



**shorter  
proofs**

for

**G-**  
**R-O-**  
**U-N-D-**  
**S-T-A-T-**  
**E-C-O-N-N-**  
**E-C-T-I-V-I-T-Y**

libor caha  
daniel nagaj  
martin schwarz

IoP SAS  
Smolenice  
CEQIP 2018



shorter  
proofs

for

G-

R-O-

U-N-D-

S-T-A-T-

E-C-O-N-N-

E-C-T-I-V-I-T-Y

libor caha  
daniel nagaj  
martin schwarz

IoP SAS  
Smolenice  
CEQIP 2018

## Shorter unentangled proofs for ground state connectivity

Libor Caha<sup>1</sup>  · Daniel Nagaj<sup>1</sup> · Martin Schwarz<sup>2</sup>

Received: 22 February 2018 / Accepted: 29 May 2018  
© Springer Science+Business Media, LLC, part of Springer Nature 2018

**Abstract** Can one considerably shorten a proof for a quantum problem by using a protocol with a constant number of unentangled provers? We consider a frustration-free variant of the QCMA-complete ground state connectivity (GSCON) problem for a system of size  $n$  with a proof of superlinear size. We show that we can shorten this proof in QMA(2): There exists a two-copy, unentangled proof with length of order  $n$ , up to logarithmic factors, while the completeness–soundness gap of the new protocol becomes a small inverse polynomial in  $n$ .

**Keywords** Quantum complexity · QMA(2) · Unentanglement · Short proofs · Ground state connectivity problem (GSCON)

### 1 Introduction: unentangled provers and short proofs

While entanglement is essential for quantum algorithms, *unentanglement* can also be an interesting resource. In quantum complexity, such a guarantee about a purported proof can significantly improve the power of a verifier. Blier and Tapp [3] discovered that two unentangled copies of a *short* witness of the type

# Caha, Nagaj, Schwarz

## Quantum Information Processing

### 17:174 (2018)



1712.07400

✉ Libor Caha  
libor.caha@savba.sk

Daniel Nagaj  
daniel.nagaj@savba.sk

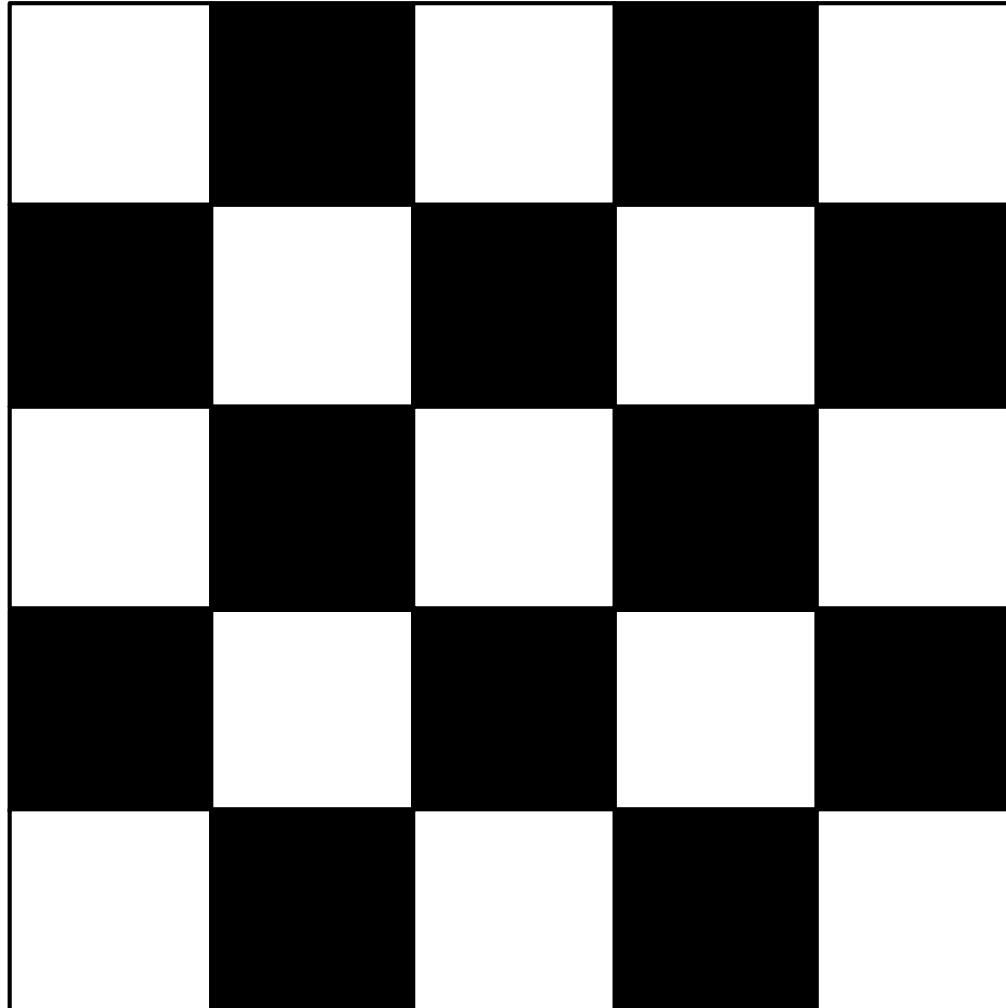
<sup>1</sup> Research Center for Quantum Information, Institute of Physics, Slovak Academy of Sciences,  
Dbravsk cesta 9, 84511 Bratislava, Slovakia

<sup>2</sup> Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany

# ● Puzzles and proofs



- 5 queens, > 10 solutions?

