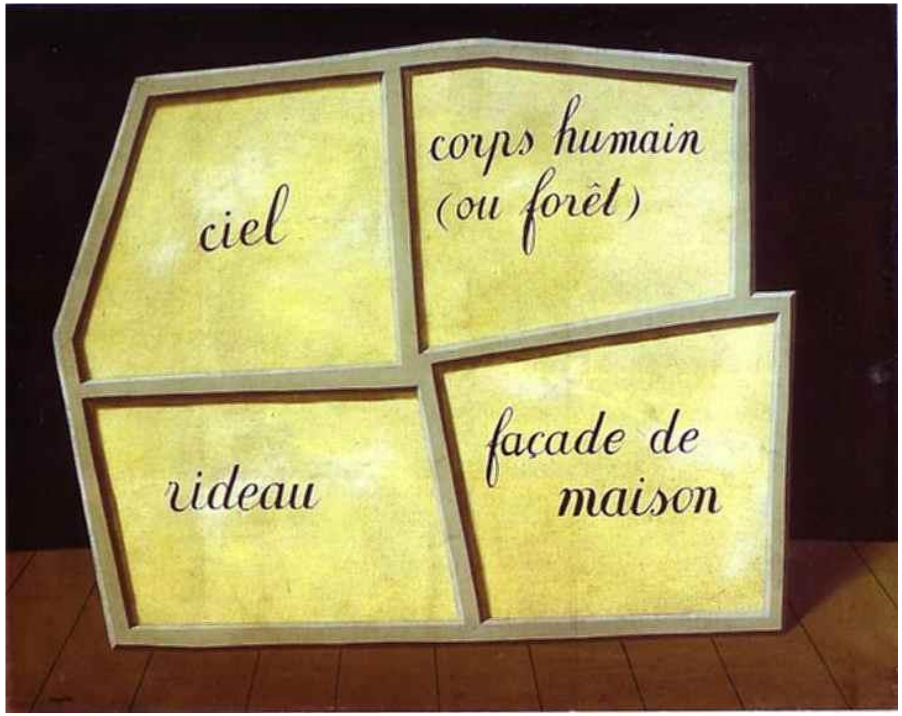
A multiprover interactive proof system for the local Hamiltonian problem



Thomas Vidick
Caltech

Joint work with Joseph Fitzsimons
SUTD and CQT, Singapore

Outline

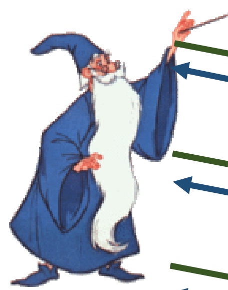
1. Local verification of classical & quantum proofs
2. Quantum multiplayer games
3. Result: a game for the local Hamiltonian problem
4. Consequences:
   a) The quantum PCP conjecture
   b) Quantum interactive proof systems

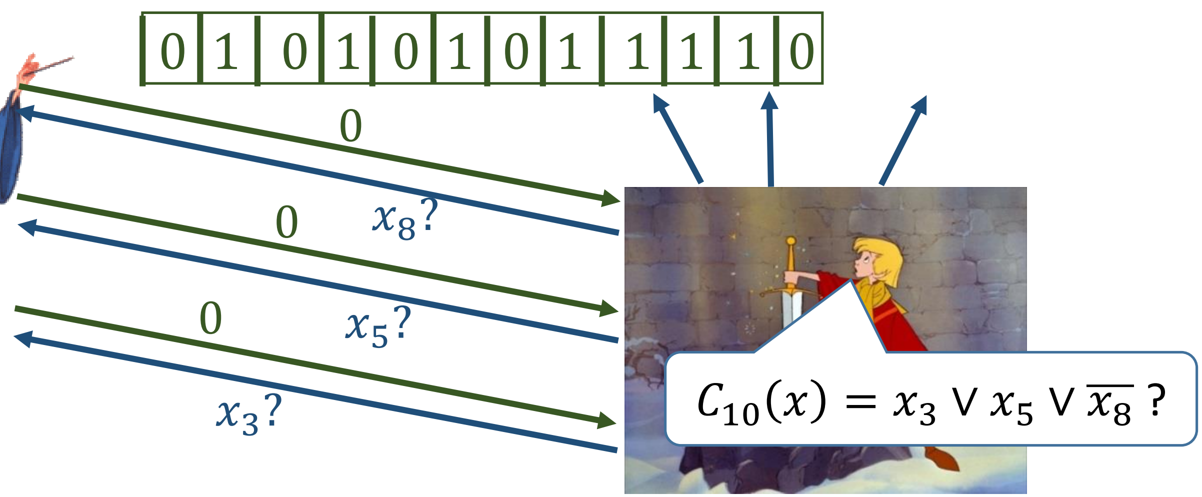
Local verification of classical proofs

- NP = { decision problems "does x have property P?"
  that have polynomial-time verifiable proofs }
  - Ex: Clique, chromatic number, Hamiltonian path
  - 3D Ising spin
  - Pancake sorting, Modal logic S5-Satisfiability, Super Mario, Lemmings
- Cook-Levin theorem: 3-SAT is complete for NP

Graph $G \to$ 3-SAT formula φ
G 3-colorable $\Leftrightarrow$ φ satisfiable

- Consequence: all problems in NP have local verification procedures
- Do we even need the whole proof?





