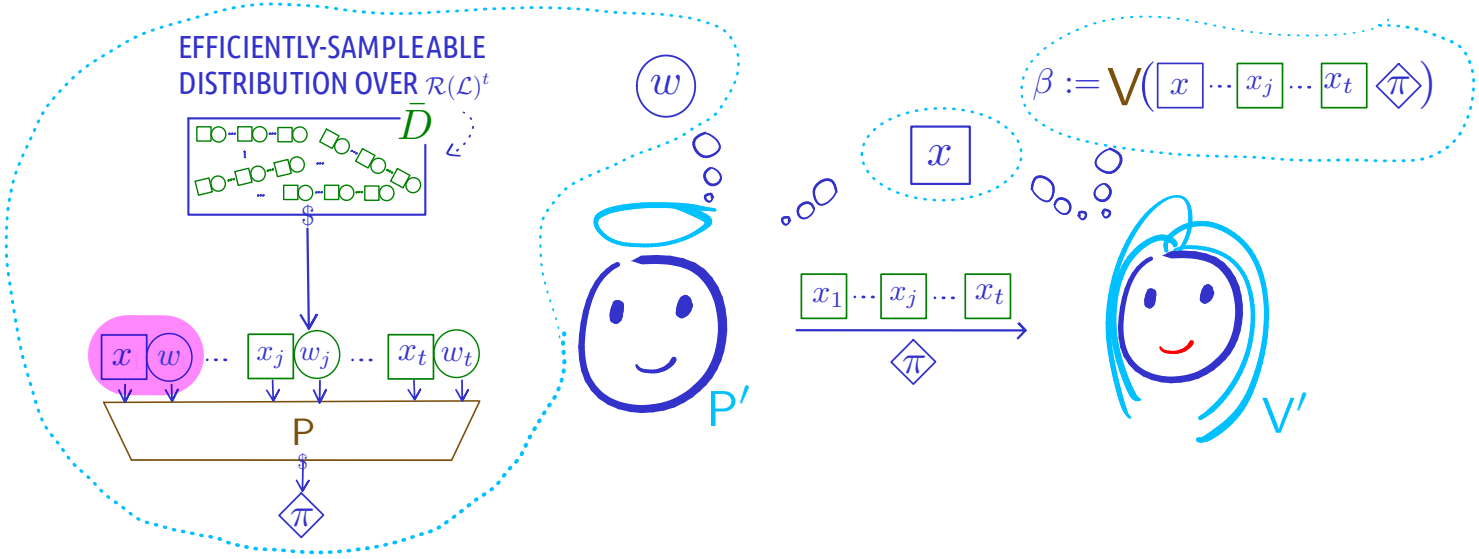
BATCH PROTOCOL $\Pi = (\mathsf{P}, \mathsf{V})$ $\mapsto$ SWI PROTOCOL... $\Pi' = (\mathsf{P}', \mathsf{V}')$

- FIRST ATTEMPT: EMBED GIVEN INSTANCE+WITNESS AT 1-st LOCATION



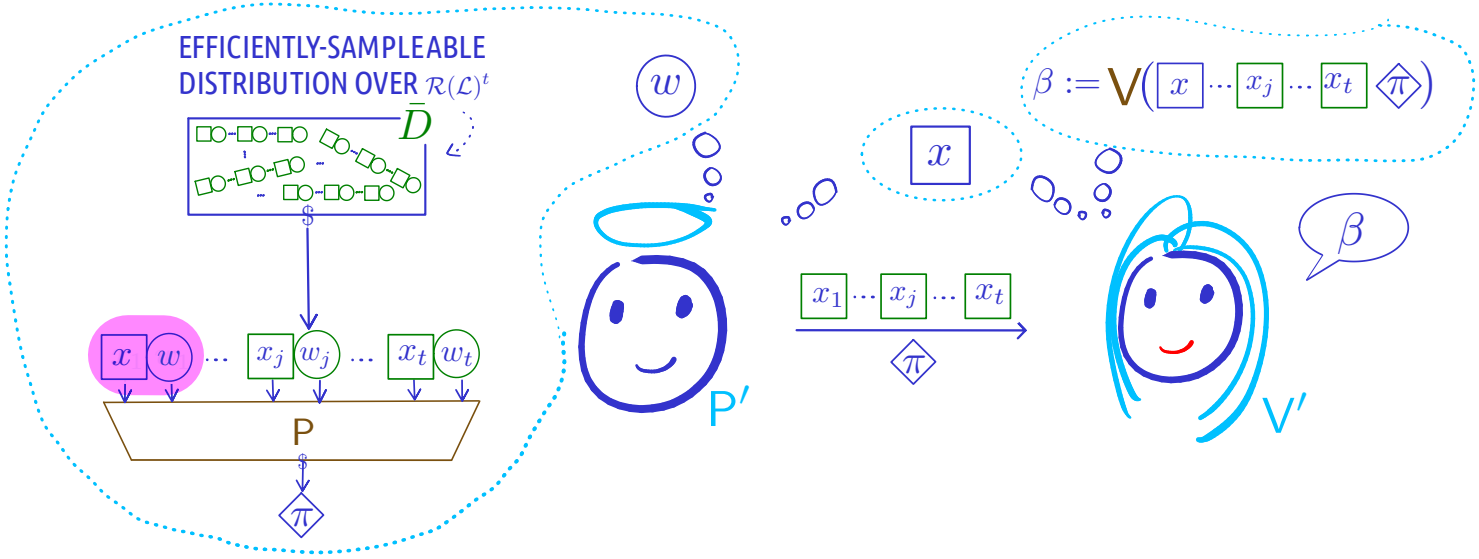
BATCH PROTOCOL $\Pi = (\mathsf{P}, \mathsf{V})$ $\mapsto$ SWI PROTOCOL... $\Pi' = (\mathsf{P}', \mathsf{V}')$

- FIRST ATTEMPT: EMBED GIVEN INSTANCE+WITNESS AT 1-st LOCATION



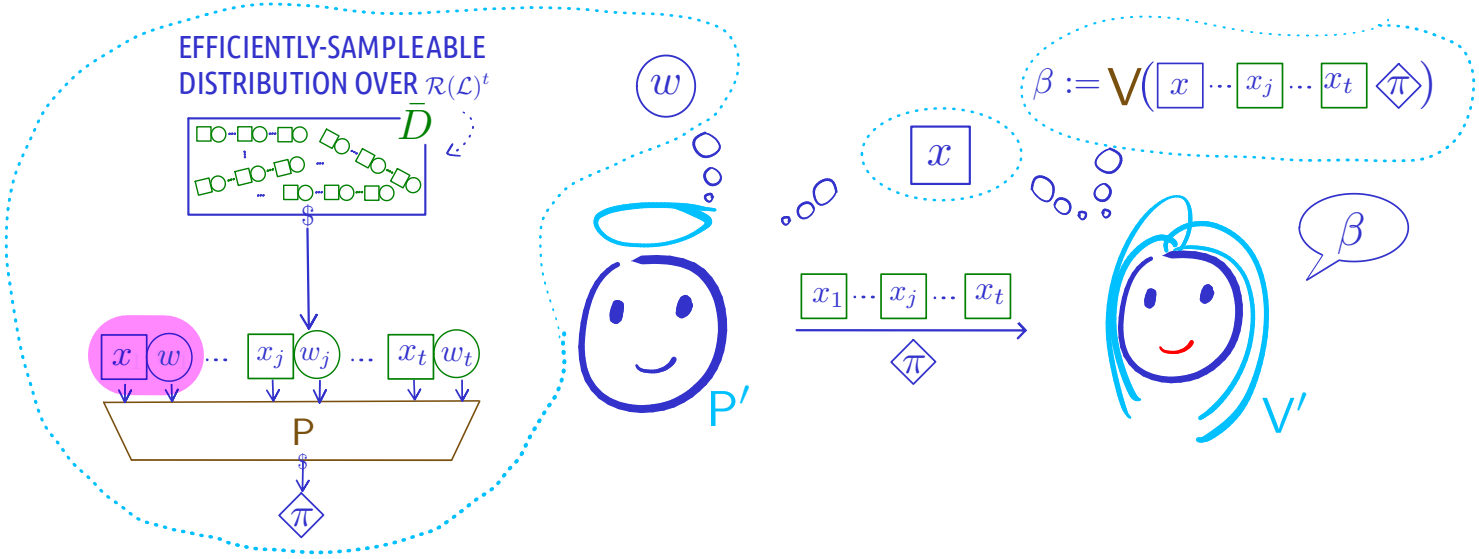
BATCH PROTOCOL $\Pi = (\mathsf{P}, \mathsf{V})$ $\mapsto$ SWI PROTOCOL... $\Pi' = (\mathsf{P}', \mathsf{V}')$

- FIRST ATTEMPT: EMBED GIVEN INSTANCE+WITNESS AT 1-st LOCATION



BATCH PROTOCOL $\Pi = (\mathsf{P}, \mathsf{V})$ $\mapsto$ SWI PROTOCOL... $\Pi' = (\mathsf{P}', \mathsf{V}')$

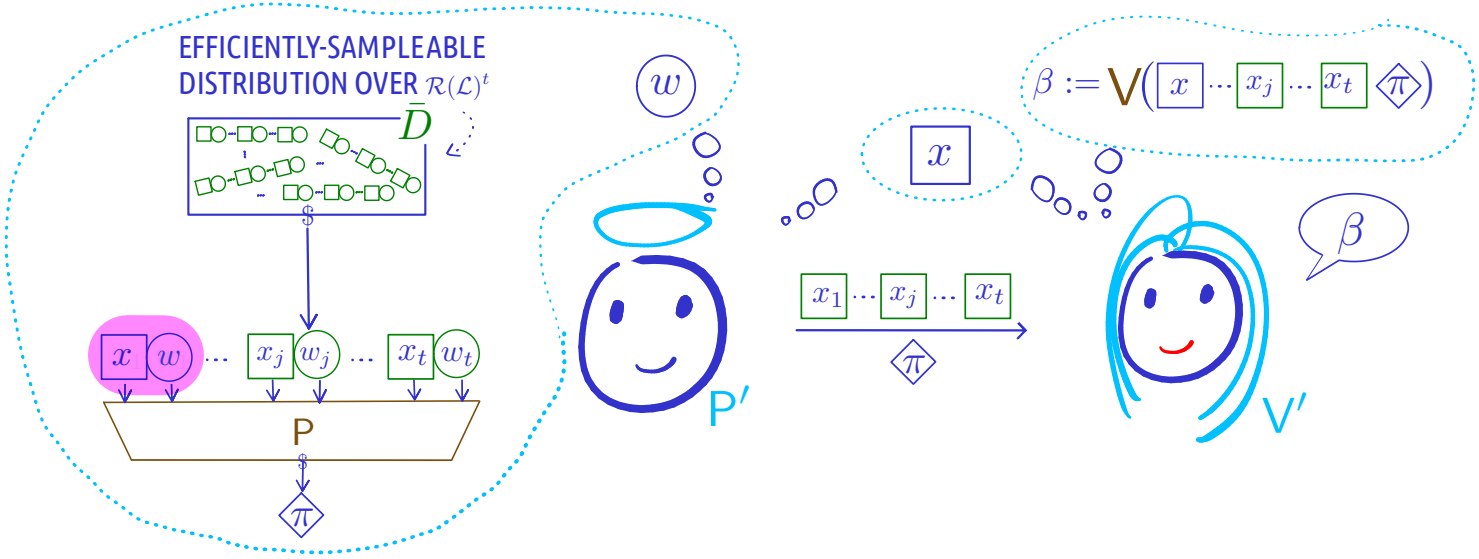
- FIRST ATTEMPT: EMBED GIVEN INSTANCE+WITNESS AT 1-st LOCATION



- Π COMPLETE AND SOUND $\Rightarrow$ Π' COMPLETE AND SOUND ✓

BATCH PROTOCOL $\Pi = (\mathsf{P}, \mathsf{V})$ $\mapsto$ SWI PROTOCOL... $\Pi' = (\mathsf{P}', \mathsf{V}')$

- FIRST ATTEMPT: EMBED GIVEN INSTANCE+WITNESS AT 1-st LOCATION



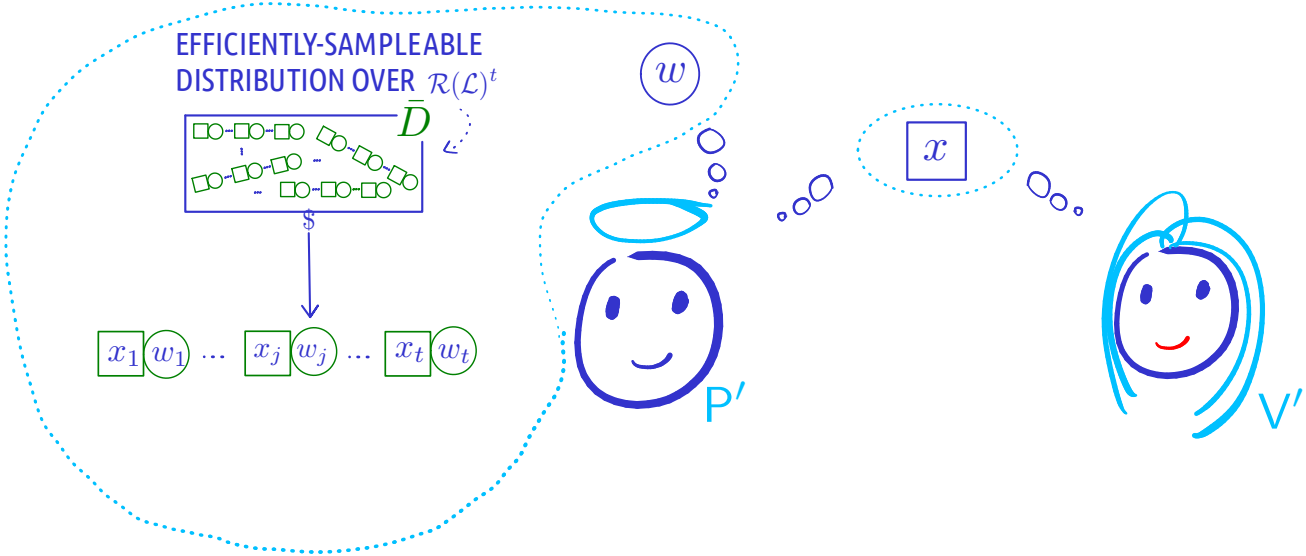
- Π COMPLETE AND SOUND $\Rightarrow$ Π' COMPLETE AND SOUND ✓
- NOT SWI! CONSIDER P THAT DUMPS WITNESS OF 1-ST INPUT ✗
  - COULD BE COMPRESSING, BUT REVEALS WITNESS

BATCH PROTOCOL $\mapsto$ SWI PROTOCOL...

