Quantum Interactive Proofs with Weak Error Bounds

Tsuyoshi Ito

Institute for Quantum Computing & School of Computer Science
University of Waterloo

Joint work with
Hirotada Kobayashi (National Institute of Informatics)
John Watrous (IQC & SCS, University of Waterloo)

A motivation for main result

QIP = PSPACE [Jain, Ji, Upadhyay, Watrous STOC’10]

A motivation for main result

QIP $\subseteq$ PSPACE [Jain, Ji, Upadhyay, Watrous STOC'10]

Proof requires the assumption of bounded error

This assumption is necessary
(unless PSPACE = EXP)

IP $\subseteq$ PSPACE [Feldman'86]

Holds even without error bounds

Why are these results so different?

Main result:
QIP with suitable weaker error bounds = EXP

Also: IP $\neq$ QIP without error bounds (unless PSPACE = EXP)

Outline

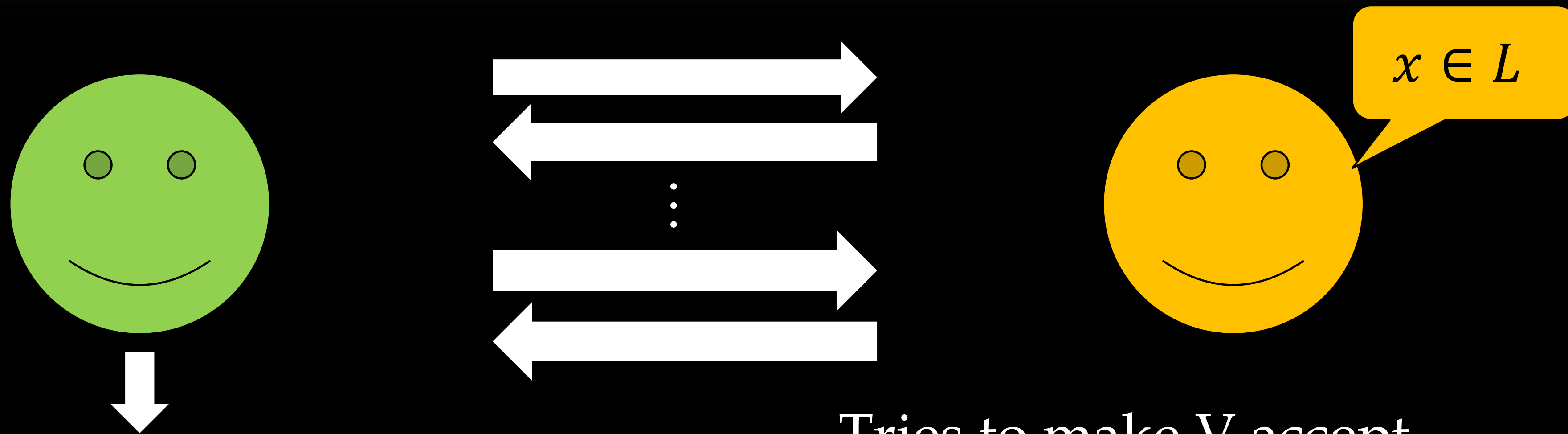
- Classical and quantum interactive proofs
- IP $\subseteq$ PSPACE vs. QIP $\subseteq$ PSPACE
- Main result: QIP with $2^{-2^{\text{poly}}}$ gap = EXP
- Proof technique:
  No-signaling 2-prover 1-round interactive proofs
- Other results
- Open problems

Interactive proofs

[Babai '85]
[Goldwasser, Micali, Rackoff '85]

Verifier
(Randomized poly-time)

Prover
(Computationally unbounded)



Accept (convinced)
Reject (unconvinced)

Tries to make V accept
with as high prob. as possible

V has to decide whether prover is honest or not
(with small error probability)

Interactive proofs

[Babai '85]
[Goldwasser, Micali, Rackoff '85]

Verifier's job:

- Completeness: $x \in L \Rightarrow \exists$P. V accepts with prob. $\geq a(|x|)$
- Soundness: $x \notin L \Rightarrow \forall$P. V accepts with prob. $\leq b(|x|)$