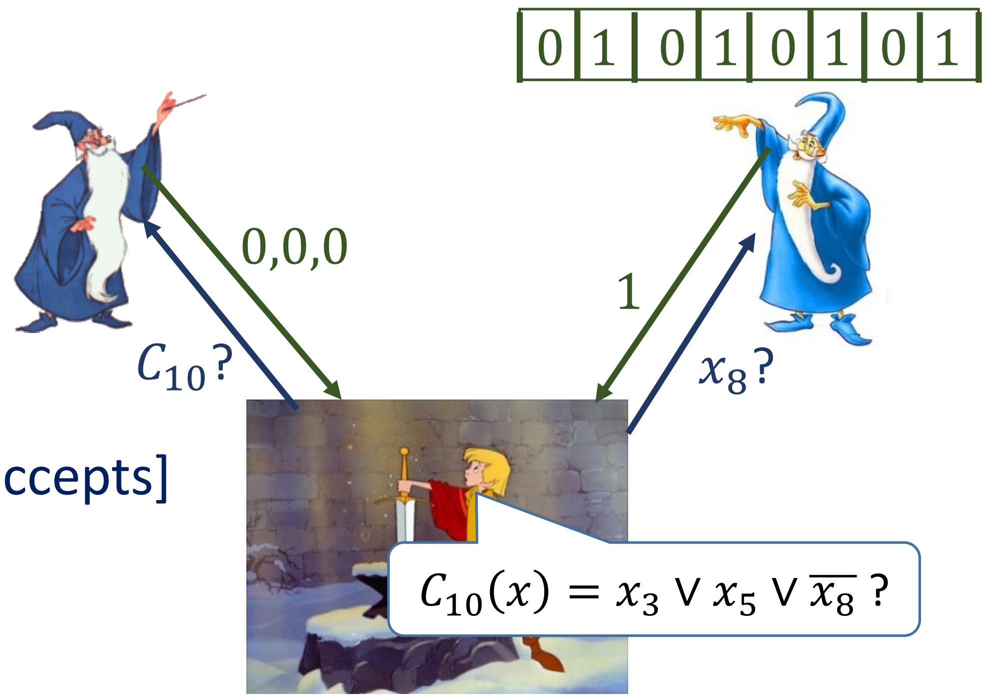
- Proof required to guarantee *consistency* of assignment

$\exists x, \varphi(x) = C_1(x) \wedge C_2(x) \wedge \cdots \wedge C_m(x) = 1?$

Is G 3-colorable?

Multiplayer games: the power of two Merlins

- Arthur ("referee") asks questions
- Two isolated Merlins ("players")
- Arthur checks answers.



- Value $\omega(G)$ = $\sup_{\text{Merlins}}$ Pr[Arthur accepts]
- Ex: 3-SAT game $G = G_\varphi$

$\exists x, \varphi(x) = C_1(x) \wedge C_2(x) \wedge \cdots \wedge C_m(x) = 1?$

- Consequence: All languages in NP have *truly local* verification procedure

- PCP Theorem: poly-time $G_\varphi \to \widetilde{G_\varphi}$ such that $\omega(G_\varphi) = 1 \Longrightarrow \omega(\widetilde{G_\varphi}) = 1$

$$\omega(G_\varphi) < 1 \Longrightarrow \omega(\widetilde{G_\varphi}) \leq 0.9$$

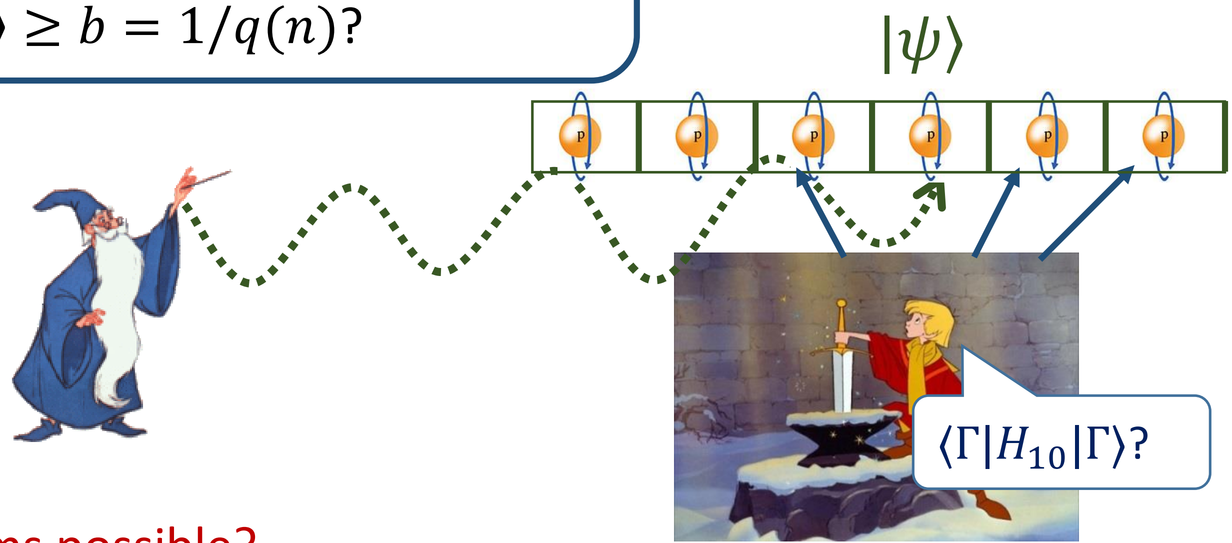
Local verification of quantum proofs

- QMA = { decision problems "does x have property P"
  that have *quantum* polynomial-time verifiable *quantum* proofs }
  - Ex: quantum circuit-sat, unitary non-identity check
  - Consistency of local density matrices, N-representability
- [Kitaev'99,Kempe-Regev'03] 3-local Hamiltonian is complete for QMA

$H = \sum_i H_i$, each H_i acts on 3 out of n qubits. Decide:

$\exists|\Gamma\rangle,\ \langle\Gamma|H|\Gamma\rangle \le a = 2^{-p(n)}$, or

$\forall|\Phi\rangle,\ \langle\Phi|H|\Phi\rangle \ge b = 1/q(n)$?