$\Pi = (\mathsf{P}, \mathsf{V})$ $\quad$ $\Pi' = (\mathsf{P}', \mathsf{V}')$

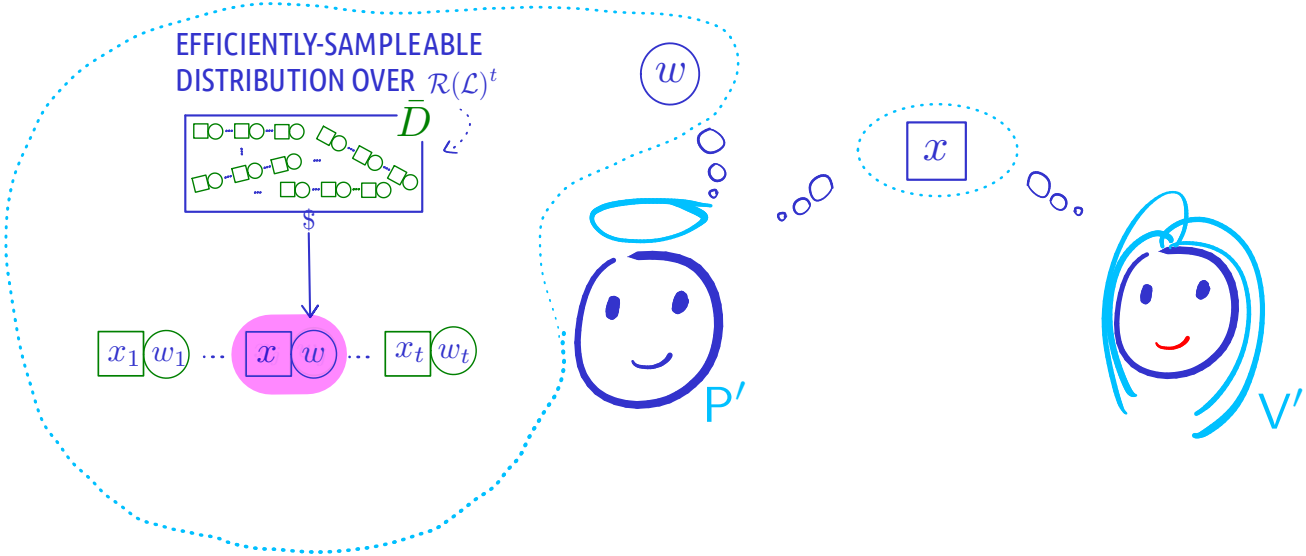
BATCH PROTOCOL $\mapsto$ SWI PROTOCOL...

$\Pi = (\mathsf{P}, \mathsf{V})$ $\Pi' = (\mathsf{P}', \mathsf{V}')$



BATCH PROTOCOL $\Pi = (\mathsf{P}, \mathsf{V})$ $\mapsto$ SWI PROTOCOL... $\Pi' = (\mathsf{P}', \mathsf{V}')$

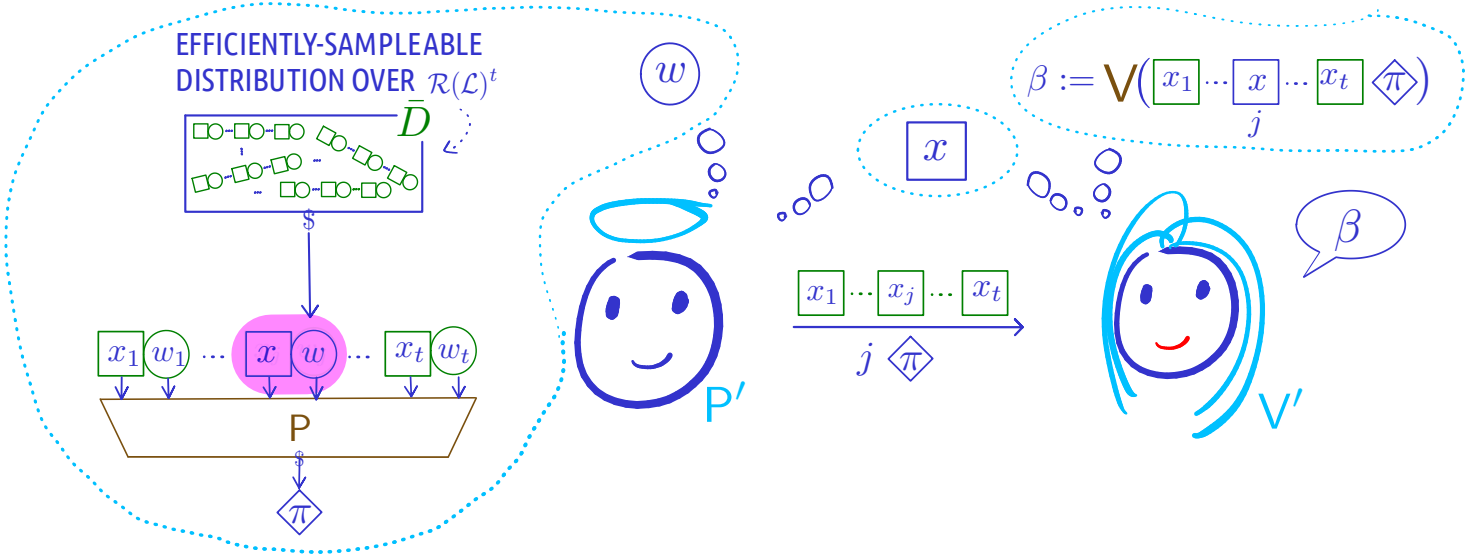
- SOLUTION: EMBED GIVEN INSTANCE+WITNESS AT RANDOM LOCATION $j \in [1, t]$



BATCH PROTOCOL $\mapsto$ SWI PROTOCOL...

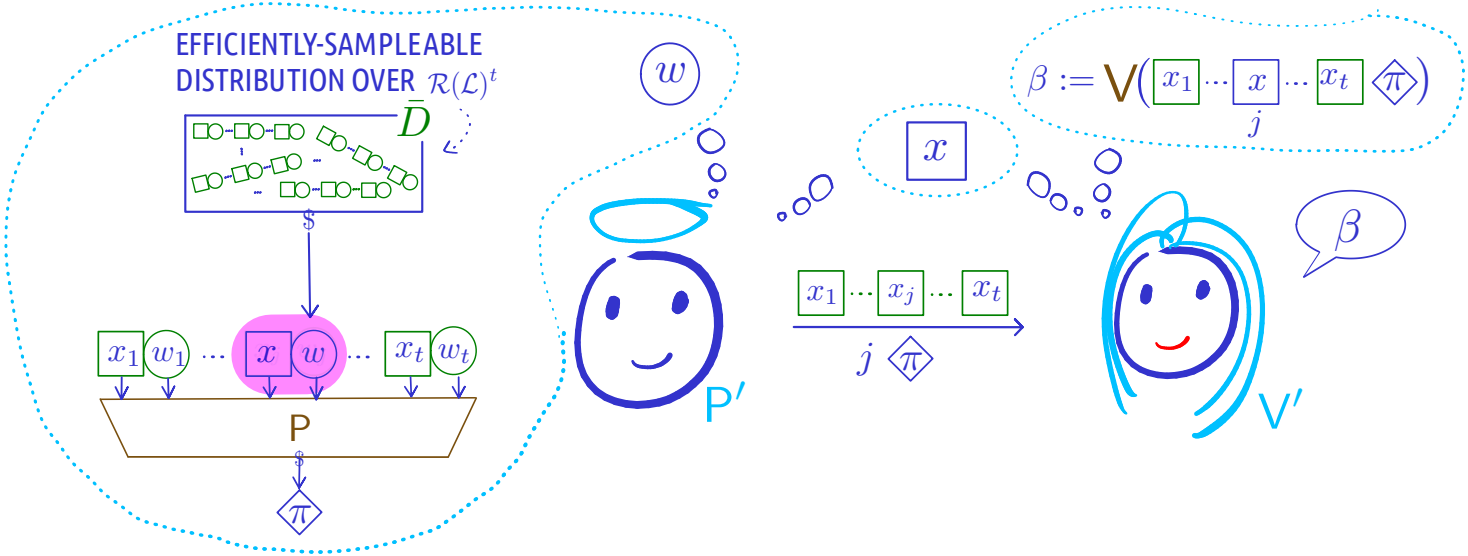
$\Pi = (\mathsf{P}, \mathsf{V})$ $\quad$ $\Pi' = (\mathsf{P}', \mathsf{V}')$

- SOLUTION: EMBED GIVEN INSTANCE+WITNESS AT RANDOM LOCATION $j \in [1, t]$



BATCH PROTOCOL $\Pi = (\mathsf{P}, \mathsf{V})$ $\mapsto$ SWI PROTOCOL... $\Pi' = (\mathsf{P}', \mathsf{V}')$

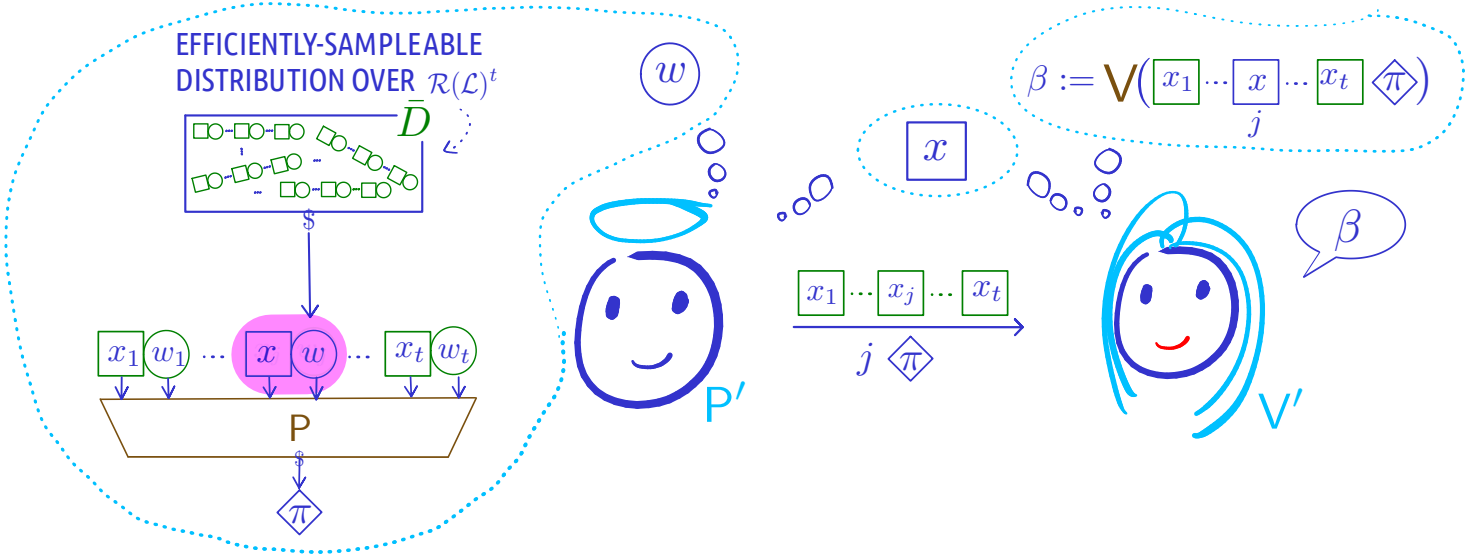
- SOLUTION: EMBED GIVEN INSTANCE+WITNESS AT RANDOM LOCATION $j \in [1, t]$



- Π COMPLETE AND SOUND $\Rightarrow$ Π' COMPLETE AND SOUND ✓

BATCH PROTOCOL $\Pi = (\mathsf{P}, \mathsf{V})$ $\mapsto$ SWI PROTOCOL... $\Pi' = (\mathsf{P}', \mathsf{V}')$