System has *bounded error* when $a(n) - b(n) \geq 1/\text{poly}$

IP: Class of languages L having a bounded-error IP system

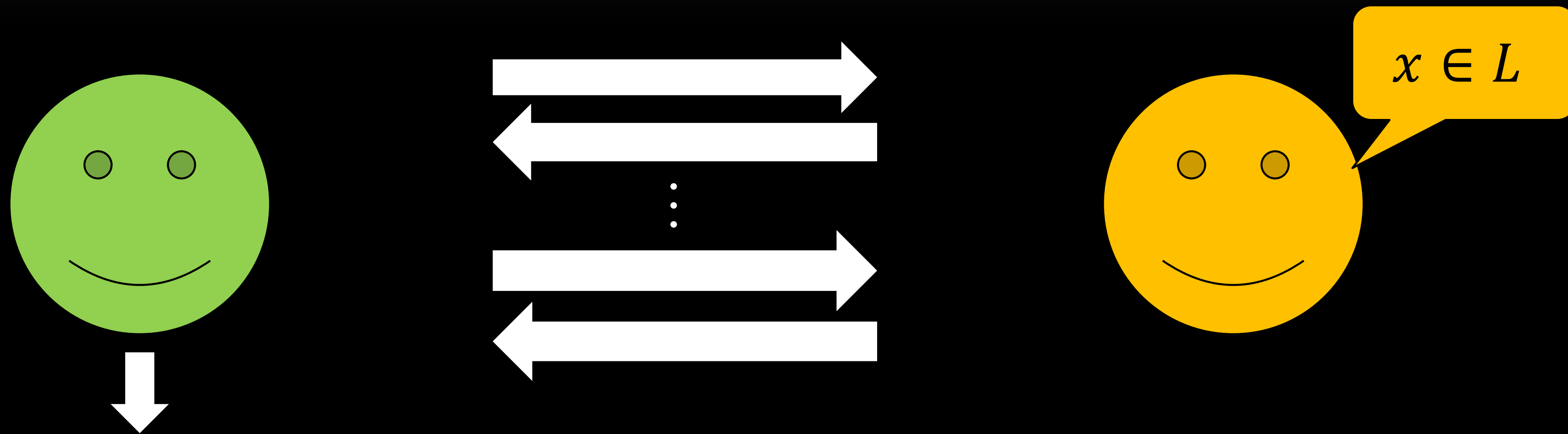
IP = PSPACE
[Lund, Fortnow, Karloff, Nisan FOCS'90; Shamir FOCS'90]

Interactive proofs

[Babai '85]
[Goldwasser, Micali, Rackoff '85]

Verifier
(Randomized poly-time)

Prover
(Computationally unbounded)



$\begin{cases} \text{Accept (convinced)} \\ \text{Reject (unconvinced)} \end{cases}$

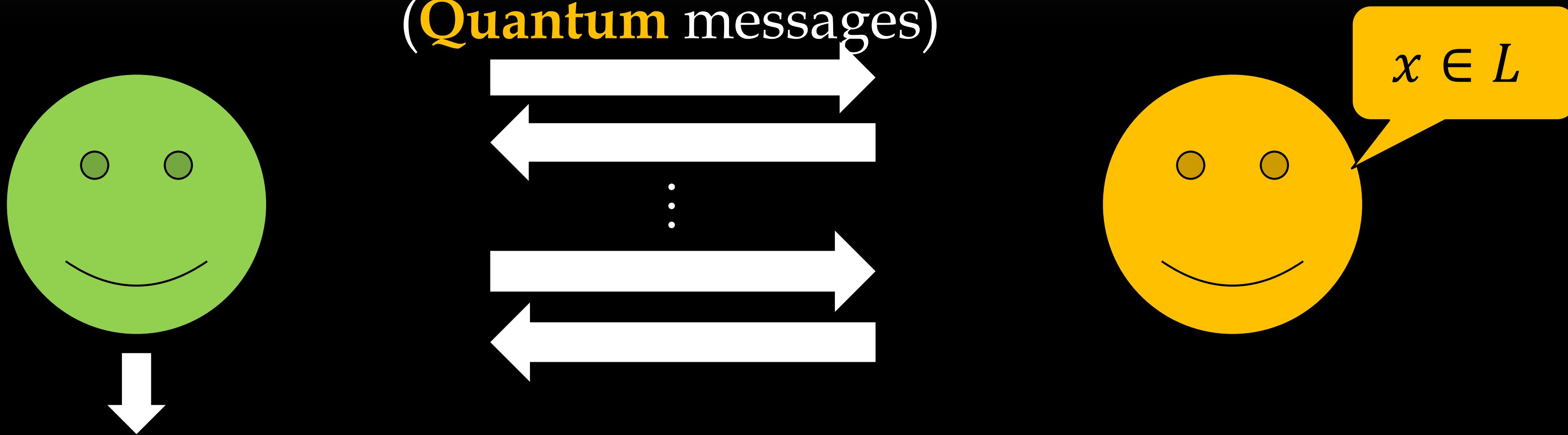
IP: Class of languages L having
a bounded-error IP system

Quantum interactive proofs [Watrous FOCS'99]

Verifier
(**Quantum** poly-time)

Prover
(Computationally unbounded)

(**Quantum** messages)