- Still need Merlin to provide complete state
- Today: is "truly local" verification of QMA problems possible?

$\exists|\Gamma\rangle, \langle\Gamma|H_1|\Gamma\rangle \le a$ & ... & $\langle\Gamma|H_m|\Gamma\rangle \le a$?

Outline

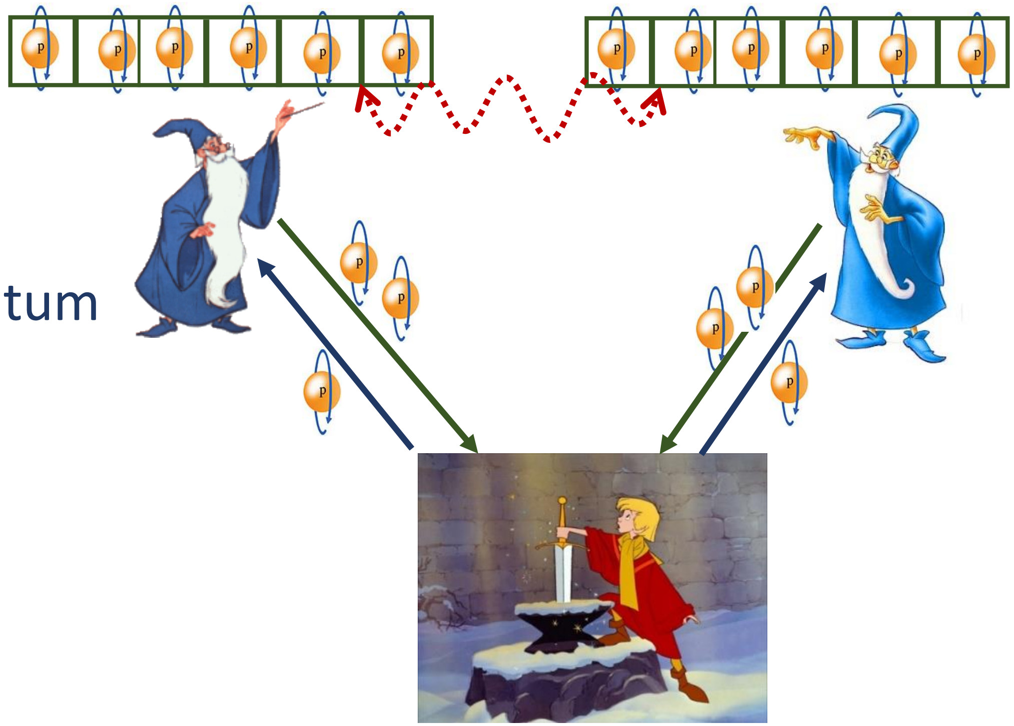
1. Local verification of classical & quantum proofs

2. Quantum multiplayer games

3. Result: a game for the local Hamiltonian problem

4. Consequences:
    a) The quantum PCP conjecture
    b) Quantum interactive proof systems

Quantum multiplayer games



- Quantum Arthur exchanges quantum messages with quantum Merlins

- Value $\omega^*(G)$ = $\sup_{\text{Merlins}}$ Pr[Arthur accepts]

Measure $\Pi = \{\Pi^{acc}, \Pi^{rej}\}$

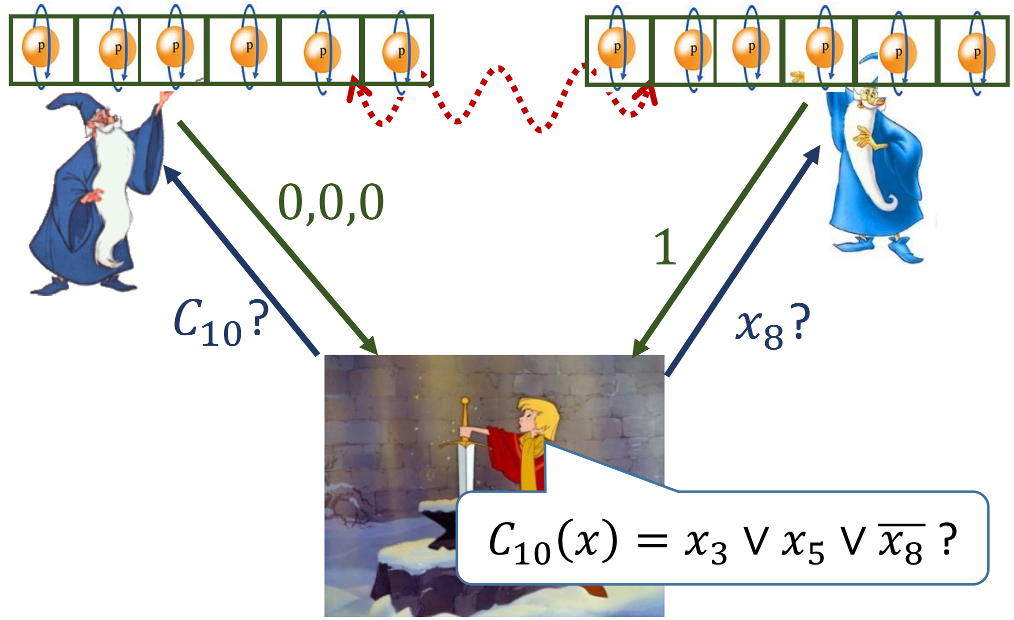
- Quantum messages → more power to Arthur

- Entanglement → more power to Merlins…

- Can Arthur use *entangled* Merlins to his advantage?