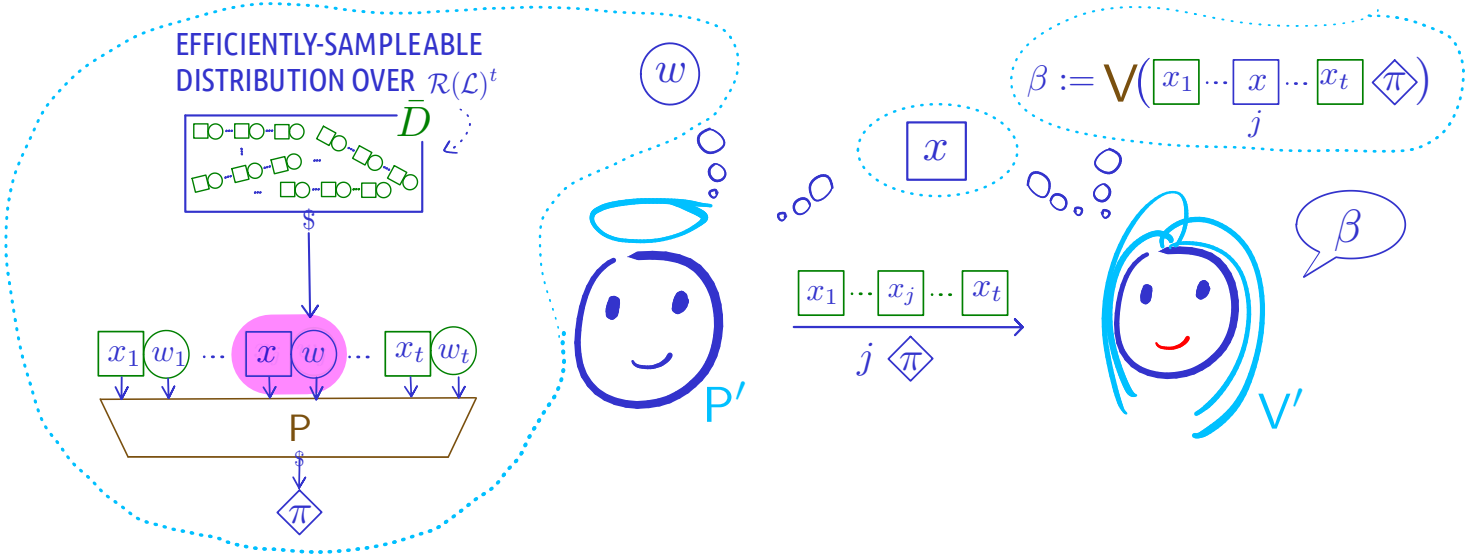
- SOLUTION: EMBED GIVEN INSTANCE+WITNESS AT RANDOM LOCATION $j \in [1, t]$



- Π COMPLETE AND SOUND $\Rightarrow$ Π' COMPLETE AND SOUND ✓
- SEEMS SWI WHEN P IS COMPRESSING

BATCH PROTOCOL $\Pi = (\mathsf{P}, \mathsf{V})$ $\mapsto$ SWI PROTOCOL... $\Pi' = (\mathsf{P}', \mathsf{V}')$

- SOLUTION: EMBED GIVEN INSTANCE+WITNESS AT RANDOM LOCATION $j \in [1, t]$



- Π COMPLETE AND SOUND $\Rightarrow$ Π' COMPLETE AND SOUND ✓
- SEEMS SWI WHEN P IS COMPRESSING

» HOW TO FIX $\bar{D}$? «

HOW TO FIX $\bar{D}$?

$\forall \mathsf{P} \exists \bar{D} \forall (x, w^0, w^1) : \mathrm{View}_{\mathsf{V}'}(x, w^0) \approx \mathrm{View}_{\mathsf{V}'}(x, w^1)$

$(\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \langle \pi^0 \rangle) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \langle \pi^1 \rangle)$

HOW TO FIX $\bar{D}$?

$\forall \mathsf{P} \exists \bar{D} \forall (x, w^0, w^1) : \mathrm{View}_{\mathsf{V}'}(x, w^0) \approx \mathrm{View}_{\mathsf{V}'}(x, w^1)$

$(\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^0) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^1)$

- CHALLENGE: DEALING WITH WORST-CASE WI
  - FIX (x, w^0, w^1) AND CONSIDER PROVER $\mathsf{P}_{\{x\}}$ THAT DUMPS THE WITNESS OF x AS PART OF PROOF π

HOW TO FIX $\bar{D}$?

$\forall \mathsf{P} \exists \bar{D} \forall (x, w^0, w^1) : \mathrm{View}_{\mathsf{V}'}(x, w^0) \approx \mathrm{View}_{\mathsf{V}'}(x, w^1)$

$(x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$

- CHALLENGE: DEALING WITH WORST-CASE WI
  - FIX (x, w^0, w^1) AND CONSIDER PROVER $\mathsf{P}_{\{x\}}$ THAT DUMPS THE WITNESS OF x AS PART OF PROOF π
- THERE EXISTS $\bar{D}$ THAT WORKS FOR $\mathsf{P}_{\{x\}}$

$x\,w^0\,w^1 \cdots x\,w^0\,w^1 \cdots x\,w^0\,w^1$

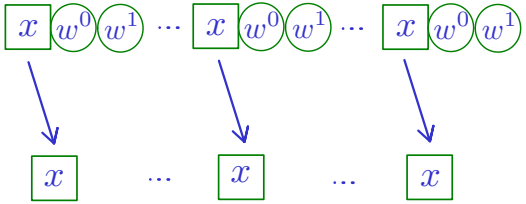
HOW TO FIX $\bar{D}$?

$\forall \mathsf{P} \exists \bar{D} \forall (x, w^0, w^1) : \mathrm{View}_{\mathsf{V}'}(x, w^0) \approx \mathrm{View}_{\mathsf{V}'}(x, w^1)$

$(x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$

- CHALLENGE: DEALING WITH WORST-CASE WI
  - FIX (x, w^0, w^1) AND CONSIDER PROVER $\mathsf{P}_{\{x\}}$ THAT DUMPS THE WITNESS OF x AS PART OF PROOF π

- THERE EXISTS $\bar{D}$ THAT WORKS FOR $\mathsf{P}_{\{x\}}$



HOW TO FIX $\bar{D}$?

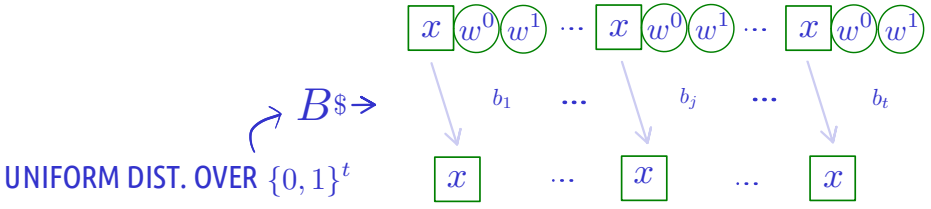
$\forall \mathsf{P} \exists \bar{D} \forall (x, w^0, w^1) : \mathrm{View}_{\mathsf{V}'}(x, w^0) \approx \mathrm{View}_{\mathsf{V}'}(x, w^1)$

$(x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$

CHALLENGE: DEALING WITH WORST-CASE WI

- FIX (x, w^0, w^1) AND CONSIDER PROVER $\mathsf{P}_{\{x\}}$ THAT DUMPS THE WITNESS OF x AS PART OF PROOF π

THERE EXISTS $\bar{D}$ THAT WORKS FOR $\mathsf{P}_{\{x\}}$



HOW TO FIX $\bar{D}$?

$\forall \mathsf{P} \exists \bar{D} \forall (x, w^0, w^1) : \mathrm{View}_{\mathsf{V}'}(x, w^0) \approx \mathrm{View}_{\mathsf{V}'}(x, w^1)$

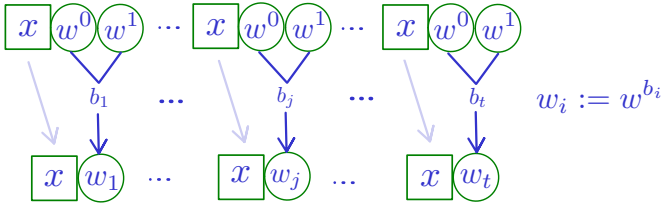
$(x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$

CHALLENGE: DEALING WITH WORST-CASE WI

- FIX (x, w^0, w^1) AND CONSIDER PROVER $\mathsf{P}_{\{x\}}$ THAT DUMPS THE WITNESS OF x AS PART OF PROOF π

THERE EXISTS $\bar{D}$ THAT WORKS FOR $\mathsf{P}_{\{x\}}$

$B^{\$} \rightarrow$ UNIFORM DIST. OVER $\{0,1\}^t$



HOW TO FIX $\bar{D}$?

$\forall \mathsf{P} \exists \bar{D} \forall (x, w^0, w^1) : \mathrm{View}_{\mathsf{V}'}(x, w^0) \approx \mathrm{View}_{\mathsf{V}'}(x, w^1)$

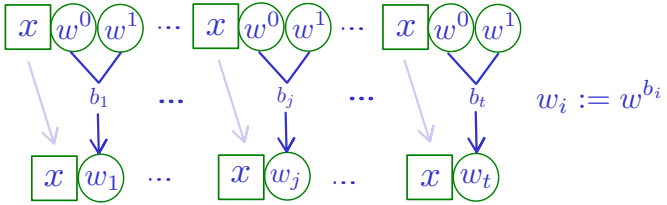
$(\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \diamond\!\!\!\!\diamond\, \pi^0) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \diamond\!\!\!\!\diamond\, \pi^1)$

CHALLENGE: DEALING WITH WORST-CASE WI

- FIX (x, w^0, w^1) AND CONSIDER PROVER $\mathsf{P}_{\{x\}}$ THAT DUMPS THE WITNESS OF x AS PART OF PROOF $\diamond\!\!\!\!\diamond\, \pi$

THERE EXISTS $\bar{D}$ THAT WORKS FOR $\mathsf{P}_{\{x\}}$

$B \xleftarrow{\$}$ UNIFORM DIST. OVER $\{0,1\}^t$



- $\mathsf{P}_{\{x^*\}}$ CANNOT REMEMBER WHICH WITNESS USED IN ALL LOCATIONS SINCE $\rho < 1$

HOW TO FIX $\bar{D}$?

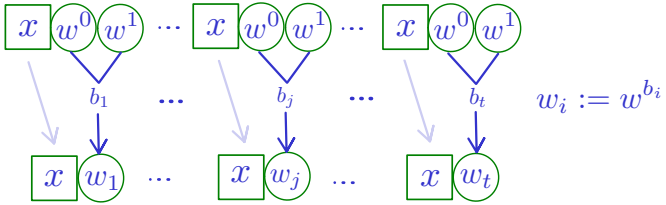
$\forall \mathsf{P} \exists \bar{D} \forall (x, w^0, w^1) : \mathrm{View}_{\mathsf{V}'}(x, w^0) \approx \mathrm{View}_{\mathsf{V}'}(x, w^1)$

$(\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \diamond\!\!\boxed{\pi^0}) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \diamond\!\!\boxed{\pi^1})$

- CHALLENGE: DEALING WITH WORST-CASE WI
  - FIX (x, w^0, w^1) AND CONSIDER PROVER $\mathsf{P}_{\{x\}}$ THAT DUMPS THE WITNESS OF x AS PART OF PROOF $\diamond\!\!\boxed{\pi}$

- THERE EXISTS $\bar{D}$ THAT WORKS FOR $\mathsf{P}_{\{x\}}$

$B \xleftarrow{\$}$ UNIFORM DIST. OVER $\{0,1\}^t$



- $\mathsf{P}_{\{x^*\}}$ CANNOT REMEMBER WHICH WITNESS USED IN ALL LOCATIONS SINCE $\rho < 1$

» HOW TO FIX $\bar{D}$ FOR GENERAL P? «

HOW TO FIX $\bar{D}$?...

[D15,D16]

1)COMPRESSION LEMMA OF DRUCKER/DELL

HOW TO FIX $\bar{D}$?...

[D15,D16]

1)COMPRESSION LEMMA OF DRUCKER/DELL

$$\forall g : \{0,1\}^t \to \{0,1\}^{\rho t} : (j, g(B|_{j\leftarrow 0}) \approx_{\sqrt{\rho}} (j, g(B|_{j\leftarrow 1})$$

UNIFORM OVER $[t]$ UNIFORM OVER $\{0,1\}^t$

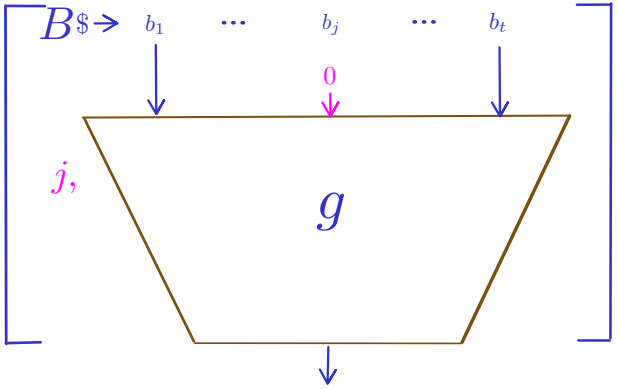
HOW TO FIX $\bar{D}$?...

[D15,D16]

1)COMPRESSION LEMMA OF DRUCKER/DELL

$$\forall g : \{0,1\}^t \to \{0,1\}^{\rho t} : (j, g(B|_{j\leftarrow 0}) \approx_{\sqrt{\rho}} (j, g(B|_{j\leftarrow 1})$$

UNIFORM OVER $[t]$ UNIFORM OVER $\{0,1\}^t$



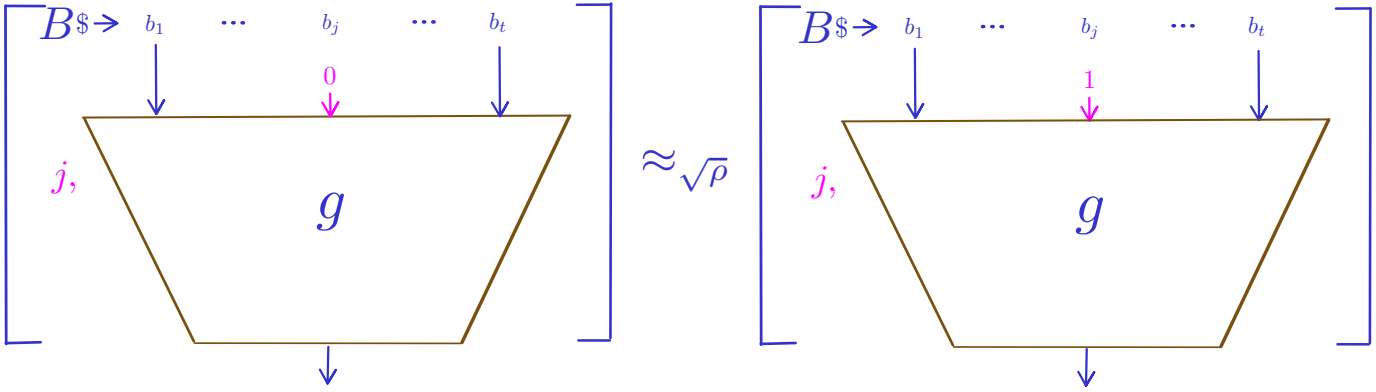
HOW TO FIX $\bar{D}$?...