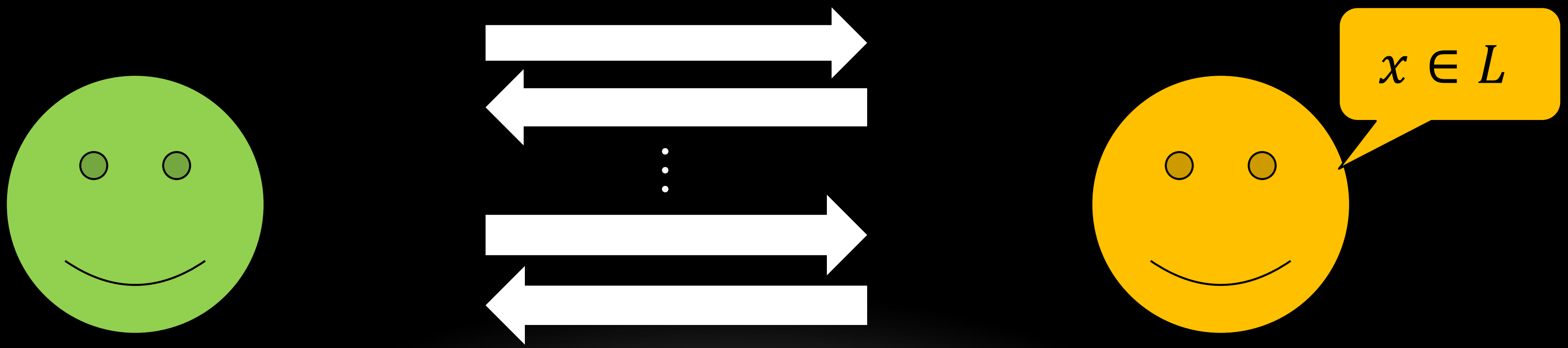
Accept (convinced)
Reject (unconvinced)

QIP: Class of languages L having
a bounded-error quantum IP system

Quantum interactive proofs

Very different from classical IP in some senses:

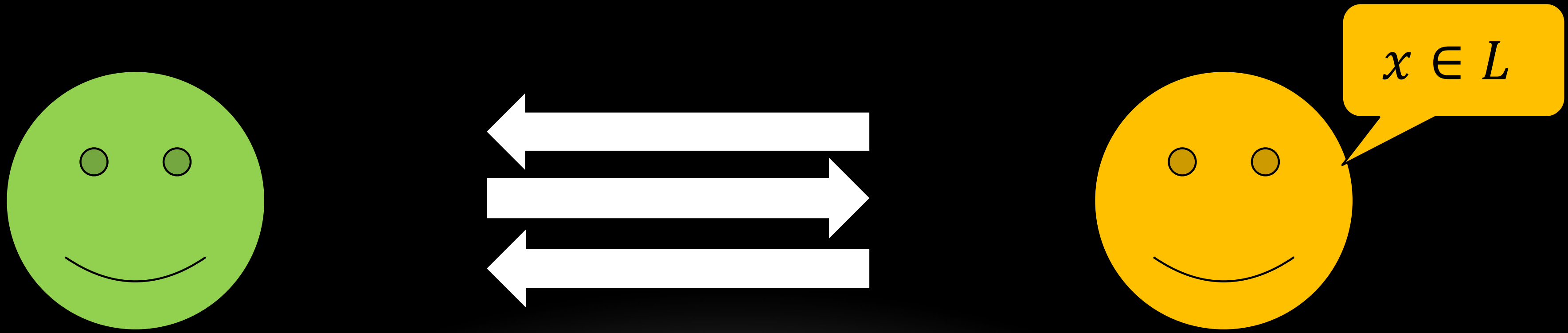
- Parallelizable to 3 messages [Kitaev, Watrous STOC'00]
- Verifier only has to send one bit which is coin flip [Marriott, Watrous CCC'04]



Quantum interactive proofs

Very different from classical IP in some senses:

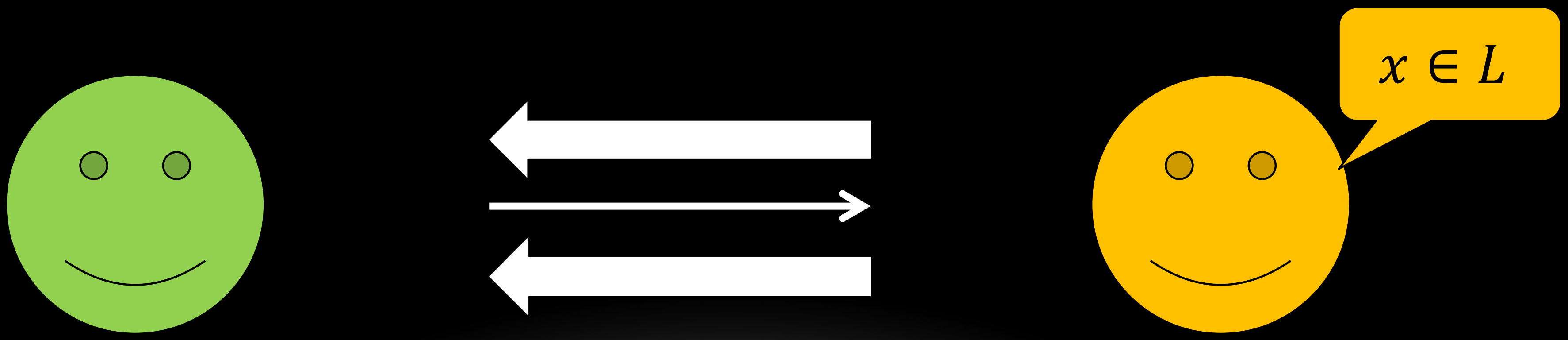
- Parallelizable to 3 messages [Kitaev, Watrous STOC'00]
- Verifier only has to send one bit which is coin flip [Marriott, Watrous CCC'04]



Quantum interactive proofs

Very different from classical IP in some senses:

- Parallelizable to 3 messages [Kitaev, Watrous STOC'00]
- Verifier only has to send one bit which is coin flip [Marriott, Watrous CCC'04]



Power of quantum interactive proofs

$$\text{PSPACE} \subseteq \text{IP} \subseteq \textbf{QIP} \subseteq \text{EXP}$$

[LFKN][Shamir] — Trivial — Semidefinite programming formulation [Kitaev, Watrous STOC'00]

[Jain, Ji, Upadhyay, Watrous STOC'10]:

$$\text{QIP} = \text{PSPACE}$$

Approximates the optimal prover by a fast parallel algorithm; heavily depends on *bounded-error* assumption

⇕

IP ⊆ PSPACE is easy: enumerate all possible responses for provers in poly-space and choose the best one

Main result

$$\text{QIP with } 2^{-2^{\text{poly}}} \text{ gap} = \text{EXP}$$

(with a standard gate set:
Toffoli, Hadamard, $\pi/2$-phase shift)

Consequences: Several new differences
between classical and quantum interactive proofs

- IP ≠ QIP in the unbounded-error setting*
- Bounded-error assumption in [JJUW10] is necessary*
- QIP systems can have $2^{-2^{\text{poly}}}$ gap, unlike IP systems

* Unless PSPACE = EXP

Easy direction: QIP with $2^{-2^{\mathrm{poly}}}$ gap ⊆ EXP

Immediate from a direct formulation of QIP systems by semidefinite programs [Gutoski, Watrous STOC'07]

QIP system

→ Semidefinite program of exponential size

→ Solve it to double-exp precision by standard algorithms for SDP

(This only uses a very special case of [GW07]:
[GW07] implies quantum refereed games with $2^{-2^{\mathrm{poly}}}$ gap are still ⊆ EXP)

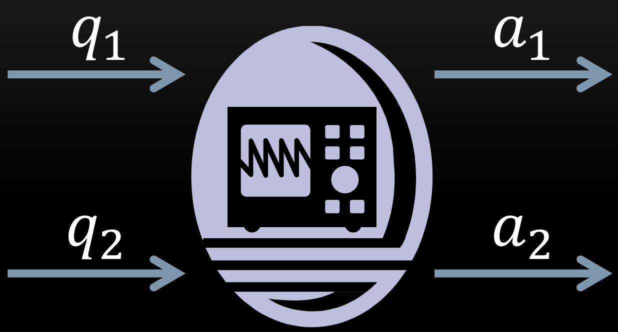
Proof outline: QIP with $2^{-2^{\mathrm{poly}}}$ gap $\supseteq$ EXP

1. Construct a no-signaling 2-prover 1-round interactive proof system with $2^{-2^{\mathrm{poly}}}$ gap for an EXP-complete problem

2. Convert it to a QIP system without ruining the gap

No-signaling box

[Khalfin and Tsirelson '85]
[Rastall '85]



Prob. dist. $p(a_1, a_2|q_1, q_2)$ satisfying *no-signaling conditions*:

- Marginal distribution of a_1 only depends on q_1

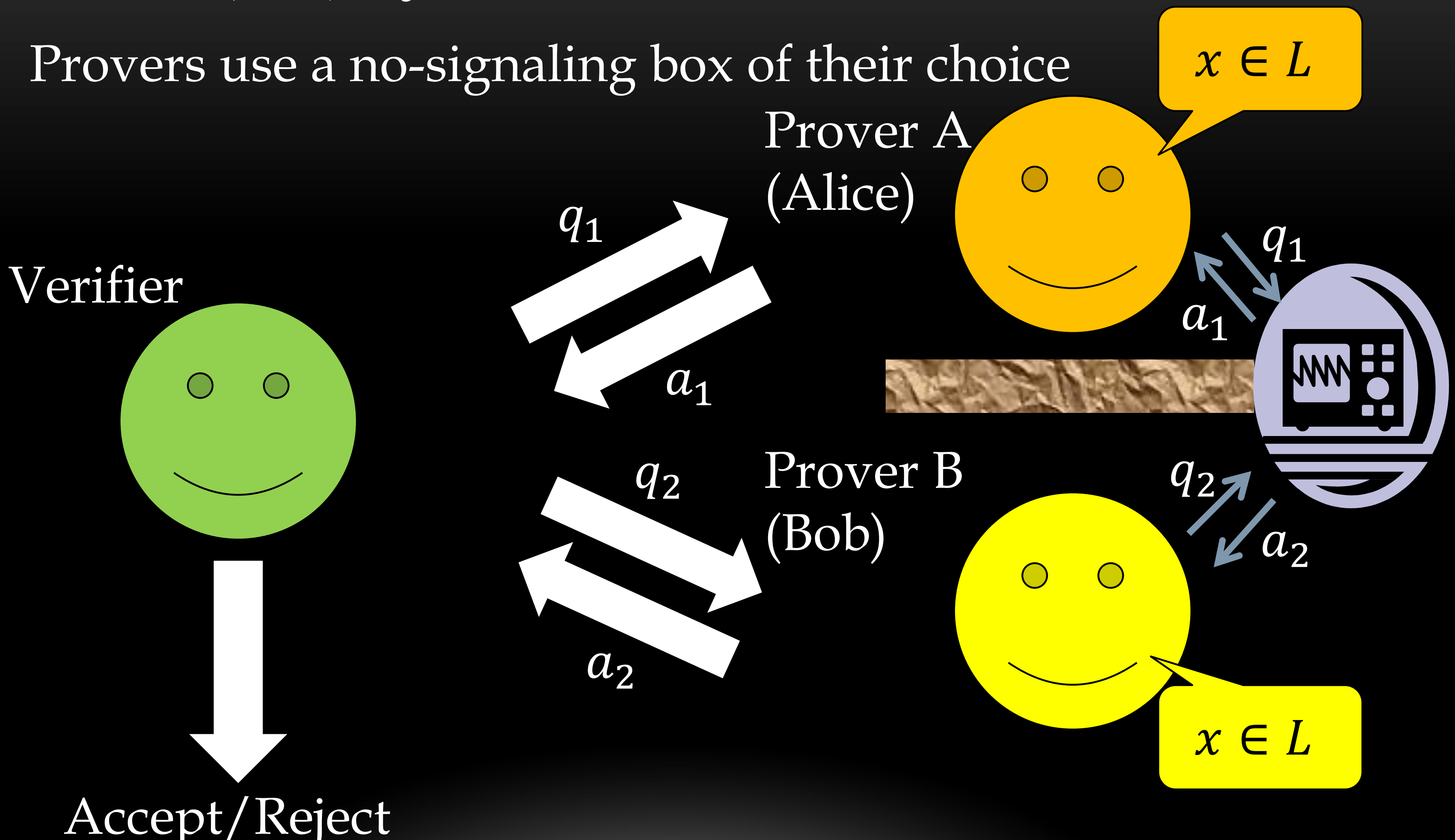
$$p_1(a_1|q_1) = \sum_{a_2} p(a_1, a_2|q_1, q_2)$$

- Marginal distribution of a_2 only depends on q_2

$$p_2(a_2|q_2) = \sum_{a_1} p(a_1, a_2|q_1, q_2)$$

$\mathrm{MIP}^{\mathrm{ns}}(2,1)$ system (considered in [Holenstein '09] etc.)

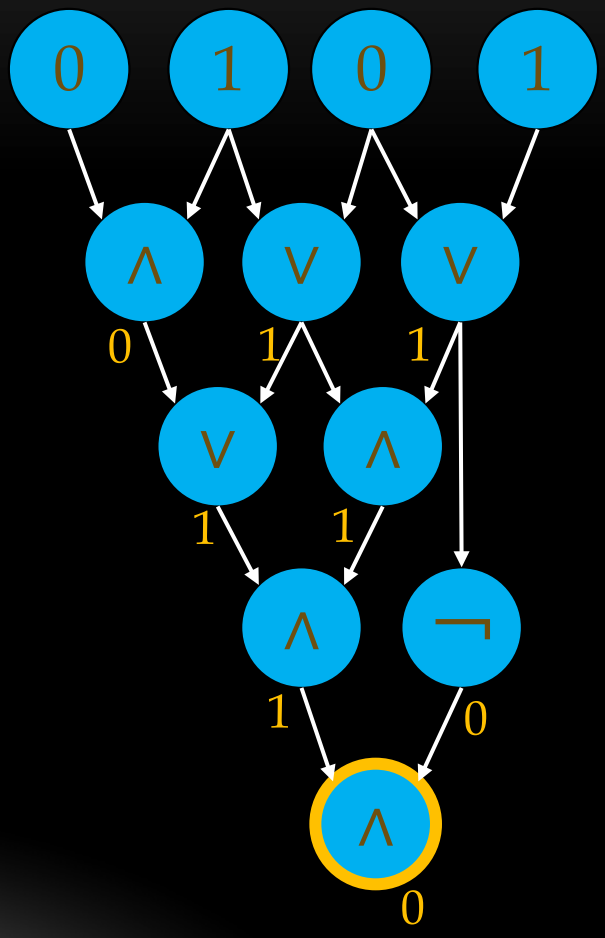
Provers use a no-signaling box of their choice