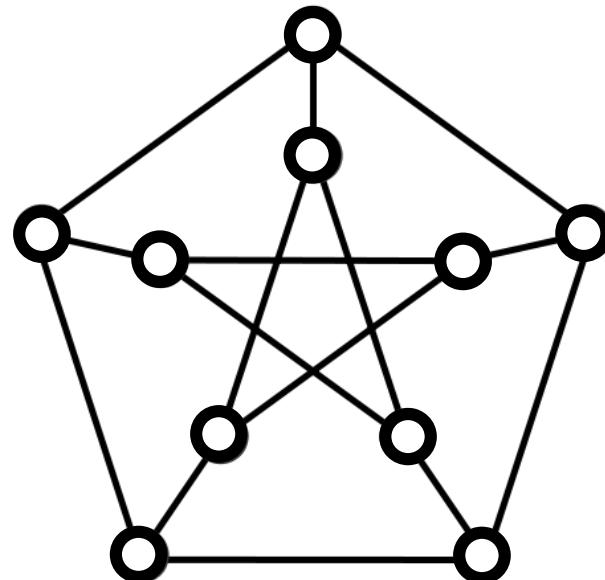


# ● NP: checkable proofs

traveling salesman: a list of cities

sudoku: fill the boxes with numbers

graph 3-coloring: vertex colors

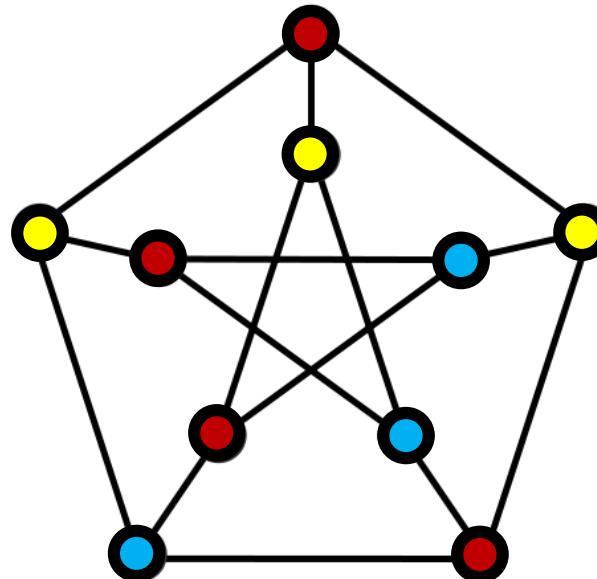


# ● NP: checkable proofs

traveling salesman: a list of cities

sudoku: fill the boxes with numbers

graph 3-coloring: vertex colors





What to  
do with  
a proof?

convince me!

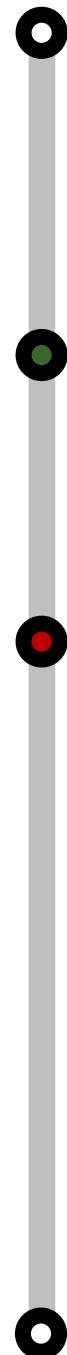
NP

Verify.

say what?

What if we  
only have  
probabilistic  
checks?

Carefully  
verify!



completeness (YES)  
convince me

stay skeptical  
soundness (NO)

MA

● probability of accepting a proof

Trust good proofs.



A tiny chance  
to detect a cheater.



probability of accepting a proof

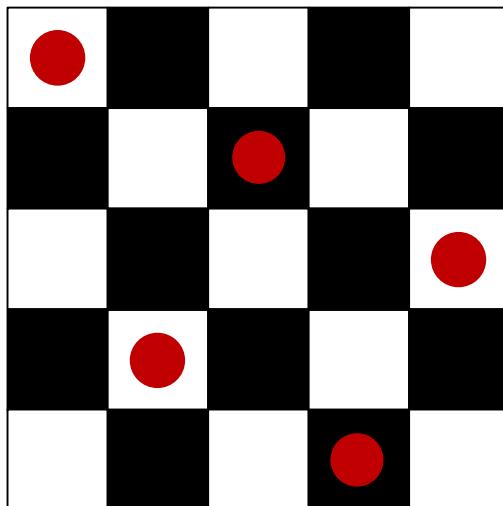
# ● Proofs and checks

deterministic / randomized

full / partial

classical / quantum

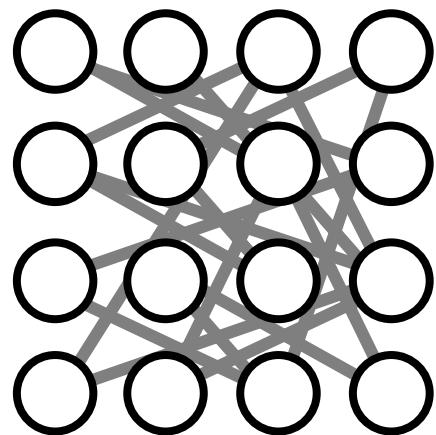
general / with promises



+ symmetries = 10.