[D15,D16]

1)COMPRESSION LEMMA OF DRUCKER/DELL

$$\forall g : \{0,1\}^t \to \{0,1\}^{\rho t} : (j, g(B|_{j\leftarrow 0}) \approx_{\sqrt{\rho}} (j, g(B|_{j\leftarrow 1})$$

UNIFORM OVER $[t]$ UNIFORM OVER $\{0,1\}^t$

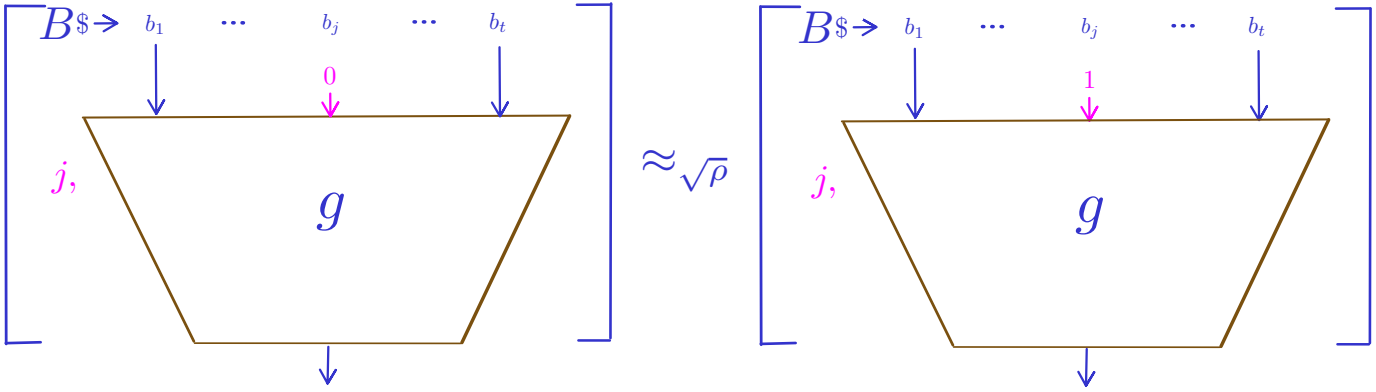


HOW TO FIX $\bar{D}$?...

[D15,D16]

1)COMPRESSION LEMMA OF DRUCKER/DELL IMPLIES WI FOR FIXED (x, w_0, w_1)

$$\forall \mathsf{P} \forall (x, w^0, w^1) \exists \bar{D} : (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^0) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^1)$$

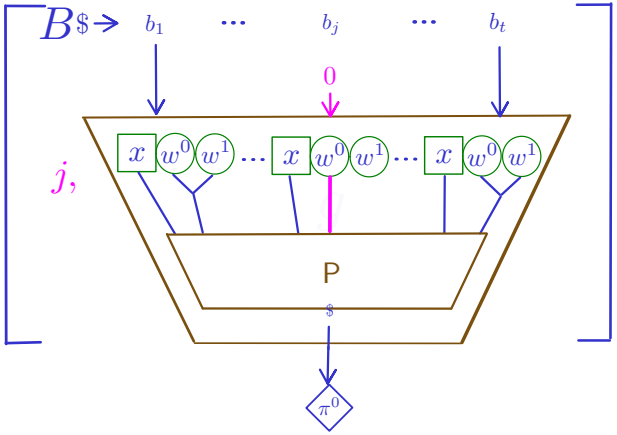


HOW TO FIX $\bar{D}$?...

[D15,D16]

1)COMPRESSION LEMMA OF DRUCKER/DELL IMPLIES WI FOR FIXED (x, w_0, w_1)

$$\forall \mathsf{P} \forall (x, w^0, w^1) \exists \bar{D} : (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \diamondsuit^0) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \diamondsuit^1)$$

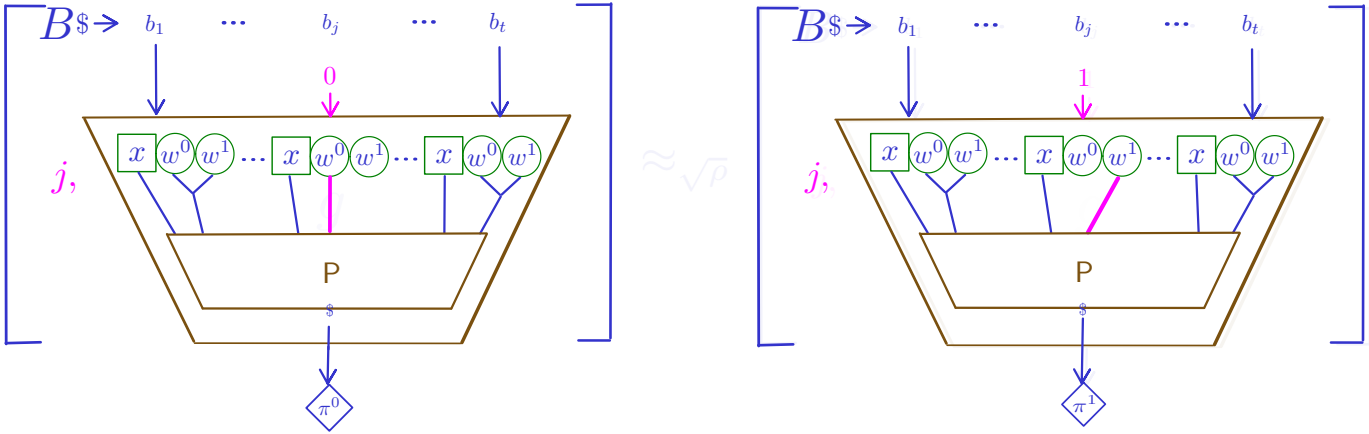


HOW TO FIX $\bar{D}$?...

[D15,D16]

1)COMPRESSION LEMMA OF DRUCKER/DELL IMPLIES WI FOR FIXED (x, w_0, w_1)

$$\forall \mathsf{P} \forall (x, w^0, w^1) \exists \bar{D} : (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^0) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^1)$$

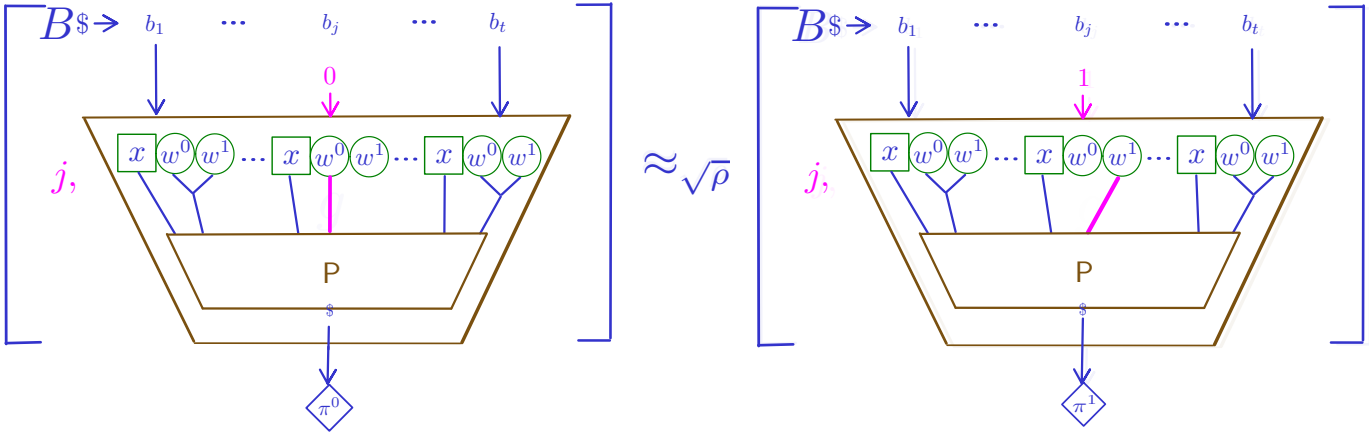


HOW TO FIX $\bar{D}$?...

[D15,D16]

1)COMPRESSION LEMMA OF DRUCKER/DELL IMPLIES WI FOR FIXED (x, w_0, w_1)

$$\forall \mathsf{P} \forall (x, w^0, w^1) \exists \bar{D} : (x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$$



HOW TO FIX $\bar{D}$?...

1*)COMPRESSION LEMMA OF DRUCKER/DELL IMPLIES "DISTRIBUTIONAL WI"

$$\forall \mathsf{P} \forall D \exists \bar{D} : \left(\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \langle \pi^0 \rangle\right) \approx \left(\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \langle \pi^1 \rangle\right)$$

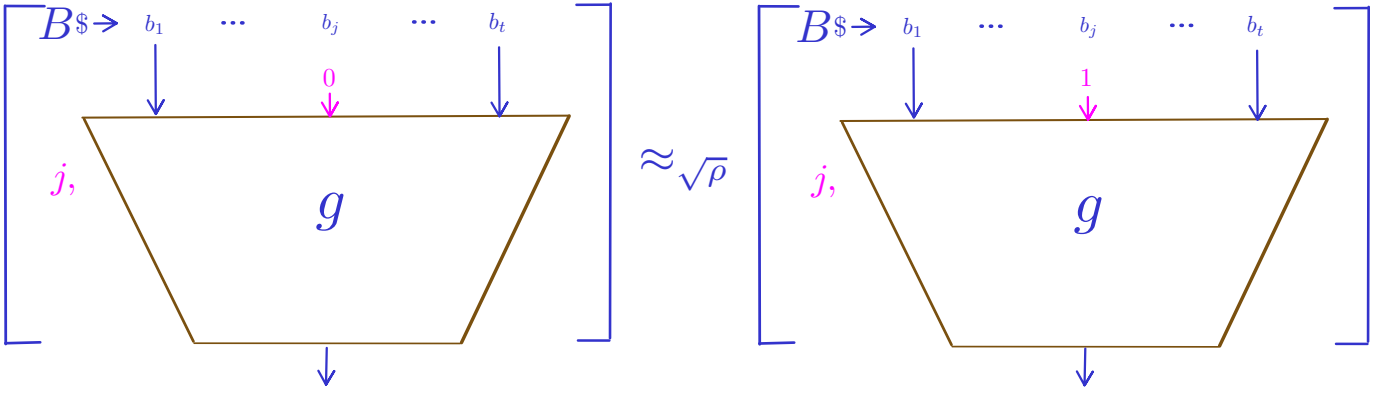
EFFICIENTLY-SAMPLEABLE
DISTRIBUTION OVER (x, w^0, w^1)

HOW TO FIX $\bar{D}$?...

1*)COMPRESSION LEMMA OF DRUCKER/DELL IMPLIES "DISTRIBUTIONAL WI"

$$\forall \mathrm{P} \forall D \exists \bar{D} : \left(\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^0\right) \approx \left(\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^1\right)$$

EFFICIENTLY-SAMPLEABLE
DISTRIBUTION OVER (x, w^0, w^1)

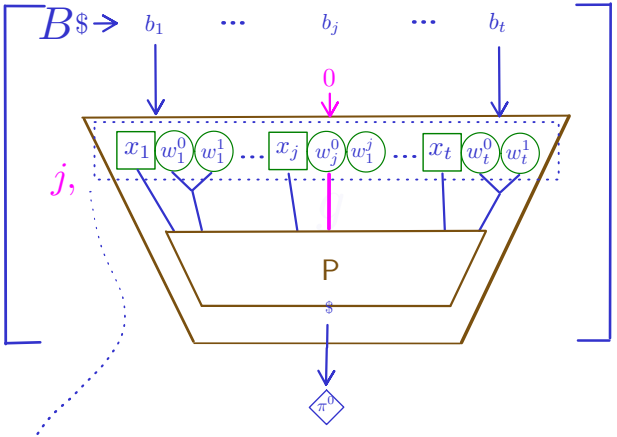


HOW TO FIX $\bar{D}$?...