The power of entangled Merlins (1)

The clause-vs-variable game



$\exists x, \varphi(x) = C_1(x) \wedge C_2(x) \wedge \cdots \wedge C_m(x) = 1?$

- No entanglement:

  $\omega(G_\varphi) = 1 \Leftrightarrow \varphi$ SAT

- Magic Square game: $\exists$ 3-SAT φ,

  φ UNSAT but $\omega^*(G_\varphi) = 1$!

- Not a surprise: $\omega^*(G) \gg \omega(G)$

  is nothing else than Bell inequality violation

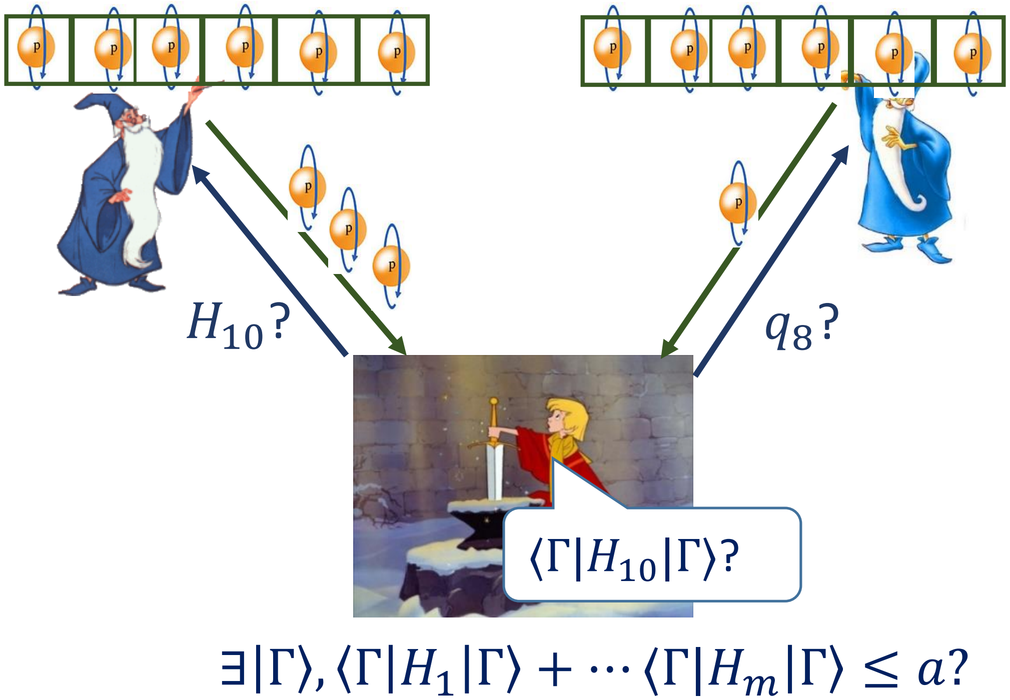
- [KKMTV'08,IKM'09] More complicated $\varphi \rightarrow \widetilde{G_\varphi}$ s.t. φ SAT $\Leftrightarrow \omega^*(\widetilde{G_\varphi}) = 1$

  $\rightarrow$ Arthur can still use entangled Merlins to decide problems in NP

- Can Arthur use entangled Merlins to decide QMA problems?

The power of entangled Merlins (2)

A Hamiltonian-vs-qubit game?



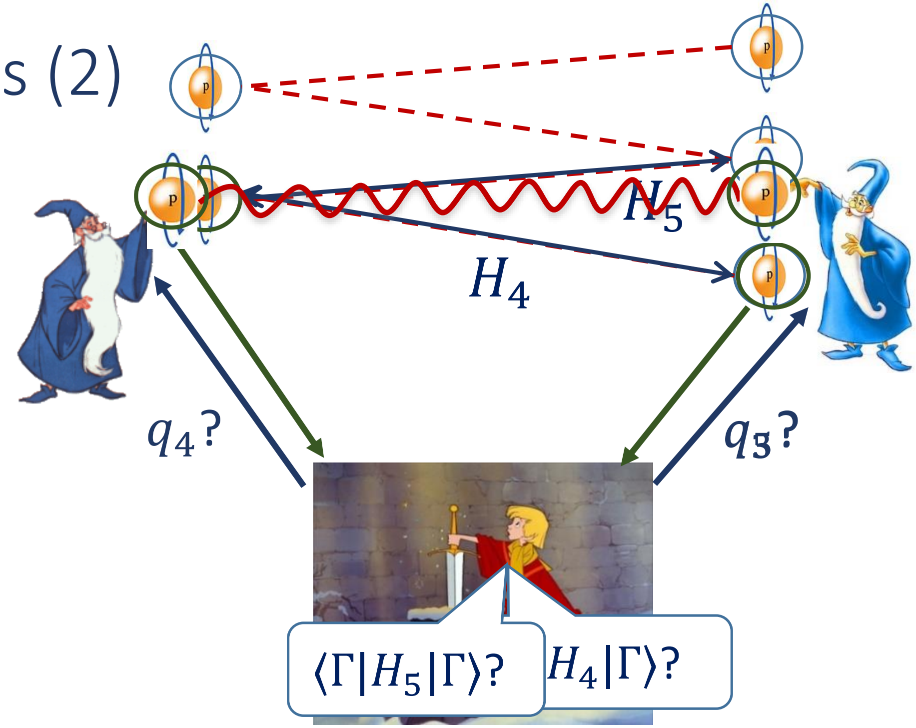
- Given H , can we design $G = G_H$ s.t.:
  $\exists|\Gamma\rangle, \langle\Gamma|H|\Gamma\rangle \leq a \quad \Rightarrow \; \omega^*(G) \approx 1$
  $\forall|\Phi\rangle, \langle\Phi|H|\Phi\rangle \geq b \Rightarrow \; \omega^*(G) \ll 1$