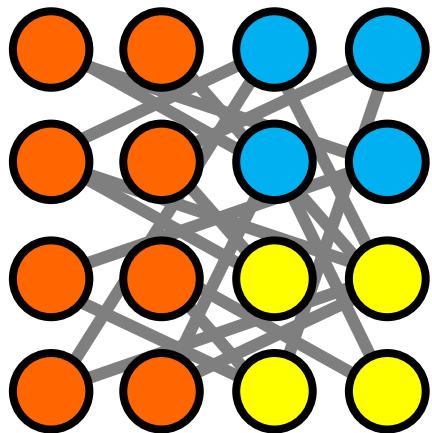
# ■ Quantum proofs for G3C

a “long” classical  
proof: the colors



# ■ Quantum proofs for G3C

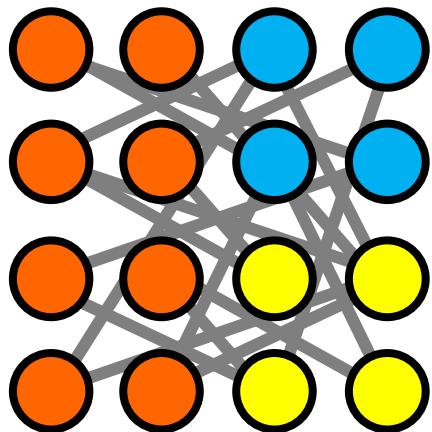
a “long” classical  
proof: the colors



# ■ Quantum proofs for G3C

a “long” classical proof: the colors

a “short” quantum proof: superpose

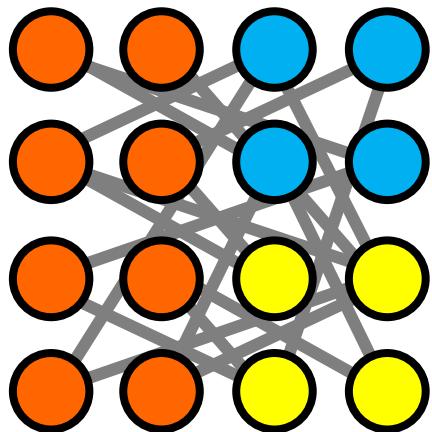


$$\frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle |\tilde{c}_i\rangle$$

# ■ Quantum proofs for G3C

a “long” classical proof: the colors

a “short” quantum proof: superpose



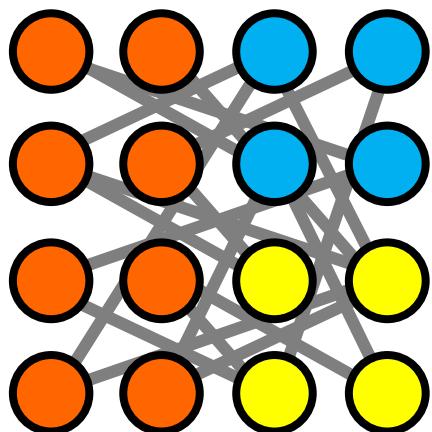
$$\frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle |\tilde{c}_i\rangle$$

How short is it?

