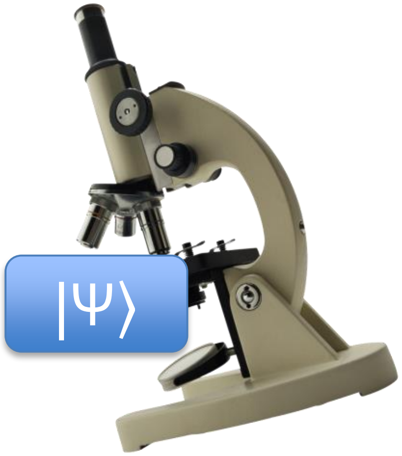
Robust self-testing of multi-qubit states

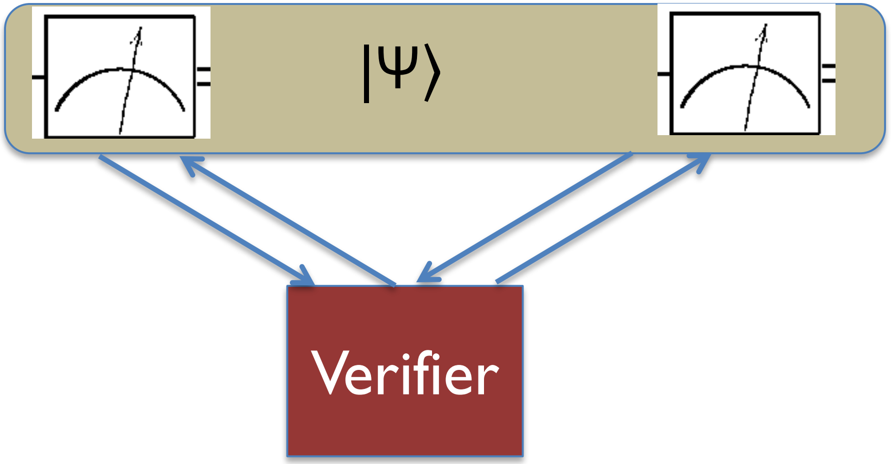
Anand Natarajan (MIT)
and Thomas Vidick (Caltech)
arXiv:1610.03574

Self-testing

Certifying an unknown quantum state up to local isometry assuming only QM and causality



vs.

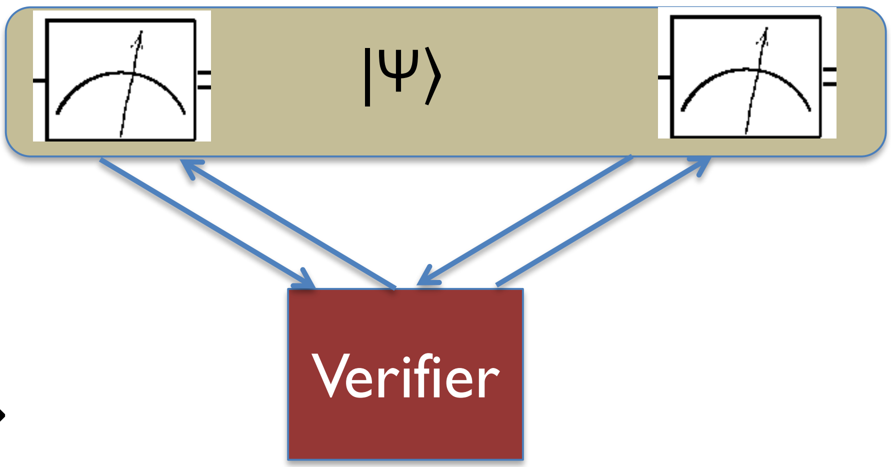


Tomography

Self-test
(aka nonlocal game, 1-round MIP*)