1*)COMPRESSION LEMMA OF DRUCKER/DELL IMPLIES "DISTRIBUTIONAL WI"

$$\forall \mathrm{P} \forall D \exists \bar{D} : \left(\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \diamond^{\pi^0}\right) \approx \left(\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \diamond^{\pi^1}\right)$$

EFFICIENTLY-SAMPLEABLE DISTRIBUTION OVER (x, w^0, w^1)



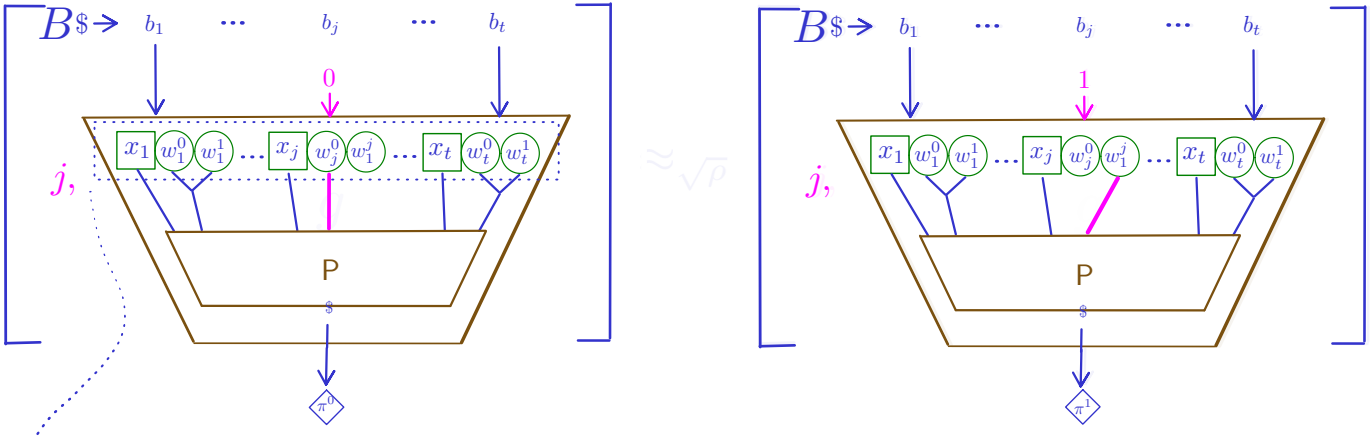
$\approx_{\sqrt{P}}$

HOW TO FIX $\bar{D}$?...

1*)COMPRESSION LEMMA OF DRUCKER/DELL IMPLIES "DISTRIBUTIONAL WI"

$$\forall P \forall D \exists \bar{D} : (x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$$

EFFICIENTLY-SAMPLEABLE
DISTRIBUTION OVER (x, w^0, w^1)

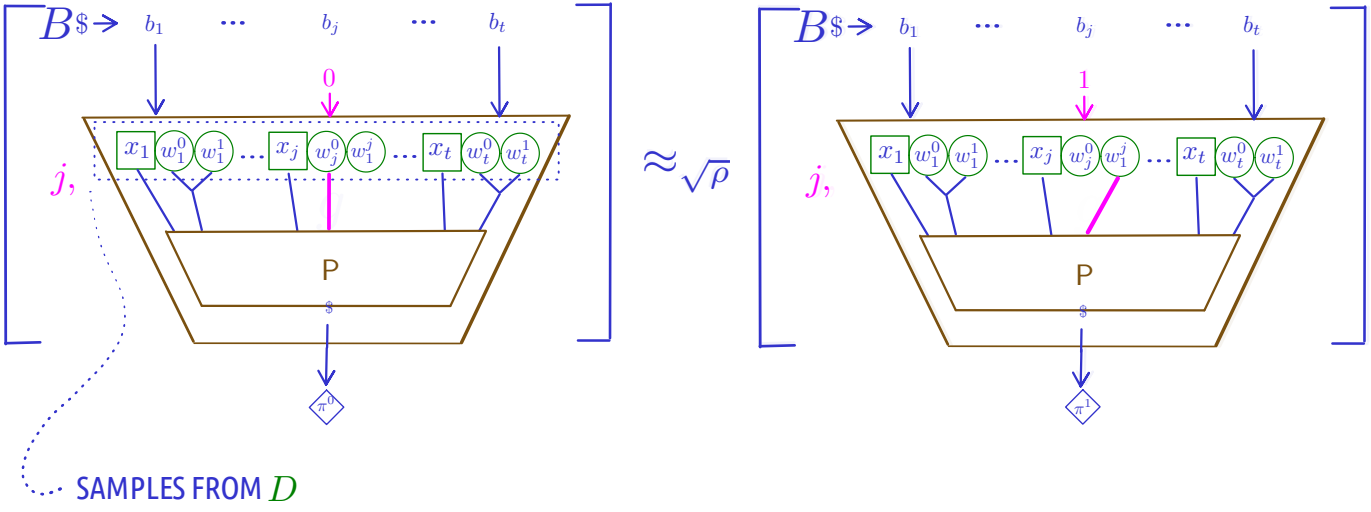


HOW TO FIX $\bar{D}$?...

1*)COMPRESSION LEMMA OF DRUCKER/DELL IMPLIES "DISTRIBUTIONAL WI"

$$\forall \mathrm{P} \forall D \exists \bar{D} : \left(\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \diamondsuit^{\pi^0}\right) \approx \left(\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \diamondsuit^{\pi^1}\right)$$

EFFICIENTLY-SAMPLEABLE
DISTRIBUTION OVER (x, w^0, w^1)



HOW TO FIX $\bar{D}$?...

2)DISTRIBUTIONAL WI TO (WORST-CASE) WI

$\forall \mathsf{P} \forall D \exists \bar{D} : (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^0) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^1)$

$\forall \mathsf{P} \exists \bar{D} \forall D : (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^0) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^1)$

HOW TO FIX $\bar{D}$?...

2) DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]

$\forall \mathsf{P} \forall D \exists \bar{D} : (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \langle \pi^0 \rangle) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \langle \pi^1 \rangle)$

$\forall \mathsf{P} \exists \bar{D} \forall D : (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \langle \pi^0 \rangle) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \langle \pi^1 \rangle)$

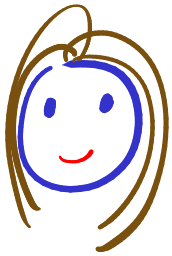
HOW TO FIX $\bar{D}$?...

2)DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]

ZERO-SUM GAME

ROW PLAYER

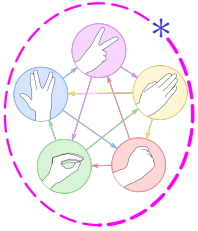
COLUMN PLAYER



HOW TO FIX $\bar{D}$?...

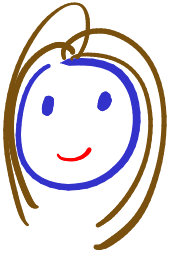
2)DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]

ZERO-SUM GAME



ROW PLAYER

COLUMN PLAYER

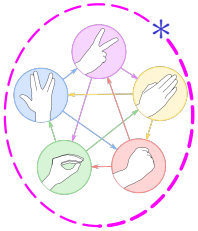


∗ IMAGE: NOJHAN, WIKIPEDIA

HOW TO FIX $\bar{D}$?...

2)DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]

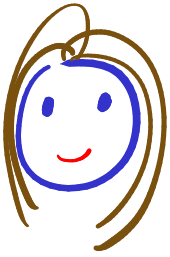
ZERO-SUM GAME



ROW PLAYER

R

COLUMN PLAYER

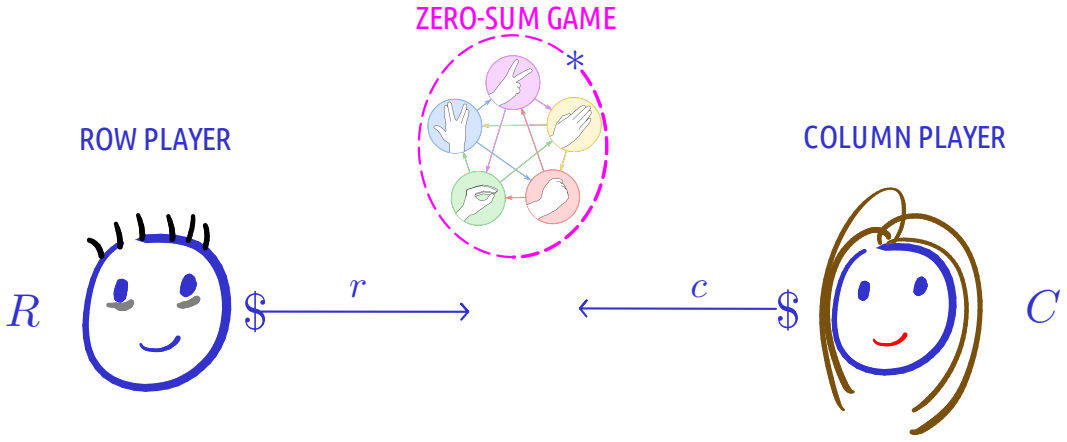


C

∗ IMAGE: NOJHAN, WIKIPEDIA

HOW TO FIX $\bar{D}$?...

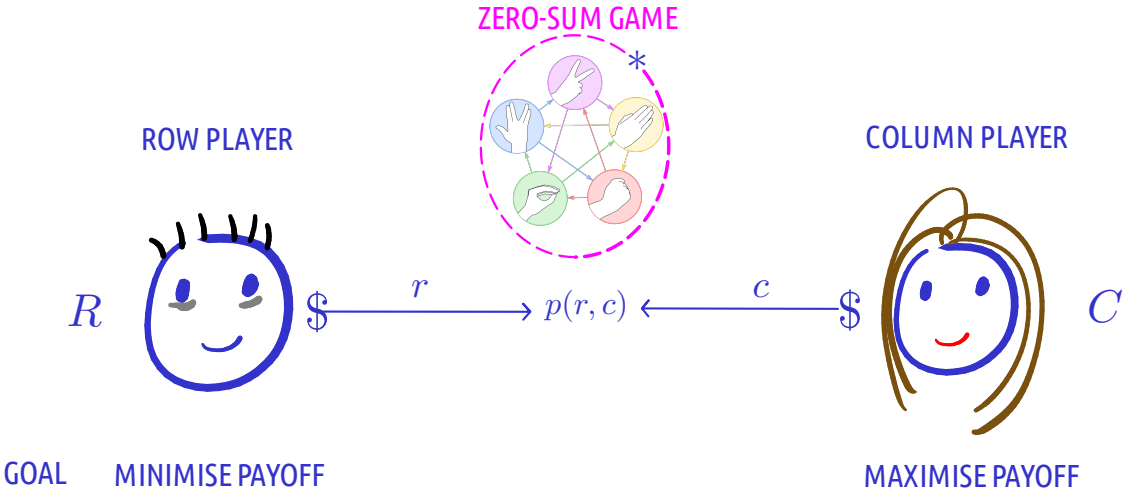
2)DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]



∗ IMAGE: NOJHAN, WIKIPEDIA

HOW TO FIX $\bar{D}$?...

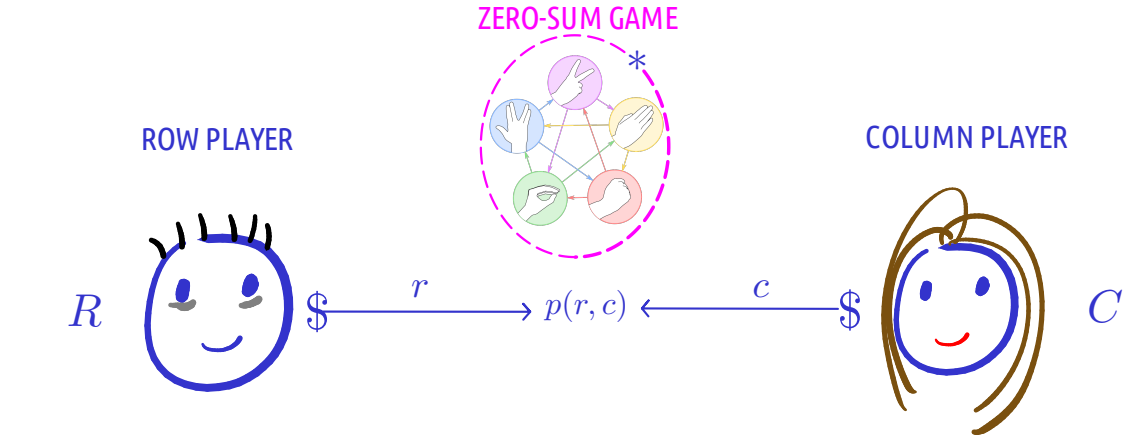
2)DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]



∗ IMAGE: NOJHAN, WIKIPEDIA

HOW TO FIX $\bar{D}$?...

2)DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]



$$\min_{\rho}\max_{\chi}\mathbb{E}_{r\leftarrow\rho,c\leftarrow\chi}[p(r,c)]=\max_{\chi}\min_{\rho}\mathbb{E}_{r\leftarrow\rho,c\leftarrow\chi}[p(r,c)]$$

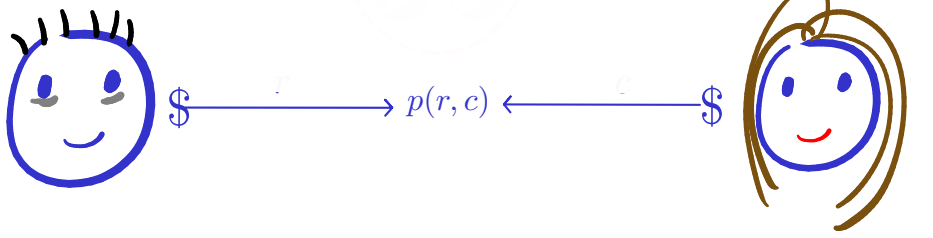
∗ IMAGE: NOJHAN, WIKIPEDIA

HOW TO FIX $\bar{D}$?...