# ■ Quantum proofs for G3C

a “long” classical proof: the colors

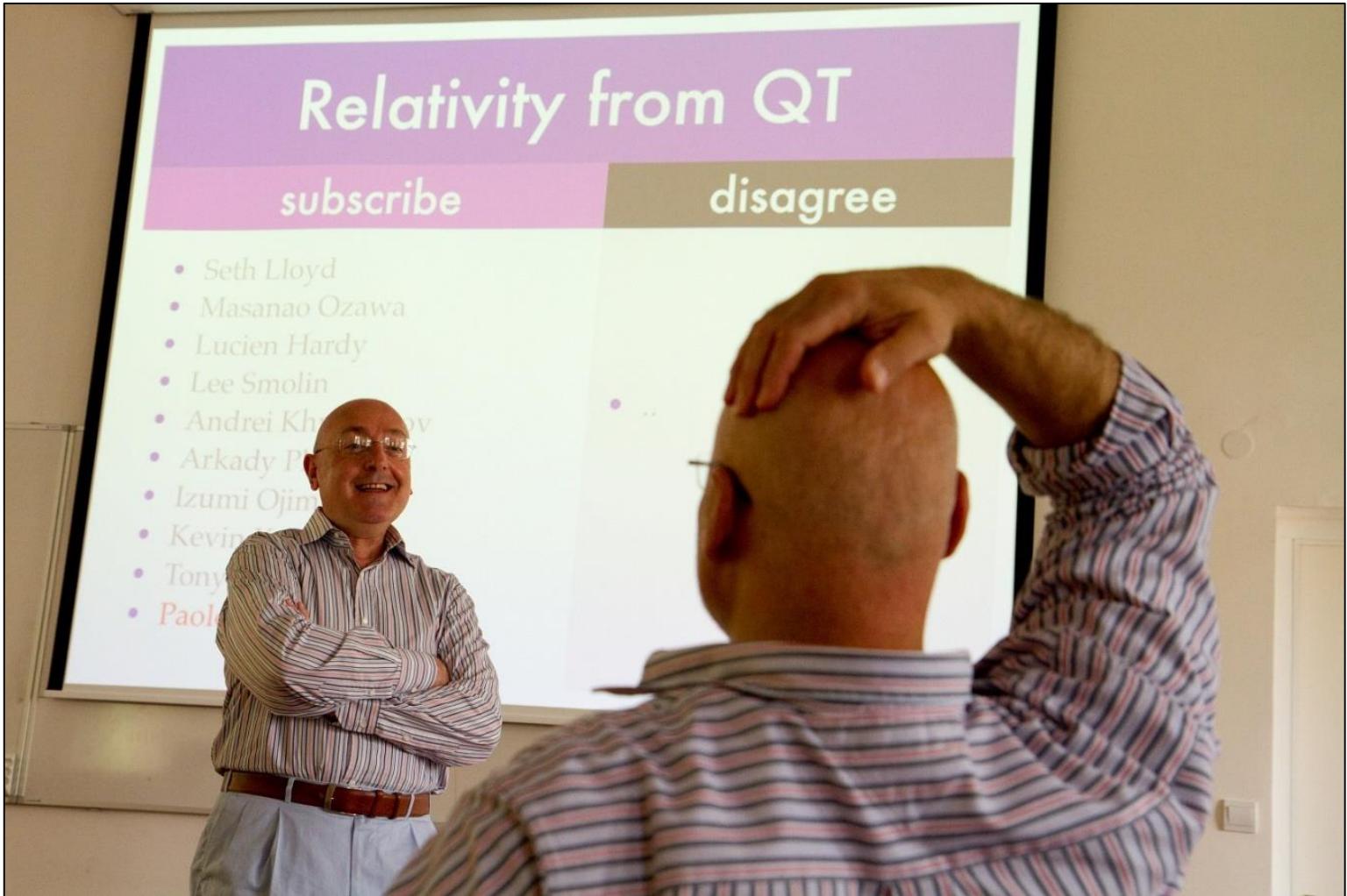
a “short” quantum proof: superpose



$$\frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle |\tilde{c}_i\rangle$$

Can you verify it?

# ■ Promise: unentanglement?



# ■ QMA(2): the power of unentanglement

2 short  
unentangled proofs

$$\frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle|c_i\rangle$$

$$\frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle|c_i\rangle$$

# ■ QMA(2): the power of unentanglement

checking 2 short  
unentangled proofs

feasibility  
compatibility

$$\frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle|c_i\rangle$$

$$\frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle|c_i\rangle$$

# ■ QMA(2): the power of unentanglement

checking 2 short  
unentangled proofs

$$\frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle|c_i\rangle$$

feasibility  
compatibility  
Fourier

$$\frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle|c_i\rangle$$


# ■ QMA(2): the power of unentanglement

[Blier & Tapp]  
[Beigi & Shor]  
[Aaronson et al.]  
[Le Gall et al.]

checking 2 short  
unentangled proofs

$$\frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle|c_i\rangle$$

feasibility  
compatibility  
Fourier

$$\frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle|c_i\rangle$$

state of the art  
2 log-size proofs, constant  $c-s$  gap

# ◆ Quantum problems & (quantum) proofs

is the ground  
energy  $< E$   
(or  $> F$ )?



# ◆ Quantum problems & (quantum) proofs

is the ground  
energy  $< E$   
(or  $> F$ )?

a proof?  
the g. s.  
verification?  
measurement



# ◆ Shorter proofs for a quantum problem

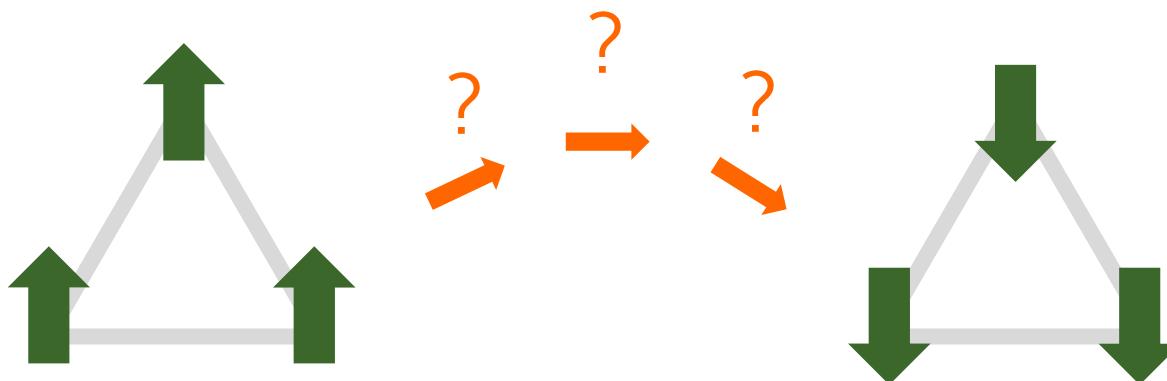
encode some quantum proof  
in a verifiable superposition?

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$



# A low energy traversal

ferro Hamiltonian  $\frac{1}{2} \sum_{i \neq j} (\mathbb{I} - Z_i Z_j)$



2

001  
010  
100  
011  
101  
110

0  
000  
111

1 & 2-local gates, keep  $E < 1.5$



# GSCON

[Sikora & Gharibian]

## traversing a ground space

H, in, out, bounds



a sequence of 1 & 2-local gates?