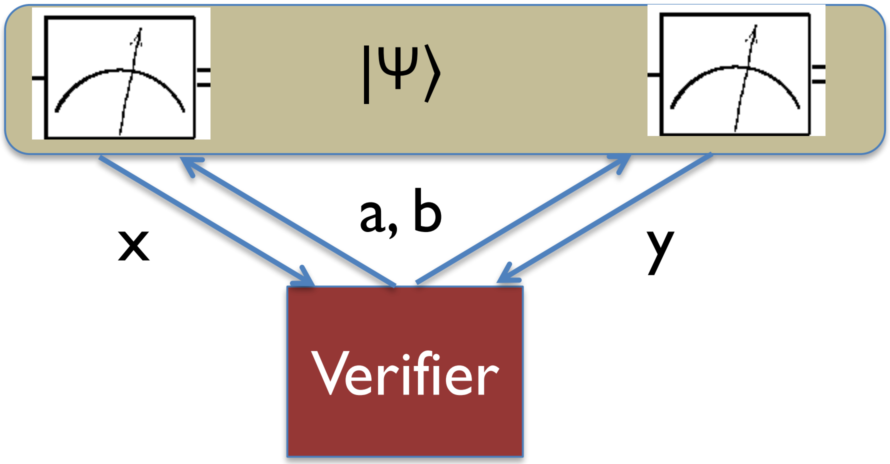
Self-testing: the setup

- We can test $|\psi\rangle$ up to error ε if:
  - Completeness:
    $\Pr[|\psi\rangle \text{ accepted}] \geq c$
  - Soundness:
    $\Pr[|\phi\rangle \text{ accepted}] \geq s \Rightarrow$
    $\exists U,V,$ s.t.
    $\|(U \otimes V)\,|\phi\rangle - |\psi\rangle\| \leq \varepsilon$
  - Robustness $= c - s$



Testing an EPR pair with CHSH

- The CHSH game is a self-test for $|\psi\rangle=(|00\rangle + |11\rangle)/\sqrt{2}$ up to ε with $c \approx 0.85$, $c - s = \Omega(\varepsilon^2)$ [MYS'12]



$x \oplus y \stackrel{?}{=} a \cdot b$

Self-testing many-qubit states

	State	Message size	Complete-ness	Soundness
MYS'12	EPR	O(1)	0.85	0.85 - ε
RUV'13	$\mathrm{EPR}^{\otimes n}$	O(n) sequential rounds	Ω(1)	c – 1/poly(n)
WBMcKS'15	$\mathrm{EPR}^{\otimes 2}$	O(1)	1	1 - ε
McK'15	$\mathrm{EPR}^{\otimes n}$	O(n)	0.94	0.94 – 1/exp(n)
Col'16,CN'16	$\mathrm{EPR}^{\otimes n}$	O(n)	1	1 – 1/poly(n)
CRSV'16	$\mathrm{EPR}^{\otimes n}$	O(log n)	0.9	0.9 – 1/poly(n)

Not robust: c-s gap shrinks with n!

Result 1: test for n EPR pairs

Thm 1: There is a 2-prover self-test for n EPR pairs up to error ε with $O(n)$-bit questions, $O(1)$-bit answers, $c = 1$, $s = 1 - \Omega(\varepsilon^{1/32})$.

First test for n EPR pairs where c-s gap constant independent of n

Application: test for ground states

Local Hamiltonian problem: given H on n qubits, is $\lambda_{min}(H) \leq a$ or $\geq b$ for $a - b = \Omega(1/poly(n))$

Thm 2: There is a 7-prover, 1-round MIP* protocol for Local Hamiltonian problem with $O(n)$-bit questions, $O(1)$-bit answers, $c = 1$, $c\text{-}s = \Omega(1)$

(Also follows from QMA $\subseteq$NEXP $\subseteq$ MIP*, but protocol is much simpler)

Application: delegated computation

Cor: 7-prover 1-round MIP* protocol for BQP with $O(n)$-bit questions, $O(1)$-bit answers, $c-s = \Omega(1)$, where honest provers need only the power of BQP.