EXP-complete problem: Succinct Circuit Value (SCV)

Given: Exponentially large Boolean circuit (suitably encoded) consisting of Const-0, Const-1, 2-input AND, 2-input OR and NOT gates, and a gate *g* in it

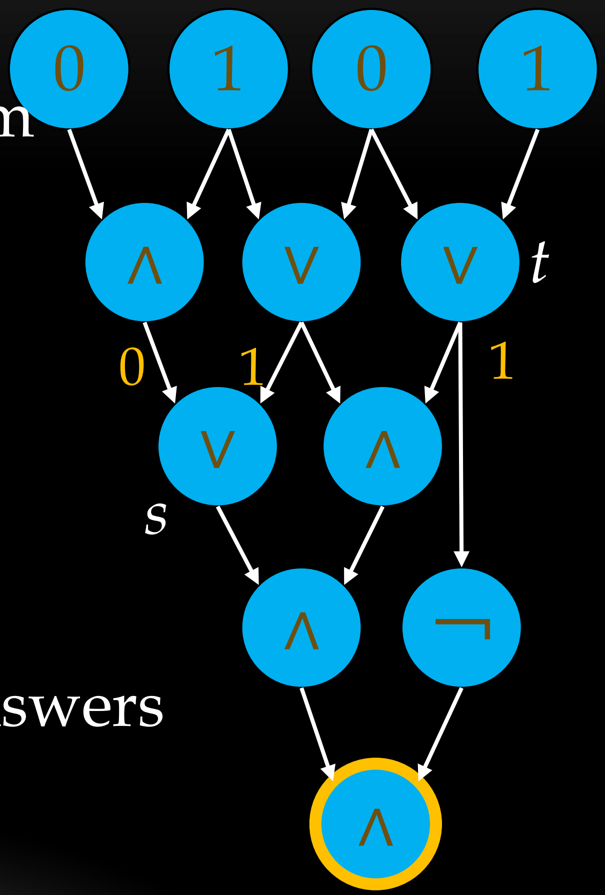
Question: Does the gate *g* output the value 1?



2-prover protocol for SCV

Verifier performs the following:

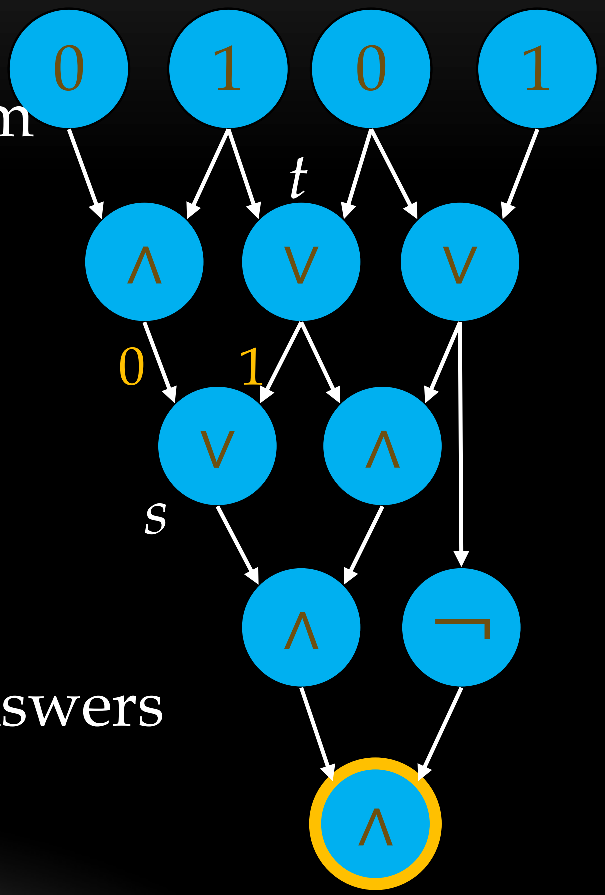
- Pick 2 gates *s*, *t* independently at random
- Ask Alice all the input values of gate *s*, and ask Bob the output value of gate *t*
- Reject if anything is wrong:
  - $s=t \Rightarrow$ answers must be consistent with the gate type
  - t is an input of $s \Rightarrow$ corresponding answers must coincide
  - $t=g \Rightarrow$ Bob's answer must be 1