2)DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]

$\forall \mathsf{P} \forall D \exists \bar{D} : (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^0) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^1)$

ZERO-SUM GAME



GOAL MINIMISE PAYOFF MAXIMISE PAYOFF

$$\min_{\rho} \max_{\chi} \mathbb{E}_{r \leftarrow \rho, c \leftarrow \chi}[p(r,c)] = \max_{\chi} \min_{\rho} \mathbb{E}_{r \leftarrow \rho, c \leftarrow \chi}[p(r,c)]$$

$\forall \mathsf{P} \exists \bar{D} \forall D : (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^0) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^1)$

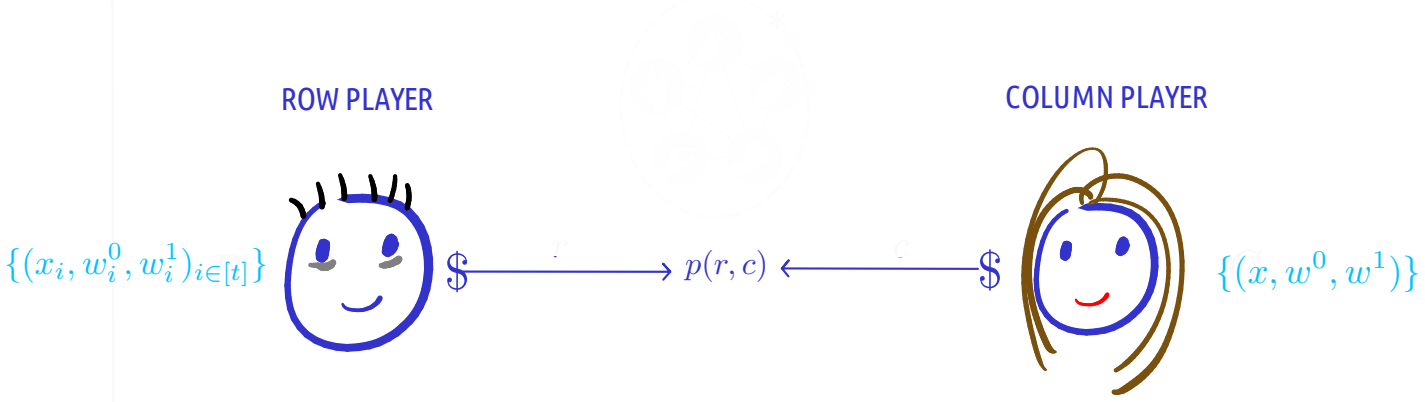
* IMAGE: NOJHAN, WIKIPEDIA

HOW TO FIX $\bar{D}$?...

2)DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]

$$\forall P \forall D \exists \bar{D} : (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^0) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^1)$$

ZERO-SUM GAME



$$\min_{\rho} \max_{\chi} \mathbb{E}_{r\leftarrow\rho, c\leftarrow\chi}[p(r,c)] = \max_{\chi} \min_{\rho} \mathbb{E}_{r\leftarrow\rho, c\leftarrow\chi}[p(r,c)]$$

$$\forall P \exists \bar{D} \forall D : (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^0) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^1)$$

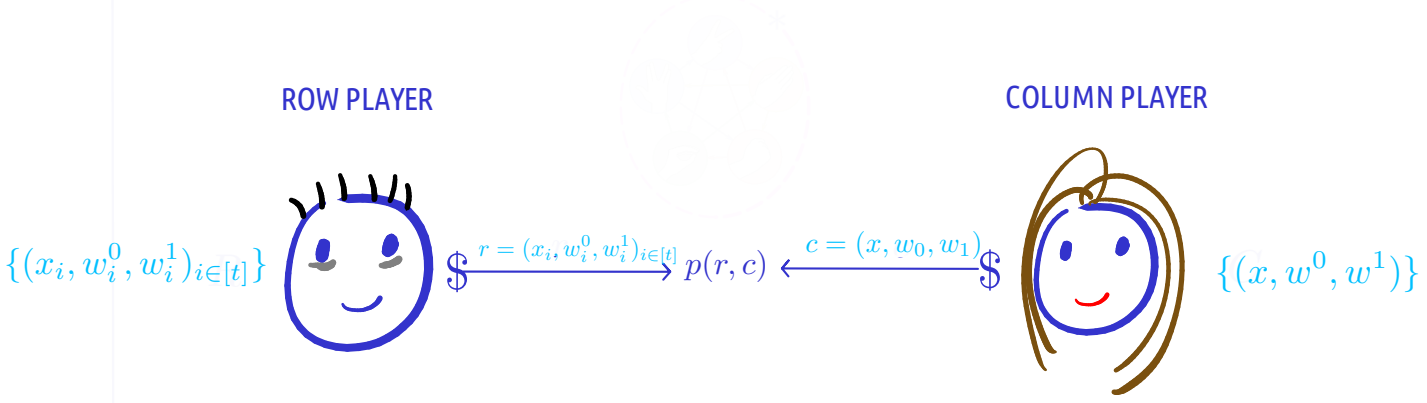
* IMAGE: NOJHAN, WIKIPEDIA

HOW TO FIX $\bar{D}$?...

2)DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]

$$\forall P \forall D \exists \bar{D} : (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^0) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^1)$$

ZERO-SUM GAME



$$\min_{\rho} \max_{\chi} \mathbb{E}_{r\leftarrow\rho, c\leftarrow\chi}[p(r,c)] = \max_{\chi} \min_{\rho} \mathbb{E}_{r\leftarrow\rho, c\leftarrow\chi}[p(r,c)]$$

$$\forall P \exists \bar{D} \forall D : (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^0) \approx (\boxed{x_1}, \cdots, \boxed{x_j}, \ldots, \boxed{x_t}, j, \pi^1)$$

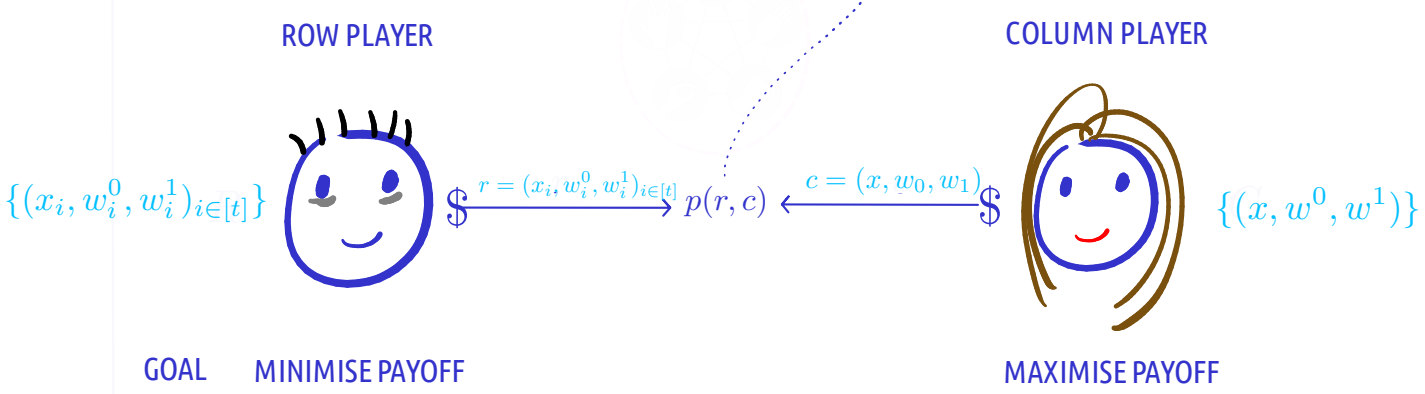
* IMAGE: NOJHAN, WIKIPEDIA

HOW TO FIX $\bar{D}$?...

2)DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]

$$\forall P \forall D \exists \bar{D} : (x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$$

ZERO-SUM GAME



$$\min_{\rho} \max_{\chi} \mathbb{E}_{r\leftarrow\rho, c\leftarrow\chi}[p(r,c)] = \max_{\chi} \min_{\rho} \mathbb{E}_{r\leftarrow\rho, c\leftarrow\chi}[p(r,c)]$$

$$\forall P \exists \bar{D} \forall D : (x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$$

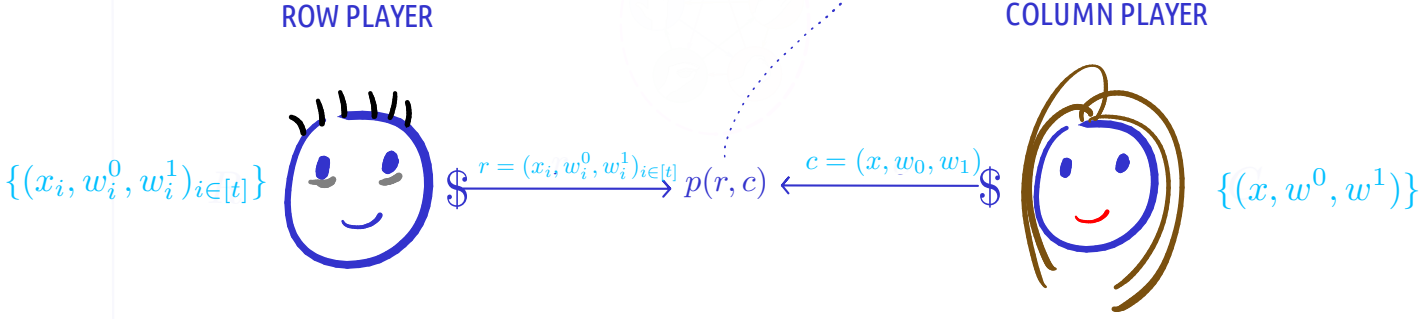
* IMAGE: NOJHAN, WIKIPEDIA

HOW TO FIX $\bar{D}$?...

2)DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]

$$\forall P \forall D \exists \bar{D} : (x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$$

ZERO-SUM GAME



$$\min_{\rho} \max_{\chi} \mathbb{E}_{r\leftarrow\rho, c\leftarrow\chi}[p(r,c)] = \max_{\chi} \min_{\rho} \mathbb{E}_{r\leftarrow\rho, c\leftarrow\chi}[p(r,c)]$$

$$\forall P \exists \bar{D} \forall D : (x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$$

* IMAGE: NOJHAN, WIKIPEDIA

HOW TO FIX $\bar{D}$?...

2)DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]

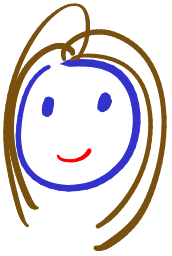
$$\forall P \forall D \exists \bar{D} : (x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$$

ZERO-SUM GAME

ROW PLAYER

COLUMN PLAYER

$\{(x_i, w_i^0, w_i^1)_{i\in[t]}\}$ $\$$ $\xrightarrow{r=(x_i,w_i^0,w_i^1)_{i\in[t]}}$ $p(r,c)$ $\xleftarrow{c=(x,w_0,w_1)}$ $\$$ $\{(x, w^0, w^1)\}$



GOAL MINIMISE PAYOFF

MAXIMISE PAYOFF

$$\min_{\bar{D}} \max_{D} \mathbb{E}_{r\leftarrow\bar{D},c\leftarrow D}[p(r,c)]$$

$$\forall P \exists \bar{D} \forall D : (x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$$

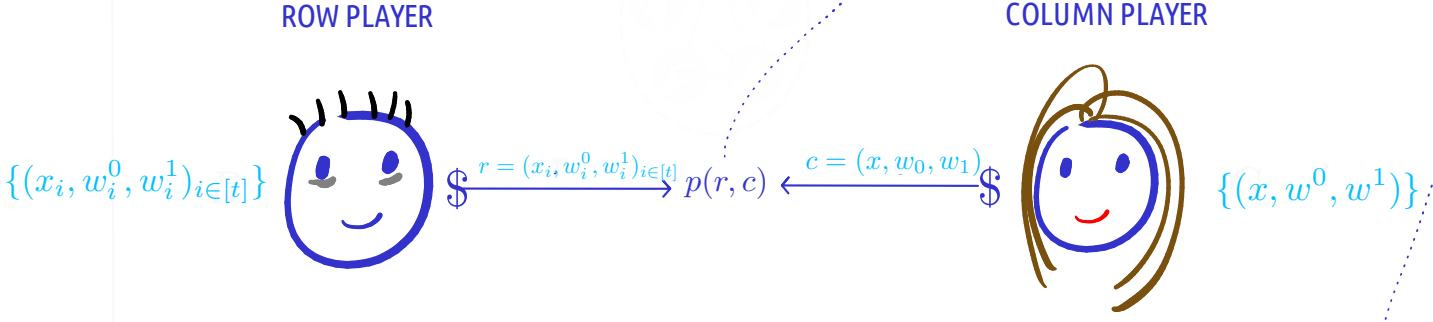
* IMAGE: NOJHAN, WIKIPEDIA

HOW TO FIX $\bar{D}$?...

2)DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]

$$\forall P \forall D \exists \bar{D} : (x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$$

ZERO-SUM GAME



$$\min_{\bar{D}} \max_{D} \mathbb{E}_{r\leftarrow\bar{D}, c\leftarrow D}[p(r,c)] = \max_{D} \min_{\bar{D}} \mathbb{E}_{r\leftarrow\bar{D}, c\leftarrow D}[p(r,c)] \approx \sqrt{\rho}$$

$$\forall P \exists \bar{D} \forall D : (x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$$

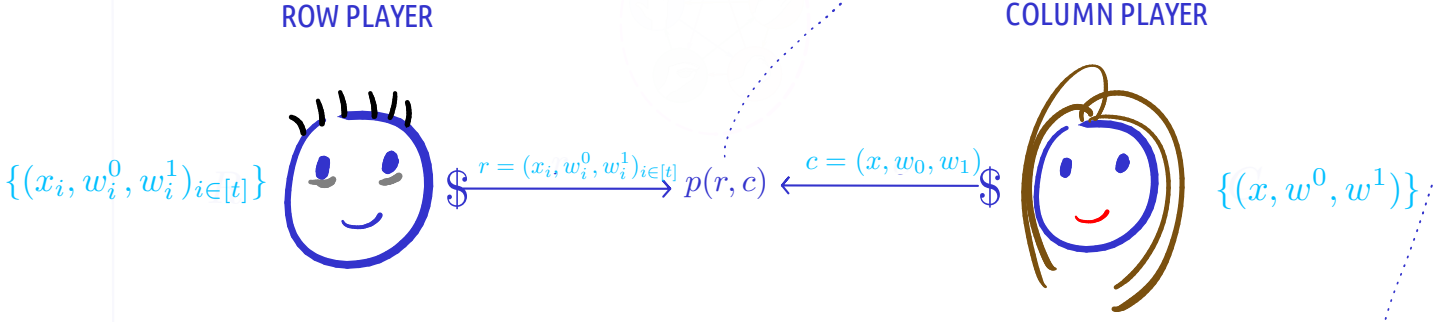
* IMAGE: NOJHAN, WIKIPEDIA

HOW TO FIX $\bar{D}$?...