Follows from thm 2 + Kitaev history state construction

Techniques

Proof Overview

- To test an n-qubit state, test n-qubit **observables**!
  - E.g. n-qubit Paulis $X(a)$, $Z(b)$
- To test observables, test the **algebraic relations** between them:
  - Linearity: $X(a)X(b) = X(a \oplus b)$
  - Anticommutation: $X(a)Z(b) = (-1)^{\langle a,b \rangle} Z(b)\, X(a)$

EPR Test

- With probability 1/4 each,
  - Tell Alice and Bob to measure in “X” basis, and perform linearity test
  - Tell Alice and Bob to measure in “Z” basis, and perform linearity test
  - Perform anticommutation test
  - Consistency test: send both players same random query, check they give same answer

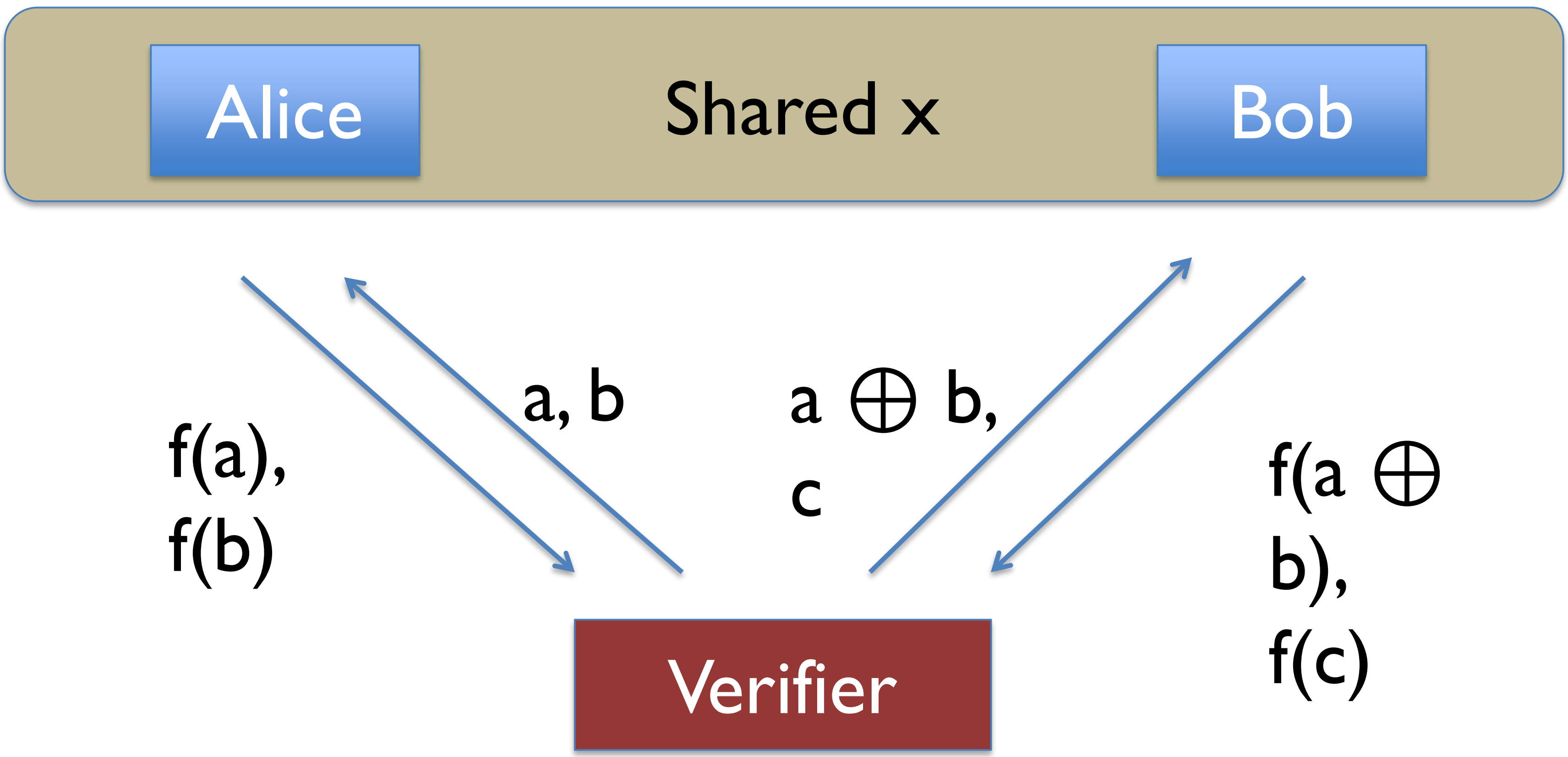
Analysis of EPR Test

- **Thm 1:** success in test → n EPR pairs
- **Lemma:** success in test → exist $X'(a)$, $Z'(b)$ *exactly* satisfying Pauli group relations
- Lemma → Theorem
  - Pauli group → isometry mapping H to $(C^2)^{\otimes n}$ and X', Z' to σ_X, σ_Z
  - Consistency test → $|\psi\rangle$ is stabilized by $\sigma_X(i) \otimes \sigma_X(i)$ and $\sigma_Z(i) \otimes \sigma_Z(i)$ for all i → EPR state