# GSCON

[Sikora & Gharibian]  
[Gosset, Mehta, Vidick]

## traversing a ground space

H, in, out, bounds



a sequence of 1 & 2-local gates?  
classical description

state of the art  
QCMA complete  
commuting Hamiltonians

# ◆ Shorter proofs for a quantum problem

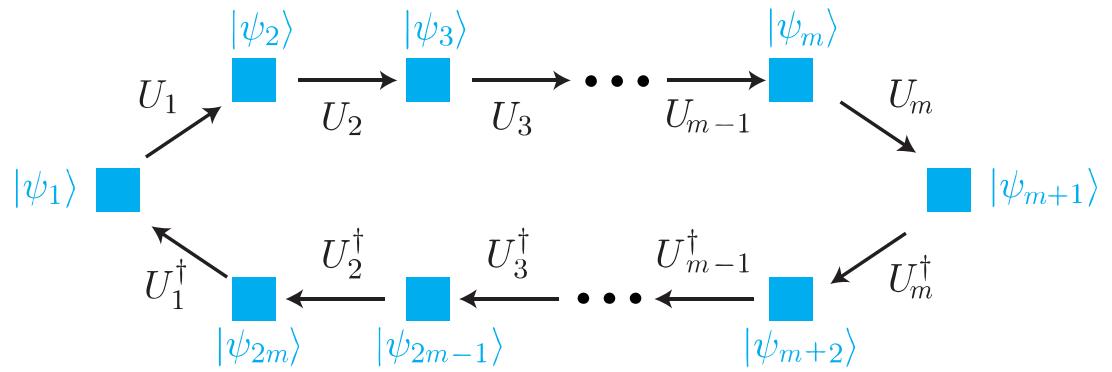
encode a quantum proof  
(a long sequence of states)  
in a verifiable superposition?

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$



# A GSCON traversal path as a superposition

a cycle



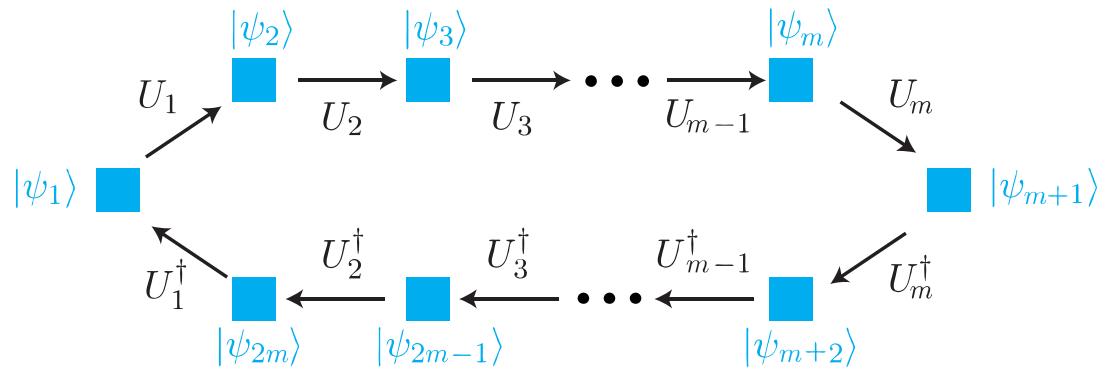
of states

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$



# A GSCON traversal path encoded in superpositions

a cycle



of states

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

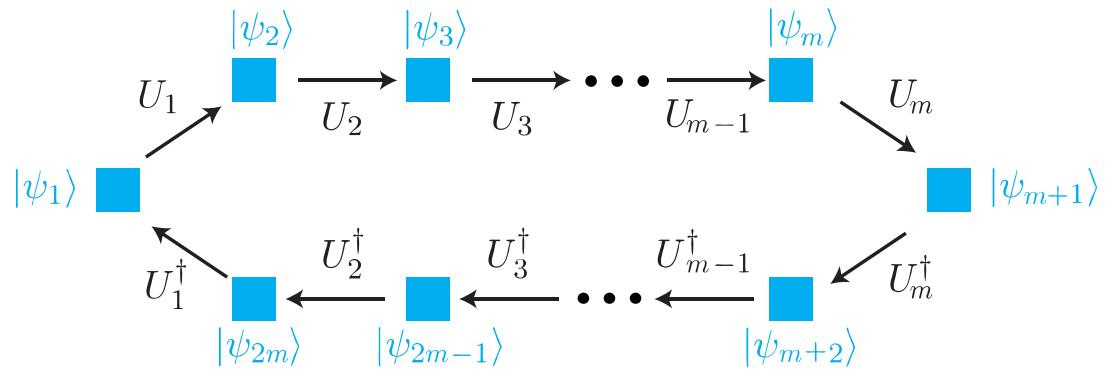
of gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