- Some immediate difficulties:
  - Cannot check for equality of reduced densities
  - Local consistency $\nRightarrow$ global consistency
    (deciding whether this holds is itself a QMA-complete problem)
  - [KobMat03] Need to *use* entanglement to go beyond NP

- Idea: split proof qubits between Merlins

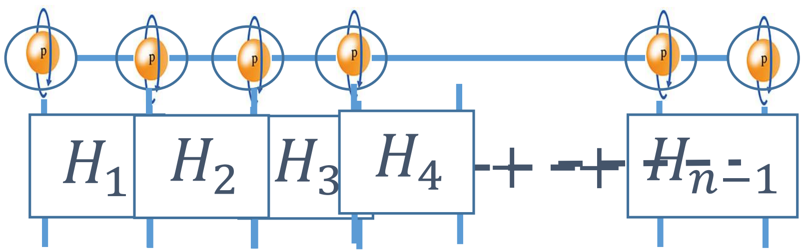
The power of entangled Merlins (2)

A Hamiltonian-vs-qubit game?



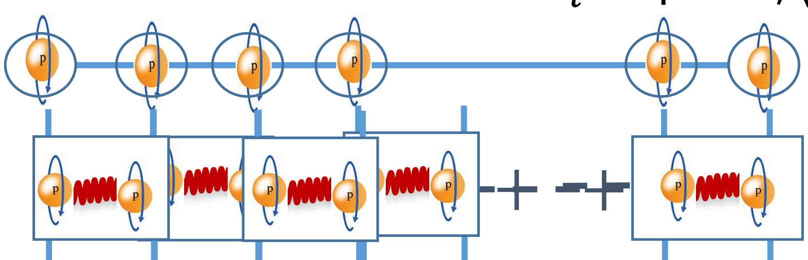
$\exists|\Gamma\rangle, \langle\Gamma|H_1|\Gamma\rangle + \cdots \langle\Gamma|H_m|\Gamma\rangle \leq a$?

- [AGIK'09] Assume H is 1D



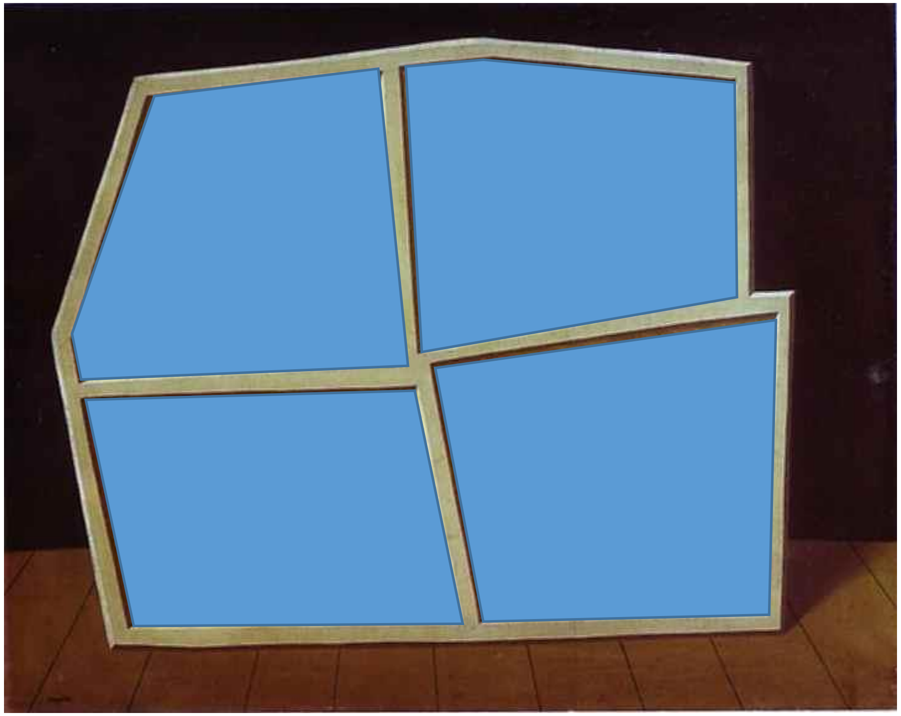
- Merlin$_1$ takes even qubits,
  Merlin$_2$ takes odd qubits
- $\omega^*(G_H) = 1 \Rightarrow \exists|\Gamma\rangle, \langle\Gamma|H|\Gamma\rangle \approx 0$?

- Bad example: the EPR Hamiltonian $H_i = |EPR\rangle\langle EPR|_{i,i+1}$ for all i



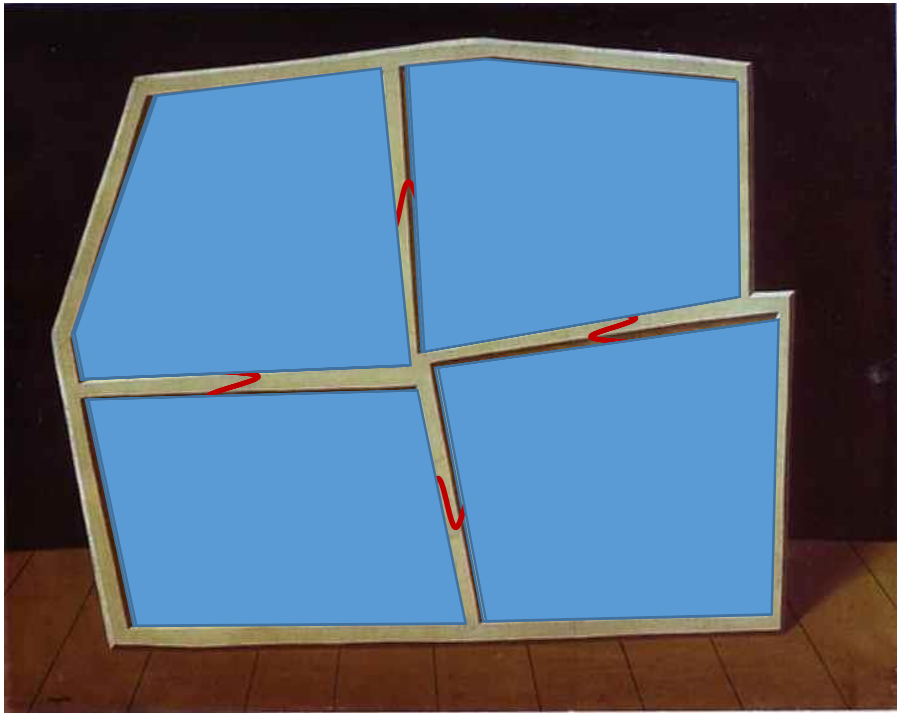
- Highly frustrated, but $\omega^*(G_H) = 1$!