Classical linearity testing

- Function $f:\{0,1\}^n \longrightarrow \{0,1\}$ is *linear* if for all points a, b, $f(a) \oplus f(b) = f(a \oplus b)$
- Example: $f(x) = \langle x, a\rangle$
- **Thm (BLR):**
  If $\Pr_{a,b}[f(a) \oplus f(b) = f(a \oplus b)] \geq 1 - \varepsilon$, then f is $O(\varepsilon)$-close to some linear function $g(x)$

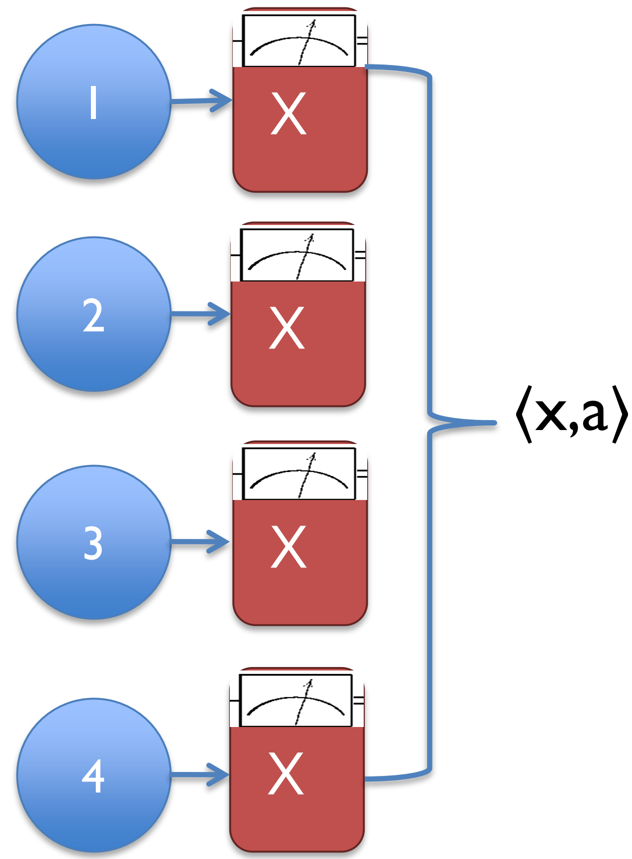
BLR Test



Check $f(a) \oplus f(b) = f(a \oplus b)$

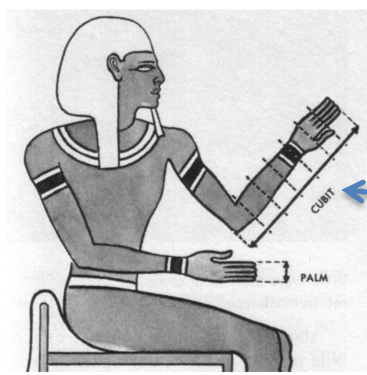
Quantum BLR Test

- $X: \{0,1\}^n \longrightarrow \mathrm{Obs}(H)$ *linear* if $\forall a,b,\ X(a)X(b) = X(a \oplus b)$
- **Thm:** if $\langle\psi|X(a)X(b)X(a\oplus b)|\psi\rangle \geq 1 - \varepsilon$, then X is ε–close to some linear Y acting on $|\psi\rangle$