# A GSCON traversal path encoded in superpositions

a cycle



of states

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\sum_{i=1}^{2m} |i+1\rangle \langle i| \otimes U_i$$

shift invariant

of gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



# The testing of the path

2 copies of the cycle  
states & gates

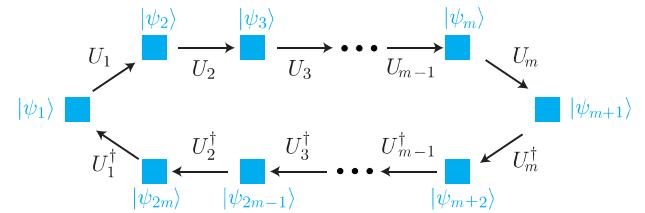
$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

consistency of  $U$ 's





# The testing of the path

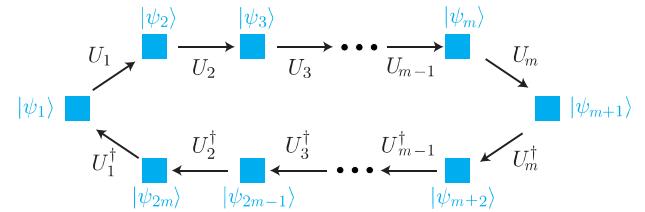
2 copies of the cycle  
states & gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



consistency of  $U$ 's, all of the  $U$ 's



# The testing of the path

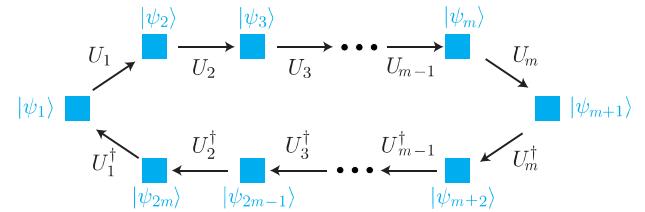
2 copies of the cycle  
states & gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



consistency of  $U$ 's, all of the  $U$ 's  
consistency of states



# The testing of the path

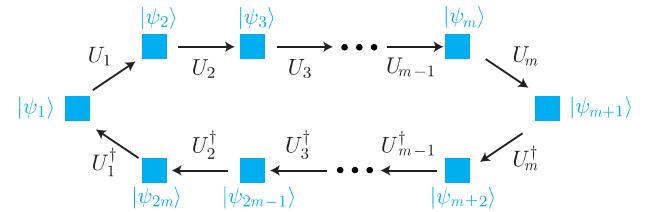
2 copies of the cycle  
states & gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



shift invariant

$$\sum_{i=1}^{2m} |i+1\rangle\langle i| \otimes U_i$$

consistency of  $U$ 's, all of the  $U$ 's  
consistency of states  
shift invariance



# The testing of the path

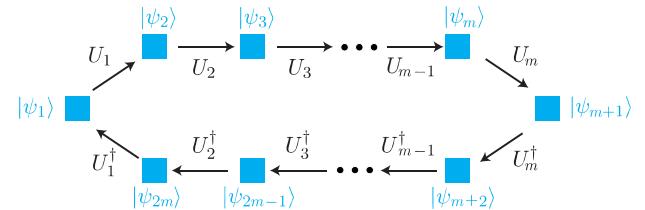
2 copies of the cycle  
states & gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



shift invariant

$$\sum_{i=1}^{2m} |i+1\rangle\langle i| \otimes U_i$$

consistency of  $U$ 's, all of the  $U$ 's  
consistency of states  
shift invariance

$$\sum_i \sum_j |i\rangle |j\rangle |u_i\rangle |\psi_j\rangle$$



# The testing of the path

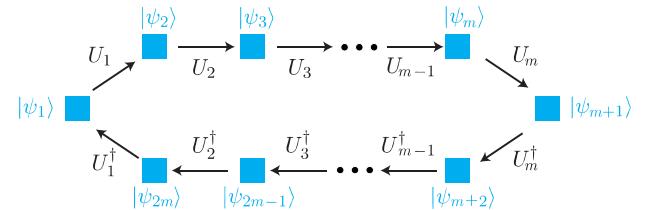
2 copies of the cycle  
states & gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



shift invariant

$$\sum_{i=1}^{2m} |i+1\rangle\langle i| \otimes U_i$$

consistency of  $U$ 's, all of the  $U$ 's

consistency of states

shift invariance

$$\sum_i \sum_j |i\rangle |j\rangle |u_i\rangle |\psi_j\rangle$$



# The testing of the path

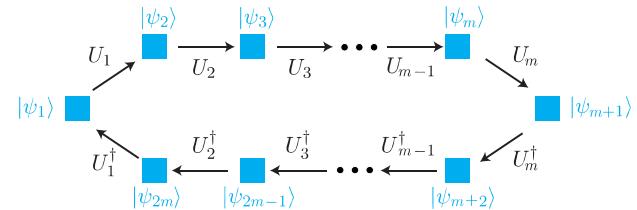
2 copies of the cycle  
states & gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



shift invariant

$$\sum_{i=1}^{2m} |i+1\rangle\langle i| \otimes U_i$$

consistency of  $U$ 's, all of the  $U$ 's  
consistency of states  
shift invariance

$$\sum_i |i\rangle |u_i\rangle |\psi_i\rangle$$



# The testing of the path

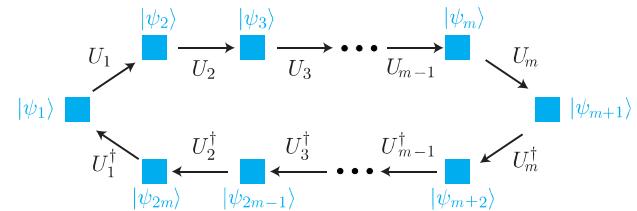
2 copies of the cycle  
states & gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