The difficulty



?

The difficulty



Can we check existence of global state
$|\Gamma\rangle$ from "local snapshots" only?

Outline

1. Checking proofs locally

2. Entanglement in quantum multiplayer games

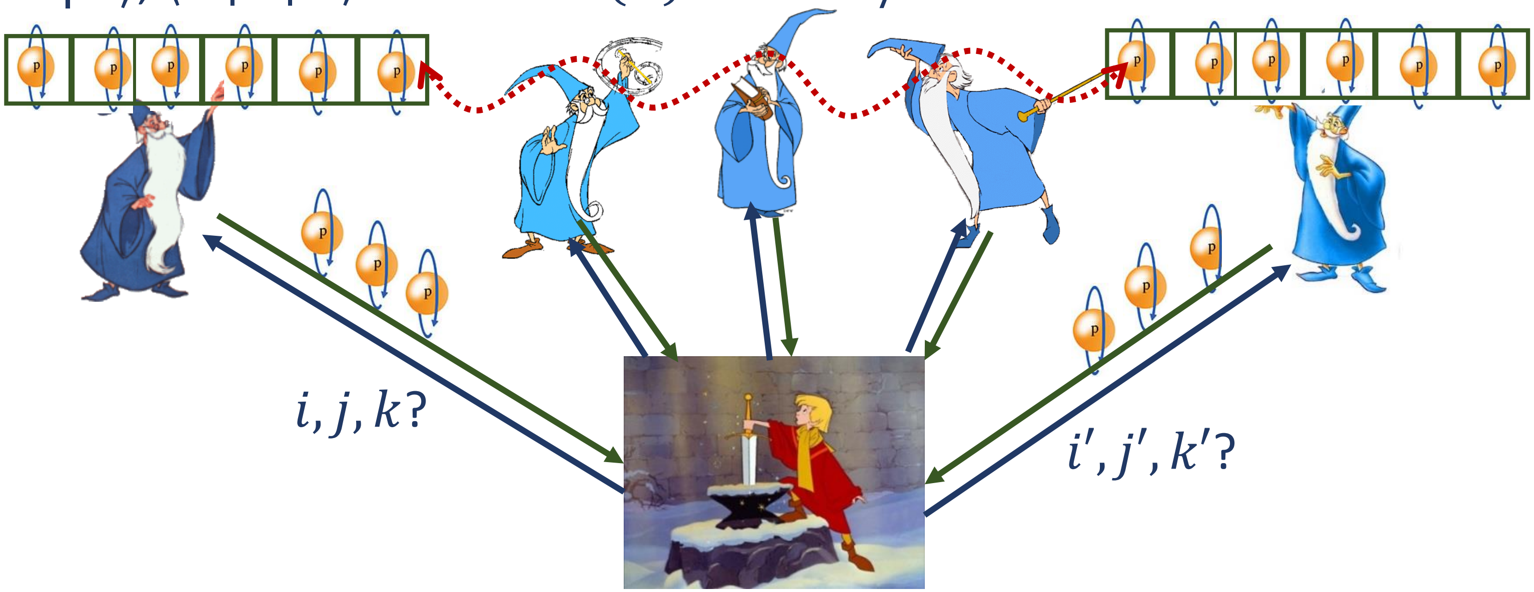
3. Result: a quantum multiplayer game for the local Hamiltonian problem

4. Consequences:
    1. The quantum PCP conjecture
    2. Quantum interactive proof systems

Result: a five-player game for LH

Given 3-local H on n qubits, design 5-player $G = G_H$ such that:

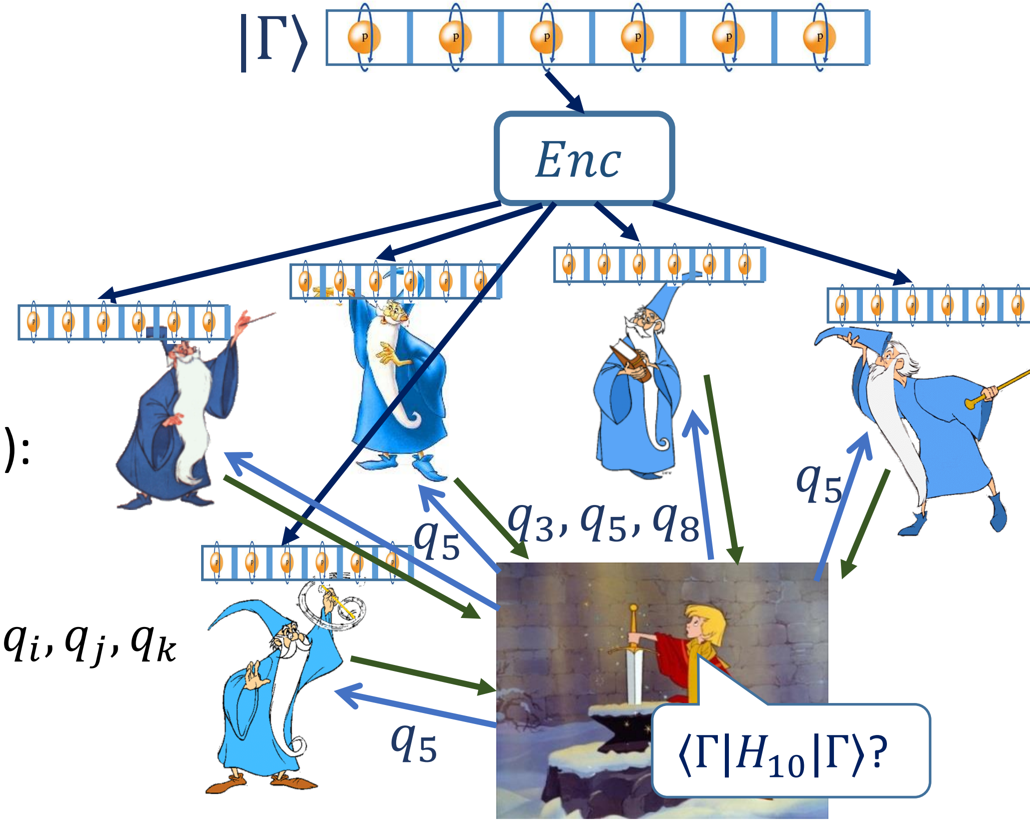
- $\exists |\Gamma\rangle, \langle\Gamma|H|\Gamma\rangle \leq a \;\Rightarrow\; \omega^*(G) \geq 1 - a/2$
- $\forall |\Phi\rangle, \langle\Phi|H|\Phi\rangle \geq b \Rightarrow \omega^*(G) \leq 1 - b/n^c$



- Consequence: the value $\omega^*(G)$ for G with n classical questions, 3 answer qubits, 5 players, is QMA-hard to compute to within $\pm 1/poly(n)$

- Consequence: $QMIP \subsetneq QMIP^*(1 - 2^{-p}, 1 - 2 \cdot 2^{-p})$ (unless $NEXP = QMA_{EXP}$)

The game $G = G_H$



$\exists|\Gamma\rangle, \langle\Gamma|H_1|\Gamma\rangle + \cdots \langle\Gamma|H_m|\Gamma\rangle \leq a$?

- ECC E corrects ≥ 1 error
  (ex: 5-qubit Steane code)

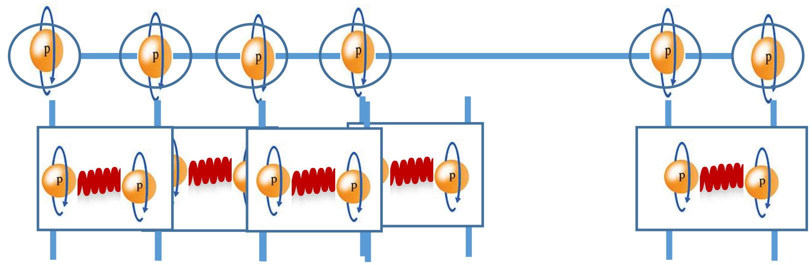
- Arthur runs two tests (prob 1/2 each):

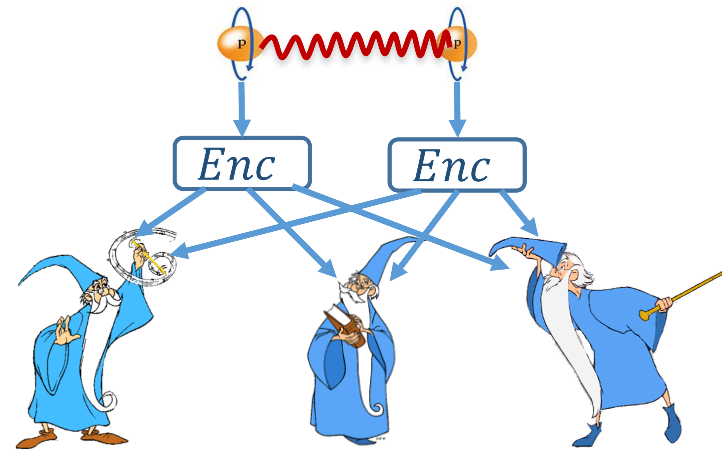
1. Select random H_ℓ on q_i, q_j, q_k
   a) Ask each Merlin for its share of q_i, q_j, q_k
   b) Decode E
   c) Measure H_ℓ
2. Select random H_ℓ on q_i, q_j, q_k
   a) Ask one (random) Merlin for its share of q_i, q_j, q_k.
      Select $s \in \{i, j, k\}$ at random; ask remaining Merlins for their share of q_s
   b) Verify that all shares of q_s lie in codespace

- Completeness: $\exists|\Gamma\rangle, \langle\Gamma|H|\Gamma\rangle \leq a \Rightarrow \omega^*(G) \geq 1 - a/2$ ✓

Soundness: cheating Merlins (1)