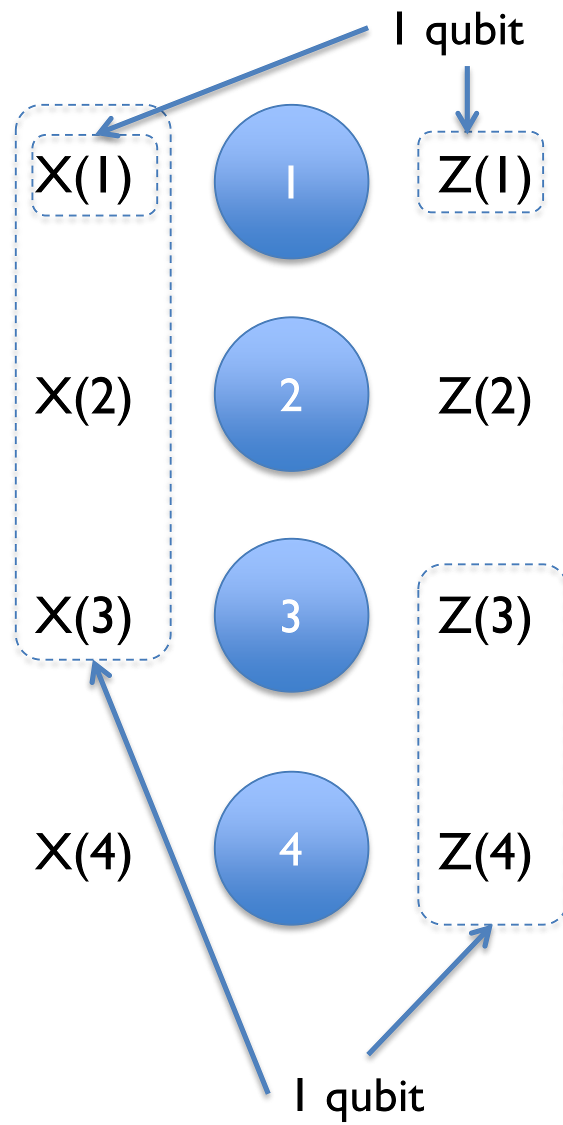


Anticommutation Test

- Any anticommuting pair $X(a), Z(b)$ defines a qubit!
- $\langle \mathrm{CHSH}(a,b) \rangle \geqslant 1-\varepsilon \rightarrow X(a)Z(b)|\psi\rangle \approx -Z(b)X(a)\,|\psi\rangle$
- (Also works with Magic Square)