shift invariant

$$\sum_{i=1}^{2m} |i+1\rangle\langle i| \otimes U_i$$

consistency of  $U$ 's, all of the  $U$ 's  
consistency of states  
shift invariance

$$\sum_i |i\rangle |u_i\rangle |\psi_i\rangle$$



# The testing of the path

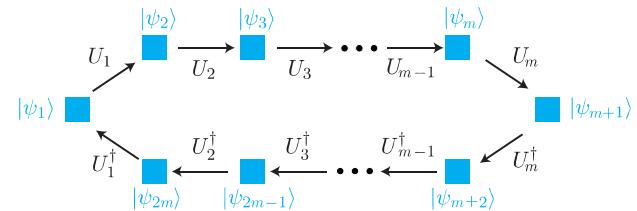
2 copies of the cycle  
states & gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



shift invariant

$$\sum_{i=1}^{2m} |i+1\rangle\langle i| \otimes U_i$$

consistency of  $U$ 's, all of the  $U$ 's  
consistency of states  
shift invariance

$$\sum_i |i\rangle |u_i\rangle U_i |\psi_i\rangle$$



# The testing of the path

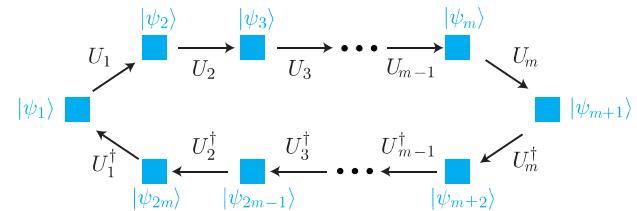
2 copies of the cycle  
states & gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



shift invariant

$$\sum_{i=1}^{2m} |i+1\rangle\langle i| \otimes U_i$$

consistency of  $U$ 's, all of the  $U$ 's  
consistency of states  
shift invariance

$$\sum_i |i\rangle |u_i\rangle U_i |\psi_i\rangle$$



# The testing of the path

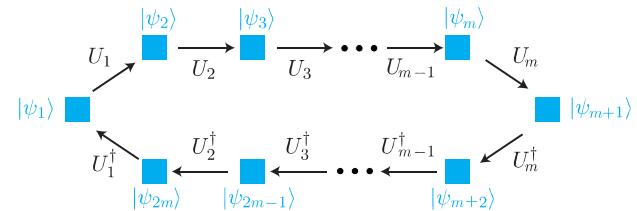
2 copies of the cycle  
states & gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



shift invariant

$$\sum_{i=1}^{2m} |i+1\rangle\langle i| \otimes U_i$$

consistency of  $U$ 's, all of the  $U$ 's  
consistency of states  
shift invariance

$$\sum_i |i\rangle U_i |\psi_i\rangle$$



# The testing of the path

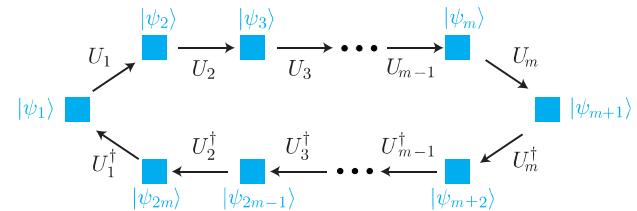
2 copies of the cycle  
states & gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



shift invariant

$$\sum_{i=1}^{2m} |i+1\rangle\langle i| \otimes U_i$$

consistency of  $U$ 's, all of the  $U$ 's  
consistency of states  
shift invariance

$$\sum_i |i\rangle |\psi_{i+1}\rangle$$



# The testing of the path

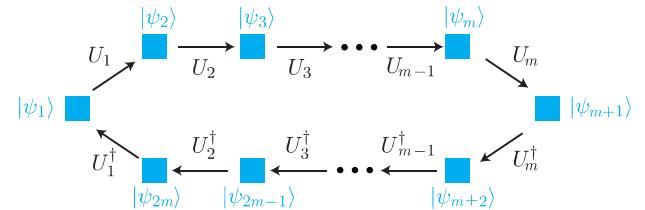
2 copies of the cycle  
states & gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



shift invariant

$$\sum_{i=1}^{2m} |i+1\rangle\langle i| \otimes U_i$$

consistency of  $U$ 's, all of the  $U$ 's  
consistency of states  
shift invariance

$$\sum_i |i+1\rangle |\psi_{i+1}\rangle$$



# The testing of the path

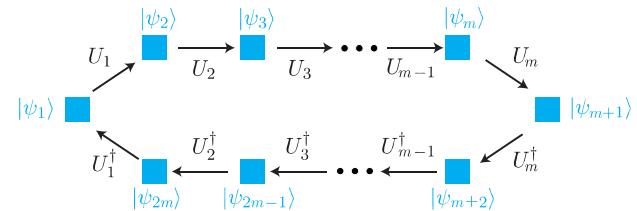
2 copies of the cycle  
states & gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



shift invariant

$$\sum_{i=1}^{2m} |i+1\rangle\langle i| \otimes U_i$$

consistency of  $U$ 's, all of the  $U$ 's  
consistency of states  
shift invariance