2)DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]

$$\forall P \forall D \exists \bar{D} : (x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$$

ZERO-SUM GAME



$$\min_{\bar{D}} \max_{D} \mathbb{E}_{r\leftarrow\bar{D}, c\leftarrow D}[p(r,c)] = \max_{D} \min_{\bar{D}} \mathbb{E}_{r\leftarrow\bar{D}, c\leftarrow D}[p(r,c)] \approx \sqrt{\rho}$$

$$\forall P \exists \bar{D} \forall D : (x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$$

* IMAGE: NOJHAN, WIKIPEDIA

HOW TO FIX $\bar{D}$?...

SPARSE VERSION OF [LY94]

2)DISTRIBUTIONAL WI TO (WORST-CASE) WI VIA MINIMAX THEOREM [vN28]

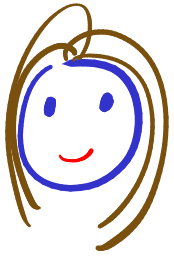
$$\forall \mathsf{P} \forall D \exists \bar{D} : (x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$$

ZERO-SUM GAME

ROW PLAYER

COLUMN PLAYER

$\{(x_i, w_i^0, w_i^1)_{i\in[t]}\}$ $\$ \xrightarrow{r=(x_i,w_i^0,w_i^1)_{i\in[t]}} p(r,c) \xleftarrow{c=(x,w_0,w_1)} \$$ $\{(x, w^0, w^1)\}$



GOAL MINIMISE PAYOFF

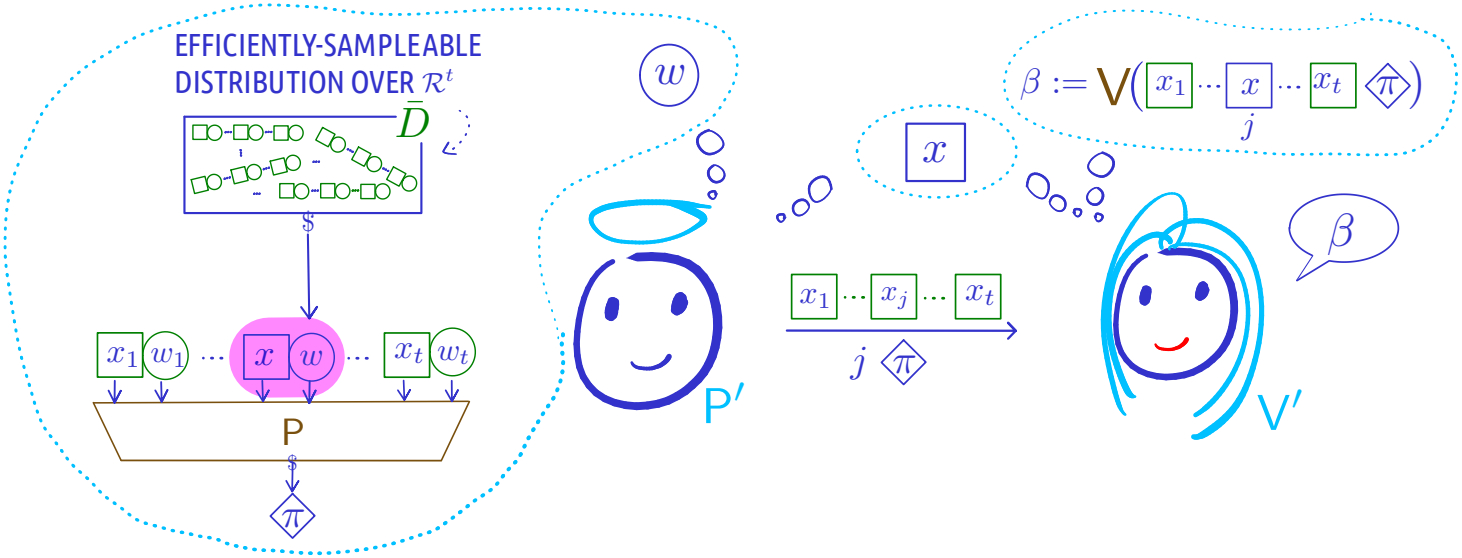
MAXIMISE PAYOFF

$$\min_{\bar{D}} \max_{D} \mathbb{E}_{r\leftarrow\bar{D},c\leftarrow D}[p(r,c)] = \max_{D} \min_{\bar{D}} \mathbb{E}_{r\leftarrow\bar{D},c\leftarrow D}[p(r,c)] \approx \sqrt{\rho}$$

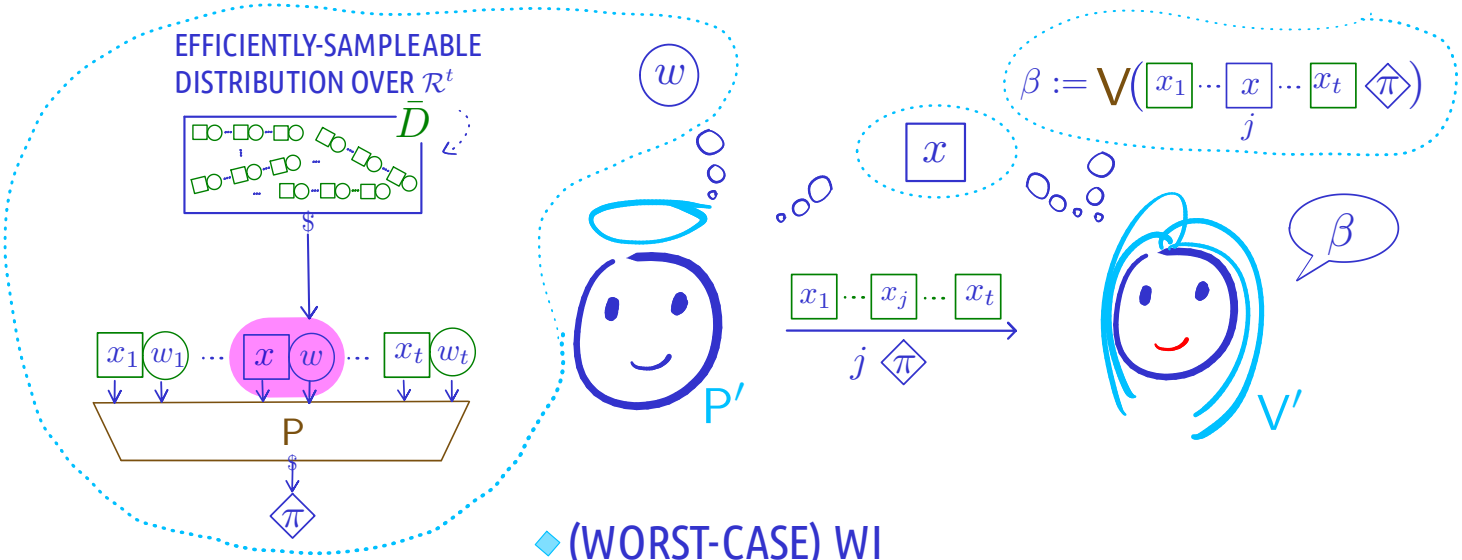
$$\forall \mathsf{P} \exists \bar{D} \forall D : (x_1, \cdots, x_j, \ldots, x_t, j, \pi^0) \approx (x_1, \cdots, x_j, \ldots, x_t, j, \pi^1)$$

* IMAGE: NOJHAN, WIKIPEDIA

TO RECAP


EFFICIENTLY-SAMPLEABLE
DISTRIBUTION OVER $\mathcal{R}^t$
$\bar{D}$
x_1 w_1 ⋯ x w ⋯ x_t w_t
P
π
w
P′
x
x_1 ⋯ x_j ⋯ x_t
j π
$\beta := \mathsf{V}(x_1 \cdots \underset{j}{x} \cdots x_t\ \pi)$
β
V′

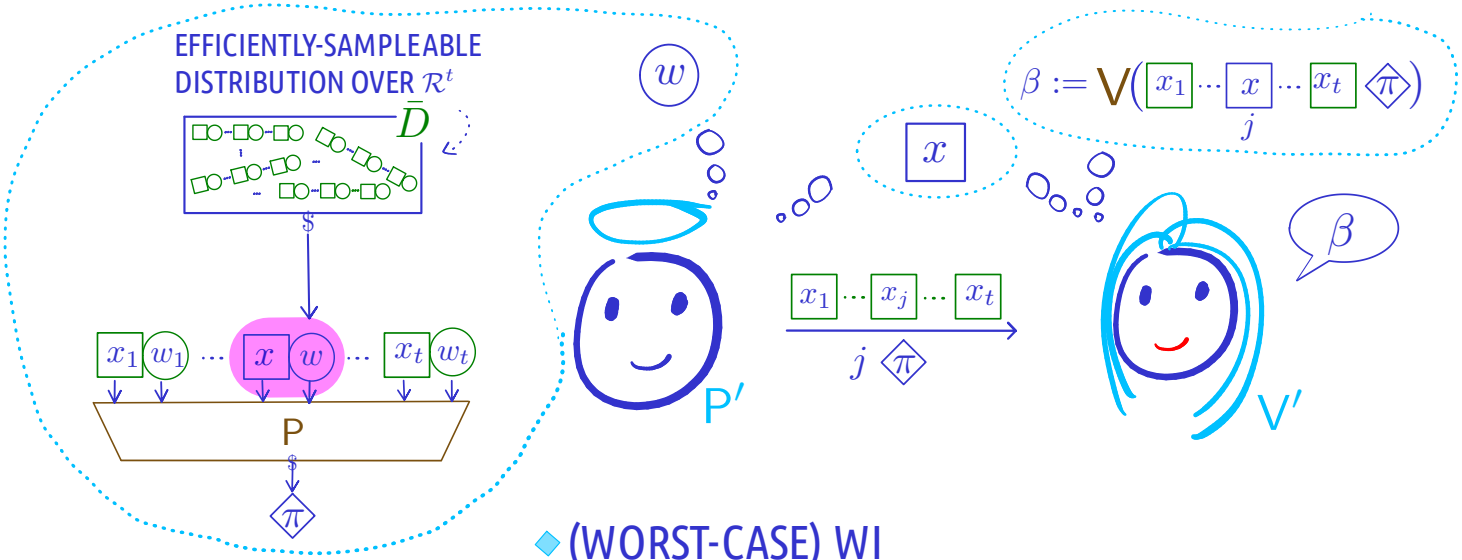
TO RECAP



- (WORST-CASE) WI

$\forall \mathsf{P} \exists \bar{D} \forall D$: Views indistinguishable

TO RECAP



◆ (WORST-CASE) WI

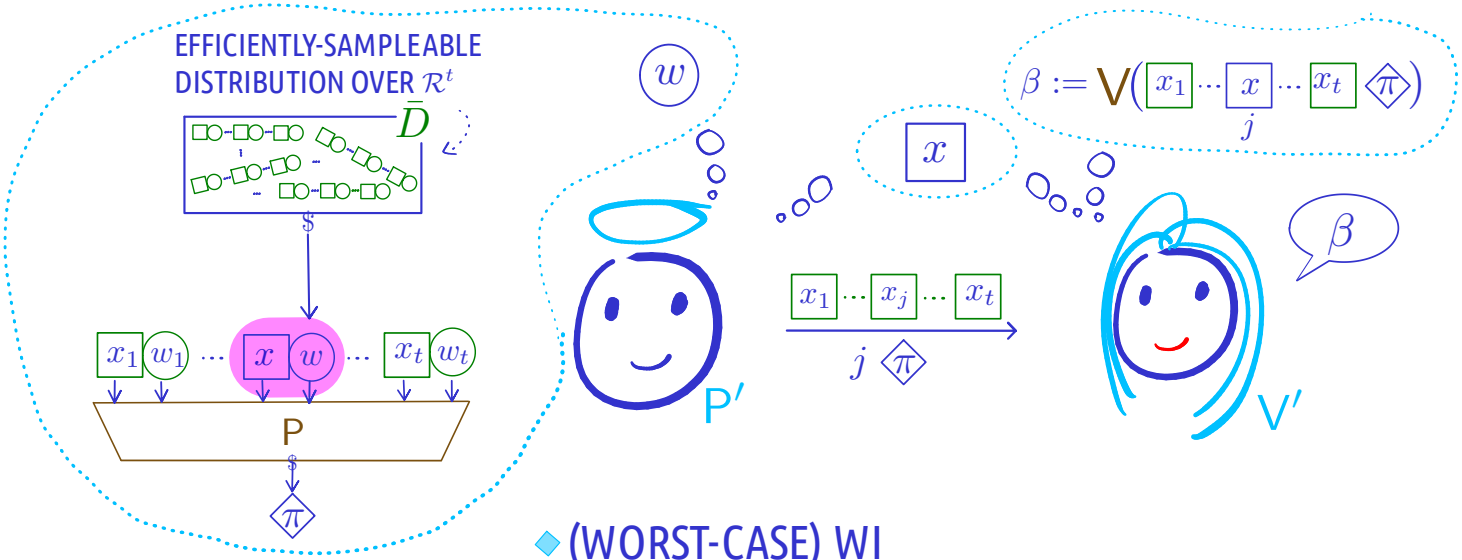
$\forall \mathsf{P} \exists \bar{D} \forall D$: Views indistinguishable