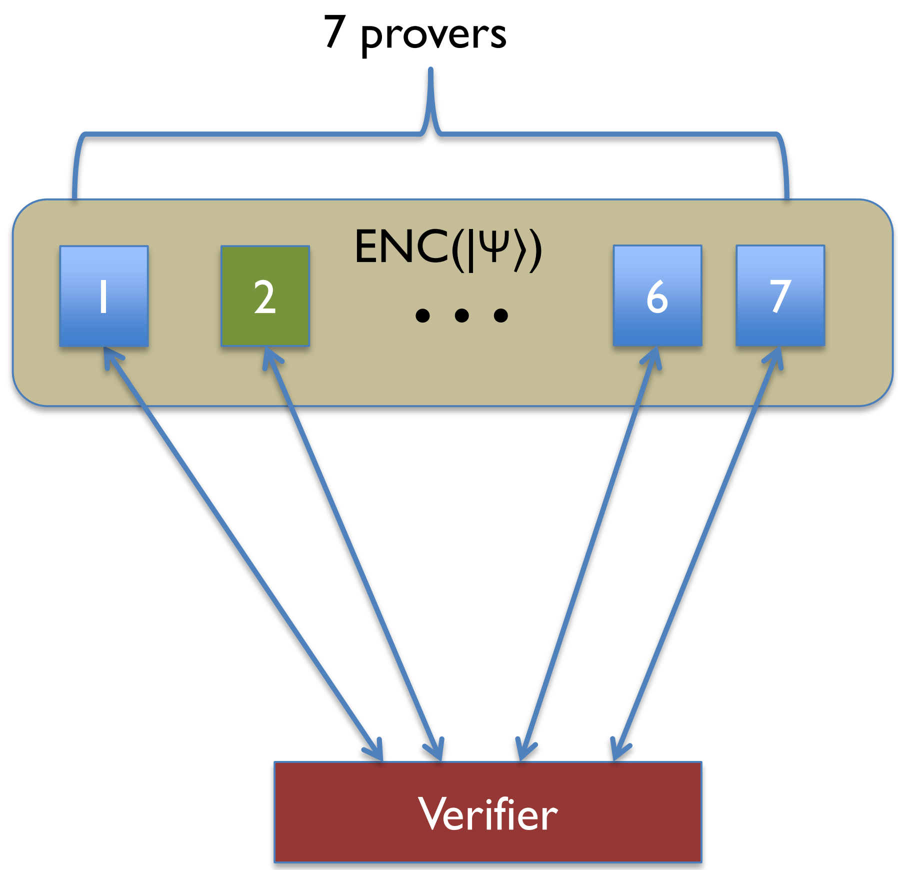


1 cubit



From EPR pairs to Ground States

- Encode each qubit of $|\Psi\rangle$ with 7-qubit code
  - Based on [FV'14], [Ji'15]
- With prob 0.5 each:
  - Pick $j \in [7]$ and play EPR test with Player j as Alice and remaining players as Bob
  - Measure Hamiltonian term



Outlook

MIP-qPCP

Conj (MIP-qPCP):
QMA $\subseteq$ MIP*(log n, c, c – δ)
(PCP: NP $\subseteq$ MIP(log n, c, c – δ))

- [FV'14]: QMA $\subseteq$ QMIP(log n, c, c – 1/poly(n))
- [Ji '15]: QMA $\subseteq$ MIP*(log n, c, c – 1/poly(n))
- [NV '16]: QMA $\subseteq$ MIP*(n, c, c – δ)
  – Toy PCP: NP $\subseteq$ MIP(n, c, c – δ)

Open questions

- MIP-qPCP
  - Can we use ideas from low-degree testing (the "old proof" of classical PCP)?
- DIQKD
- Blind delegated computation
- Alphabet reduction for quantum games
- ~~MIP* = QMIP~~ [Ji'16]
  - Can it be strengthened?

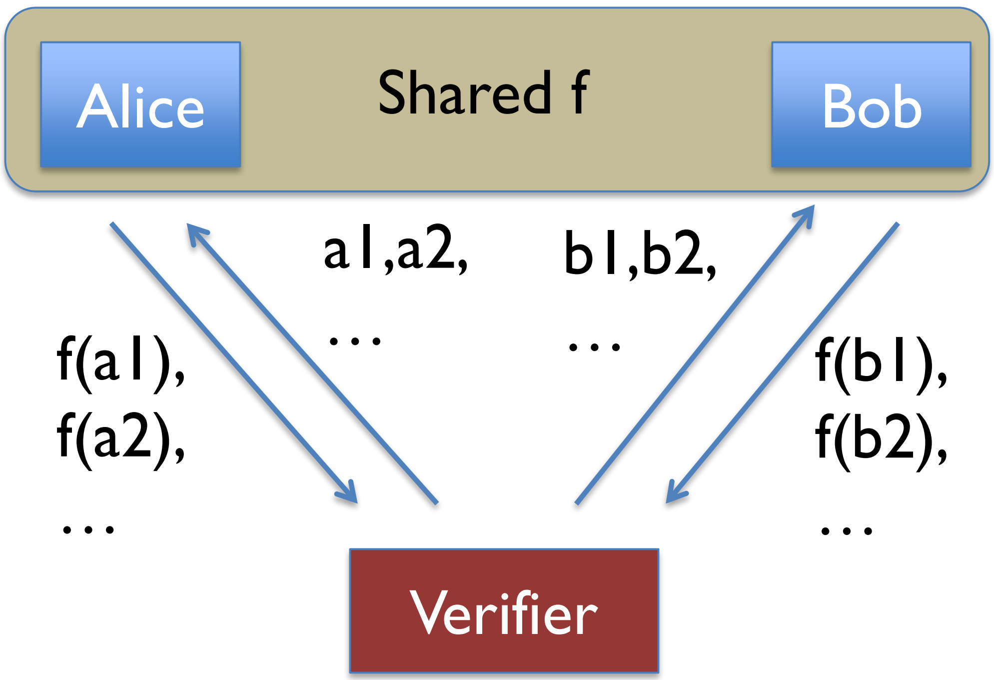
Thanks!

Any Questions?