- Example: EPR Hamiltonian



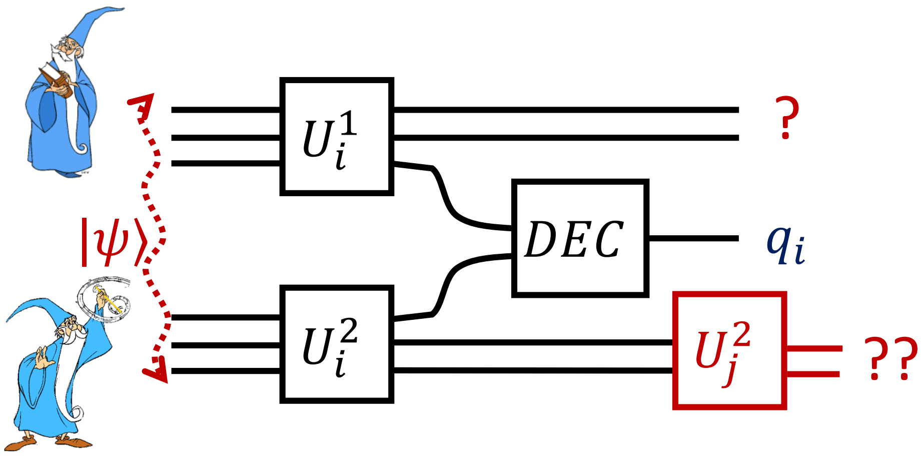


- Cheating Merlins share single EPR pair
- On question $H_\ell = \{q_\ell, q_{\ell+1}\}$, all Merlins sends back both shares of EPR
- On question q_i, all Merlins send back their share of first half of EPR
- All Merlins asked $H_\ell \rightarrow$ Arthur decodes correctly and verifies low energy ✓
- One Merlin asked $H_i = \{q_i, q_{i+1}\}$ *or* $H_{i-1} = \{q_{i-1}, q_i\}$, others asked q_i
  - If H_i, Arthur checks his first half with other Merlin's → accept ✓
  - If H_{i+1}, Arthur checks his second half with otherMerlin's → reject ✗
- Answers from 4 Merlins + code property commit remaining Merlin's qubit

Soundness: cheating Merlins (2)

- Goal: show $\forall|\Phi\rangle, \langle\Phi|H|\Phi\rangle \geq b \Rightarrow \omega^*(G) \leq 1 - b/n^c$
- Contrapositive: $\omega^*(G) > 1 - b/n^c \Rightarrow \exists|\Gamma\rangle, \langle\Gamma|H|\Gamma\rangle < b$
  → extract low-energy witness from successful Merlin's strategies

- Given:
  - 5-prover entangled state $|\psi\rangle$
  - For each i, unitary U_i extracts Merlin's answer qubit to q_i
  - For each term H_ℓ on q_i, q_j, q_k, unitary V_ℓ extracts $\{q_i, q_j, q_k\}$

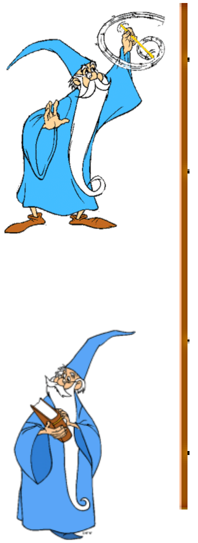


- Unitaries local to each Merlin, but no a priori notion of qubit
- Need to *simultaneously* extract $q_1, q_2, q_3, \ldots$

Soundness: cheating Merlins (3)

We give circuit generating low-energy witness $|\Gamma\rangle$
from successful Merlin's strategies

$|\Psi\rangle$



q_1
q_2

Outline

1. Checking proofs locally

2. Entanglement in quantum multiplayer games

3. Result: a quantum multiplayer game for the local Hamiltonian problem

4. Consequences:
    1. The quantum PCP conjecture
    2. Quantum interactive proof systems

Perspective: the quantum PCP conjecture

PCP theorem (1): constant-factor approximations to $\omega(G)$ are NP-hard

⟺ Clause-vs-variable game

PCP theorem (2): Given 3-SAT φ, it is NP-hard to decide between 100%-SAT vs $\leq 99\%$-SAT

Kitaev's QMA-completeness result for LH is a first step towards:

[AALV'10] Quantum PCP conjecture: There exists constants $\alpha < \beta$ such that given local $H = H_1 + \cdots + H_m$, it is QMA-hard to decide between:

- $\exists |\Gamma\rangle, \quad \langle\Gamma|H|\Gamma\rangle \leq a = \alpha m,$ or
- $\forall |\Phi\rangle, \langle\Phi|H|\Phi\rangle \geq b = \beta m$

⇕ ? No known implication!

Our results are a first step towards:

Quantum PCP conjecture*: constant-factor approximations to $\omega^*(G)$ are QMA-hard

Consequences for interactive proof systems

$L \in MIP(c,s)$ if $\exists x \to G_x$ such that
- $x \in L \Rightarrow \omega(G_x) \geq c$
- $x \notin L \Rightarrow \omega(G_x) \leq s$

$L \in QMIP^*(c,s)$ if $\exists x \to G_x$ such that
- $x \in L \Rightarrow \omega^*(G_x) \geq c$
- $x \notin L \Rightarrow \omega^*(G_x) \leq s$

- Cook-Levin:

  $NEXP = MIP(1,1-2^{-p})$
- PCP:

  $NEXP = MIP(1,1/2)$

- [KKMTV'08,IKM'09]

  $NEXP \subseteq (Q)MIP^*(1,1-2^{-p})$
- [IV'13]

  $NEXP \subseteq (Q)MIP^*(1,1/2)$

- Our result: $QMA_{EXP} \subseteq QMIP^*(1-2^{-p}, 1-2\cdot 2^{-p})$
- Consequence: $QMIP \neq QMIP^*(1-2^{-p}, 1-2\cdot 2^{-p})$

  (unless $NEXP = QMA_{EXP}$)

Summary

- Design “truly local” verification pocedure for LH
- Entangled Merlins strictly more powerful than unentangled
- Proof uses ECC to recover global witness from local snapshots

Questions

- Design a game with classical answers for LH?
  [RUV’13] requires poly rounds
- Prove Quantum PCP Conjecture*
- What is the relationship between QPCP and QPCP*?
- Are there quantum games for languages beyond QMA?

Thank you!