↓

REDUCES TO DISTRIBUTIONAL WI VIA (SPARSE) MINIMAX THEOREM

$\forall \mathsf{P} \forall D \exists \bar{D}$: Views indistinguishable

TO RECAP



- (WORST-CASE) WI

$\forall \mathsf{P} \exists \bar{D} \forall D$: Views indistinguishable

↓

REDUCES TO DISTRIBUTIONAL WI VIA (SPARSE) MINIMAX THEOREM

$\forall \mathsf{P} \forall D \exists \bar{D}$: Views indistinguishable

↓

DISTRIBUTIONAL WI VIA COMPRESSION LEMMA OF DRUCKER/DELL

PLAN

- BACKGROUND
  - DEFINITIONS: BATCH PROOFS STAT. WITNESS INDISTINGUISHABILITY (SWI)
  - WHAT CAN BE BATCHED?
- MAIN RESULT
  - BATCH PROOFS $\Rightarrow$ SWI PROOFS
  - TECHNICAL OVERVIEW
- **MORE RESULTS**
  - ONE-WAY FUNCTION + BATCH ARGUMENTS $\Rightarrow$ SZK ARGUMENTS
  - NON-INTERACTIVE (NI) BATCH ARGUMENTS $\Rightarrow$ NI SZK ARGUMENTS
- OPEN QUESTIONS

BATCH ARGUMENTS $\Rightarrow$ SWI ARGUMENTS

INTERACTIVE SETTING

NON-INTERACTIVE (NI) SETTING (CRS MODEL)

BATCH ARGUMENTS $\Rightarrow$ SWI ARGUMENTS

INTERACTIVE SETTING

BATCH ARGUMENTS

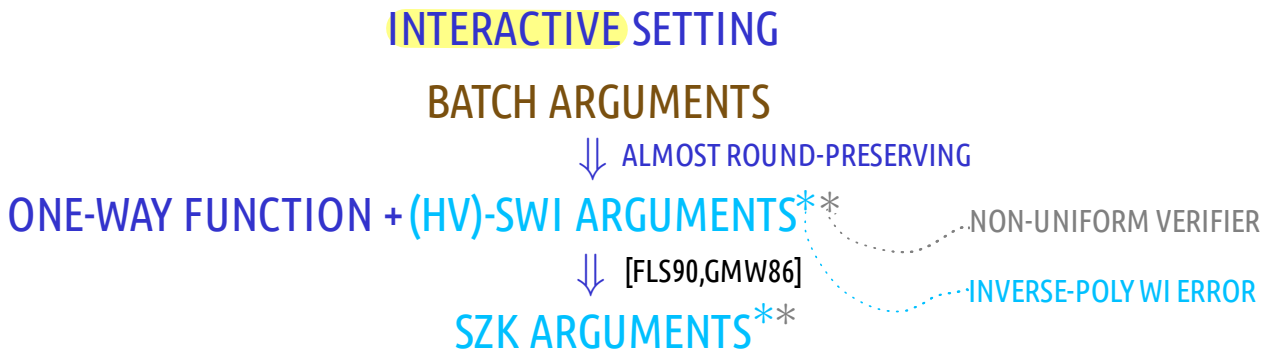
$\Downarrow$ ALMOST ROUND-PRESERVING

(HV)-SWI ARGUMENTS**

- NON-UNIFORM VERIFIER
- INVERSE-POLY WI ERROR

NON-INTERACTIVE (NI) SETTING (CRS MODEL)

BATCH ARGUMENTS $\Rightarrow$ SWI ARGUMENTS



BATCH ARGUMENTS $\Rightarrow$ SWI ARGUMENTS

INTERACTIVE SETTING

BATCH ARGUMENTS

$\Downarrow$ ALMOST ROUND-PRESERVING

ONE-WAY FUNCTION + (HV)-SWI ARGUMENTS** — NON-UNIFORM VERIFIER

$\Downarrow$ [FLS90,GMW86] — INVERSE-POLY WI ERROR

COLLISION RESISTANCE $\Rightarrow$ SZK ARGUMENTS**

NON-INTERACTIVE (NI) SETTING (CRS MODEL)

BATCH ARGUMENTS $\Rightarrow$ SWI ARGUMENTS

INTERACTIVE SETTING

BATCH ARGUMENTS

$\Downarrow$ ALMOST ROUND-PRESERVING

ONE-WAY FUNCTION + (HV)-SWI ARGUMENTS** — NON-UNIFORM VERIFIER

$\Downarrow$ [FLS90,GMW86] — INVERSE-POLY WI ERROR

COLLISION RESISTANCE $\Rightarrow$ SZK ARGUMENTS**

NON-INTERACTIVE (NI) SETTING (CRS MODEL)

(SOMEWHERE-EXTRACTABLE) NI BATCH ARGUMENTS

$\Downarrow$

NISWI ARGUMENTS**

BATCH ARGUMENTS $\Rightarrow$ SWI ARGUMENTS

INTERACTIVE SETTING

BATCH ARGUMENTS

$\Downarrow$ ALMOST ROUND-PRESERVING

ONE-WAY FUNCTION + (HV)-SWI ARGUMENTS** — NON-UNIFORM VERIFIER

$\Downarrow$ [FLS90,GMW86] — INVERSE-POLY WI ERROR

COLLISION RESISTANCE $\Rightarrow$ SZK ARGUMENTS**

NON-INTERACTIVE (NI) SETTING (CRS MODEL)

(SOMEWHERE-EXTRACTABLE) NI BATCH ARGUMENTS

$\Downarrow$

NISWI ARGUMENTS**

$\Downarrow$ [FLS90]

NISZK ARGUMENTS**

◆ BATCH ARGUMENTS ⇒ SWI ARGUMENTS

INTERACTIVE SETTING

BATCH ARGUMENTS

⇓ ALMOST ROUND-PRESERVING

ONE-WAY FUNCTION + (HV)-SWI ARGUMENTS** — NON-UNIFORM VERIFIER, INVERSE-POLY WI ERROR

⇓ [FLS90,GMW86]

COLLISION RESISTANCE ⇒ SZK ARGUMENTS**

NON-INTERACTIVE (NI) SETTING (CRS MODEL)

(SOMEWHERE-EXTRACTABLE) NI BATCH ARGUMENTS

⇓

NISWI ARGUMENTS**

⇓ [FLS90]

LOSSY PKE + NISZK ARGUMENTS**

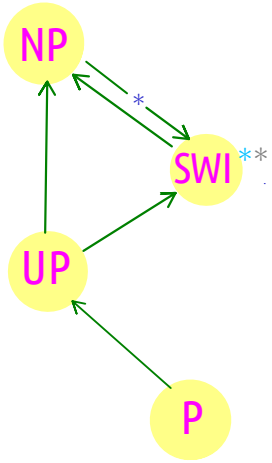
⇓ PRIVACY AMPLIFICATION [GJS19,LM20]

NISZK ARGUMENTS*

PLAN

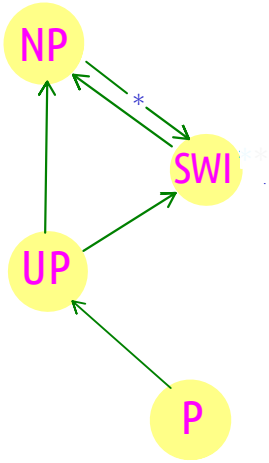
- BACKGROUND
  - DEFINITIONS: BATCH PROOFS STAT. WITNESS INDISTINGUISHABILITY (SWI)
  - WHAT CAN BE BATCHED?
- MAIN RESULT
  - BATCH PROOFS $\Rightarrow$ SWI PROOFS
  - TECHNICAL OVERVIEW
- MORE RESULTS
  - ONE-WAY FUNCTION + BATCH ARGUMENTS $\Rightarrow$ SZK ARGUMENTS
  - NON-INTERACTIVE (NI) BATCH ARGUMENTS $\Rightarrow$ NI SZK ARGUMENTS
- OPEN QUESTIONS

OPEN QUESTIONS



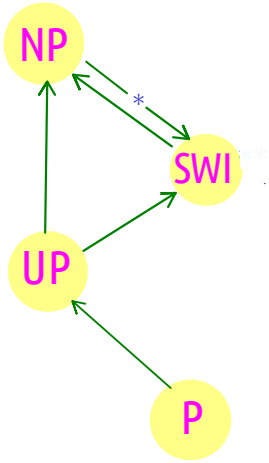
OPEN QUESTIONS

- BATCH PROOF FOR NP IMPLIES SWI PROOF FOR NP? (WITHOUT CAVEATS)
  - AMPLIFY SWI
  - UNIFORM MINIMAX?



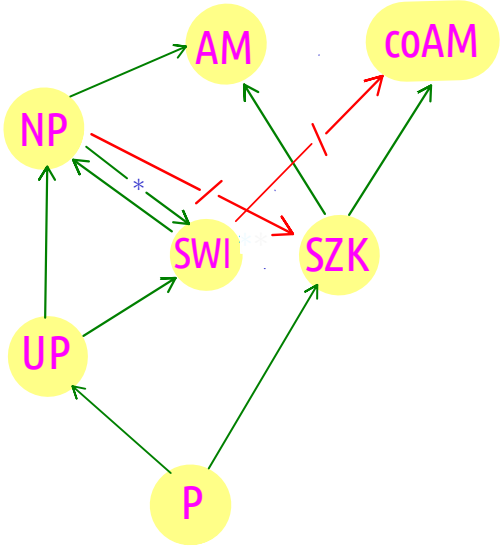
OPEN QUESTIONS

- BATCH PROOF FOR NP IMPLIES SWI PROOF FOR NP? (WITHOUT CAVEATS)
  - AMPLIFY SWI
  - UNIFORM MINIMAX?
- UNDERSTAND SWI AS A CLASS
  - DOES IT HAVE A COMPLETE PROBLEM?



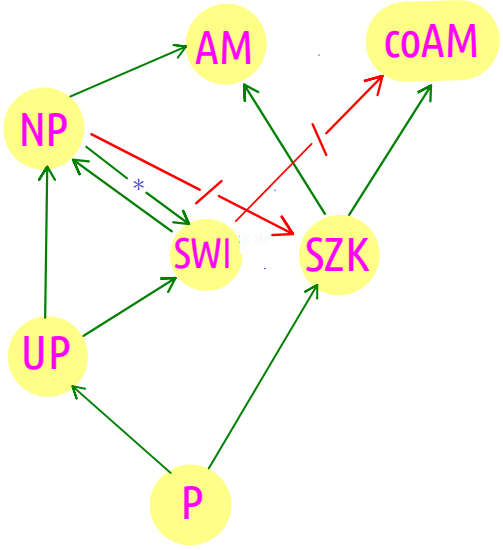
OPEN QUESTIONS

- BATCH PROOF FOR NP IMPLIES SWI PROOF FOR NP? (WITHOUT CAVEATS)
  - AMPLIFY SWI
  - UNIFORM MINIMAX?
- UNDERSTAND SWI AS A CLASS
  - DOES IT HAVE A COMPLETE PROBLEM?
  - RELATIONSHIP WITH SZK



OPEN QUESTIONS

- BATCH PROOF FOR NP IMPLIES SWI PROOF FOR NP? (WITHOUT CAVEATS)
  - AMPLIFY SWI
  - UNIFORM MINIMAX?
- UNDERSTAND SWI AS A CLASS
  - DOES IT HAVE A COMPLETE PROBLEM?
  - RELATIONSHIP WITH SZK



THANK YOU!

NATIONAL
RESEARCH
FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE

BIBLIOGRAPHY

[AH91] AIELLO & HÅSTAD, Statistical zero-knowledge languages can be recognized in two rounds, JCSS'91.

[CJJ22] CHOUDHURI, JAIN & JIN, SNARGs for P from LWE, FOCS'21

[D15] DRUCKER, New limits to classical and quantum instance compression, SICOMP'15

[D16] DELL, And-compression of NP-complete problems: Streamlined proof and minor observations, ALGORITHMICA'16

[F89] FORTNOW, The complexity of perfect zero-knowledge, ADV. COMP. RES.'89

[FLS90] FEIGE, LAPIDOT & SHAMIR, Multiple non-interactive zero knowledge proofs based on a single random string, FOCS'90

[GJS19] GOYAL, JAIN & SAHAI, Simultaneous amplification: The case of non-interactive zero-knowledge, Crypto'19

[GMW86] GOLDREICH, MICALI & WIGDERSON, Proofs that yield nothing but their validity and a methodology of cryptographic protocol design, FOCS'86

[GSV98] GOLDREICH, SAHAI & VADHAN, Honest-verifier statistical zero-knowledge equals general statistical zero-knowledge, STOC'98

[HJKS22] HULETT ET AL, SNARGs for P from sub-exponential DDH and QR, EC'22

[LM20] LANZENBERGER & MAURER, Coupling of random systems, TCC'20

[LY94] LIPTON & YOUNG, Simple strategies of zero-sum games with application to comlexity theory, STOC'94

[RR20] ROTHBLUM & ROTHBLUM, Batch verification and proofs of proximity with polylog overhead, TCC'20

[RRR18] REINGOLD, ROTHBLUM & ROTHBLUM, Constant-round interactive proofs for delegating computation, SICOMP' 2021

[vN28] von NEUMANN, Zur theorie der gesellschaftsspiele, MAT. ANN.'28

[WW22], WATERS & WU, Batch arguments for NP and more from standard bilinear group assumptions, Crypto'22