(If I don't get to your question, ask Zhengfeng Ji)

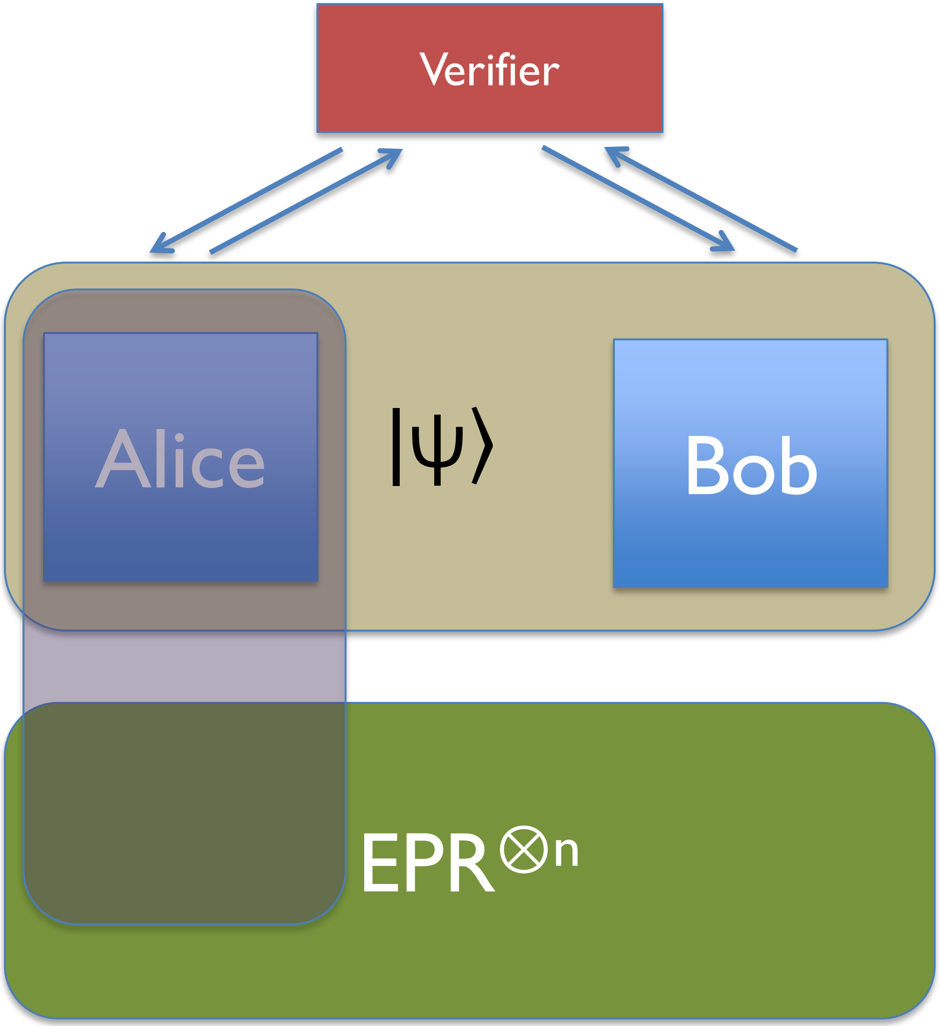
Property Testing

- Classical analog of self-testing
- Given a Boolean function $f: \{0,1\}^n \to \{0,1\}$
  - Promised f *satisfies* some global property, or is *far from* satisfying it,
  - Determine which, by making *few* queries to f



Proof of lemma

- In *analysis only* adjoin n EPR pairs
- C(a,b) := X(a)Z(b) $\otimes$ $\sigma_X(a)\ \sigma_Z(b)$
- X, Z pass EPR test $\rightarrow$C(a,b) passes BLR test
- Quantum BLR $\rightarrow$ exist linear C'(a,b) close to C(a,b)
- X'(a) := C'(a,0) $\otimes$ $\sigma_X(a)$, Z'(b) := C'(0,b) $\otimes$ $\sigma_Z(b)$



Self-testing and qPCP

- Self test = Nonlocal game = 1-round MIP*
- Classically: PCP theorem ~ hardness for MIP with constant c-s gap
  - Equivalent to hardness of approximation for CSPs
- Quantumly: MIP-qPCP := hardness for MIP* with constant c-s gap?
  - *Not* necessarily equivalent to hardness of approximation for Hamiltonians