2-prover protocol for SCV

Verifier performs the following:

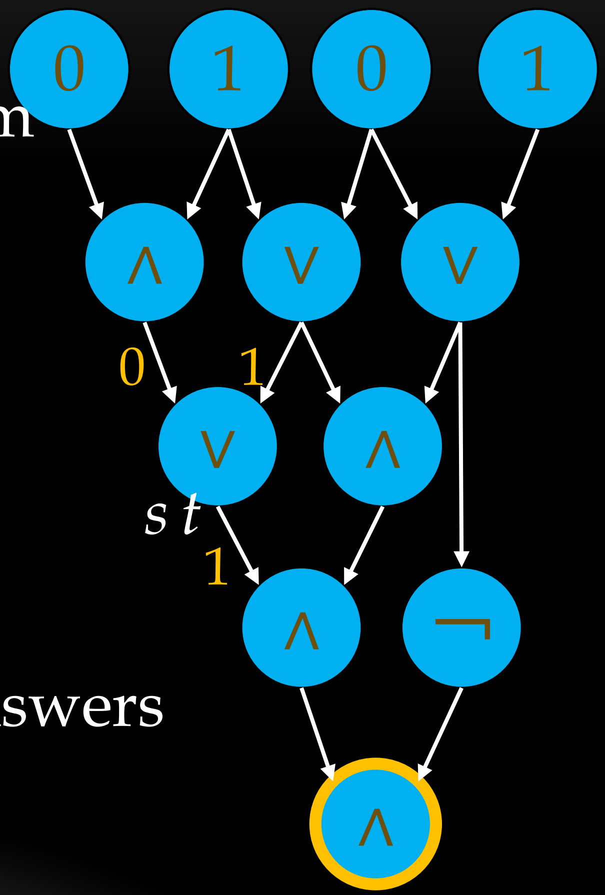
- Pick 2 gates *s*, *t* independently at random
- Ask Alice all the input values of gate *s*, and ask Bob the output value of gate *t*
- Reject if anything is wrong:
  - $s=t \Rightarrow$ answers must be consistent with the gate type
  - t is an input of $s \Rightarrow$ corresponding answers must coincide
  - $t=g \Rightarrow$ Bob's answer must be 1



2-prover protocol for SCV

Verifier performs the following:

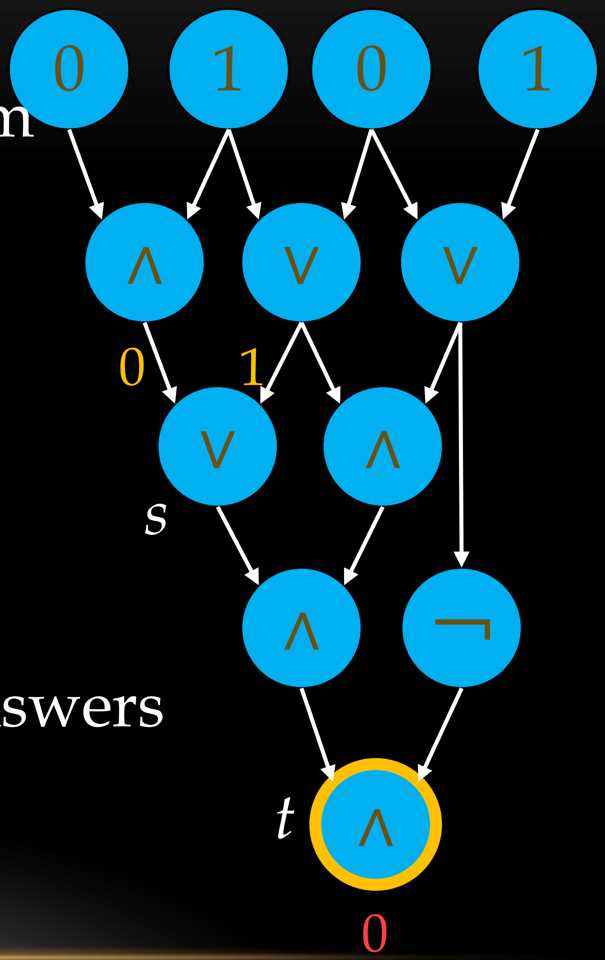
- Pick 2 gates *s*, *t* independently at random
- Ask Alice all the input values of gate *s*, and ask Bob the output value of gate *t*
- Reject if anything is wrong:
  - $s=t \Rightarrow$ answers must be consistent with the gate type
  - t is an input of $s \Rightarrow$ corresponding answers must coincide
  - $t=g \Rightarrow$ Bob's answer must be 1



2-prover protocol for SCV

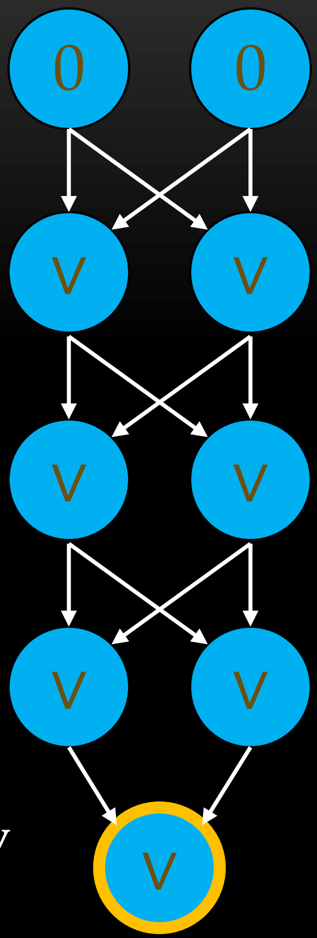
Verifier performs the following:

- Pick 2 gates s, t independently at random
- Ask Alice all the input values of gate s, and ask Bob the output value of gate t
- Reject if anything is wrong:
  - $s=t \Rightarrow$ answers must be consistent with the gate type
  - t is an input of $s \Rightarrow$ corresponding answers must coincide
  - $t=g \Rightarrow$ Bob's answer must be 1



Properties

- Perfect completeness
- Verifier almost always accepts without checking anything
  → Soundness error can be as bad as
  $1 - 4/N = 1 - 2^{-\mathrm{poly}}$
  (N = the number of gates)
  even without allowing no-signaling boxes
- Even worse with no-signaling boxes:
  Soundness error can be $1 - 2^{-(N-1)/2} = 1 - 2^{-2^{\mathrm{poly}}}$
- Soundness error is $\leq 1 - 2^{-2^{\mathrm{poly}}}$ even with no-signaling boxes (by simple proof using induction)



No-signaling 2-prover 1-round system to QIP system

- Generate s, t as max-ent states: $\sum_s |s\rangle_S |s\rangle_{S'} \otimes \sum_t |t\rangle_T |t\rangle_{T'}$
- Send both S and T to the prover,
  and receive S, T and corresponding answers A, B:

$$\sum_s \boxed{|s\rangle_S |s\rangle_{S'} |a(s)\rangle_A} \otimes \sum_t |t\rangle_T |t\rangle_{T'} |b(t)\rangle_B$$

$$|s\rangle_S |s\rangle_{S'}$$

- Randomly perform one of the following tests:
  1. Measure S', T', A, B and check the answers are consistent
  2. Send S and A, receive S, and check S and S' are max-ent
  3. Send T and B, receive T, and check T and T' are max-ent

Properties

- Perfect completeness
- Soundness error $\geq 1 - 2^{-2^{\mathrm{poly}}}$
- Soundness error $\leq 1 - 2^{-2^{\mathrm{poly}}}$:
  - Verifier's test ensures prover acts according to some "approximately no-signaling" strategy in 2-prover protocol
  - Soundness of 2-prover protocol ensures if $x \notin L$, no-signaling strategies cannot make verifier accept well
  - [Holenstein'09] "Approximately no-signaling" strategies cannot outperform no-signaling strategies by much

Other results

- QIP(2) (= 2-message QIP) with $2^{-\mathrm{poly}}$ gap ⊇ PSPACE (easy consequence of [Wehner ICALP'06])
- Upper bounds on some classes with sharp threshold
  - QIP with no gap ⊆ EXPSPACE (use [GW07] and PSPACE algorithm for exact semidefinite feasibility problem [Canny STOC'88])
  - QMA_1 (= 1-message QIP with perfect completeness) with no gap ⊆ PSPACE (use [MW04] and a parallel algorithm for linear dependence [Csanky '76])

Open problems

- PSPACE $\subseteq$ QIP with $2^{-\text{poly}}$ gap $\subseteq$ EXP

Can we reduce the error of multiplicative weights update?

- EXP $\subseteq$ QIP without gap $\subseteq$ EXPSPACE

Does semidefinite feasibility have a QIP protocol without gap?
How small can be the gap of QIP protocols?

- PSPACE $\subseteq$ QIP(2) without gap $\subseteq$ EXPSPACE

Answering these hopefully leads to new paradigms
for protocol construction / simulation