$$\sum_i |i+1\rangle |\psi_{i+1}\rangle$$



# The testing of the path

2 copies of the cycle  
states & gates

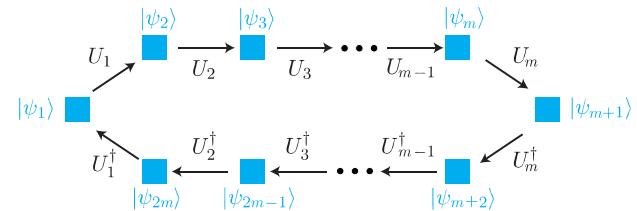
$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

consistency of  $U$ 's, all of the  $U$ 's  
consistency of states  
shift invariance



shift invariant

$$\sum_{i=1}^{2m} |i+1\rangle\langle i| \otimes U_i$$

$$\sum_i |i+1\rangle |\psi_{i+1}\rangle$$



# The testing of the path

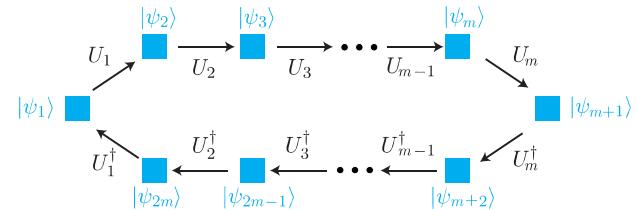
2 copies of the cycle  
states & gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



shift invariant

$$\sum_{i=1}^{2m} |i+1\rangle\langle i| \otimes U_i$$

consistency of  $U$ 's, all of the  $U$ 's  
consistency of states  
shift invariance  
low energy



# The testing of the path

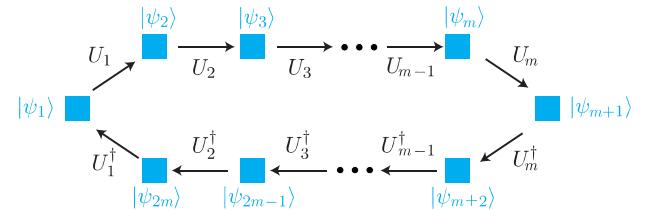
2 copies of the cycle  
states & gates

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$



shift invariant

$$\sum_{i=1}^{2m} |i+1\rangle\langle i| \otimes U_i$$

consistency of  $U$ 's, all of the  $U$ 's  
consistency of states  
shift invariance  
low energy, start & finish

# Reliability of the short $n^{\log m}$ unentangled proofs?



$1/\text{poly}(n)$   
A tiny  
chance  
to detect  
a cheater.



probability of accepting a proof

# Reliability of the short $n^{\log m}$ unentangled proofs?

Is it cool?



$1/\text{poly}(n)$   
A tiny  
chance  
to detect  
a cheater.

$m = n^{a>1}$   
For looong  
sequences.



probability of accepting a proof

# ↔ short<sup>un</sup>tangled proofs

Can we find **short** proofs for quantum problems, if we assume the proofs come from unentangled sources?

We consider a frustration-free variant of the QCMA-complete **GSCON** problem (ground state connectivity) for a system of size  $n$  with a superlinear size proof. We show that we can shorten this proof in QMA(2): there exists a two-copy, **unentangled** proof with length of order  $n$  (up to log factors), with an inverse polynomial completeness-soundness gap.

## of ground state connectivity

Libor Caha  
Daniel Nagaj  
Martin Schwarz

RCI Institute of Physics  
Slovak Academy of Sciences  
Bratislava  
Dahlem Center for COS  
Freie Universität Berlin

### 1 short proofs for NP

Blier & Tapp, Beigi  
graph 3-coloring  
NP-complete



a long proof  
the vertex colors

a short quantum proof  
a log-size superposition

$$\frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle |c_i\rangle$$

### 2 consistency checks

two unentangled copies  
do they match?  
do they have all the info?  
do they encode a solution?

the tests  
SWAP & measure: proper colors?  
Fourier: info about all vertices?

### 4 ground state connectivity

Gharibian & Sikora, Gosev et al.

traverse a low-energy subspace  
of a local Hamiltonian  
using local gates



a classical witness: the sequence of gates  
QCMA-complete: a successful traversal ~ an accepting quantum computation  
also QCMA-complete for commuting Hamiltonians

### 5 shorter GSCON proofs

Caha, Nagaj & Schwarz

shorten a long ( $m = n^2$ ) GSCON witness  
to size  $\sim n$  using two unentangled proofs

encode the gates  
in a superposition

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |u_i\rangle$$

encode the states  
in a cyclical sequence

$$\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$$

cyclically invariant under

$$\sum_{i=1}^{2m} |i+1\rangle \langle i| \otimes U_i$$

### 6 a probabilistic technique

apply the gates

$$\sum_i \frac{1}{\sqrt{2m}} |i\rangle |u_i\rangle \sum_j \frac{1}{\sqrt{2m}} |j\rangle |U_i| \psi_j \rangle$$

forget gates by projection

$$\sum_i \frac{1}{\sqrt{2m}} |i\rangle \langle i| \sum_j \frac{1}{\sqrt{2m}} |j\rangle |U_i| \psi_j \rangle$$

project on identical labels

$$\sum_i \frac{1}{\sqrt{2m}} |i\rangle \langle i| U_i | \psi_i \rangle$$

uncompute one label & shift

$$\sum_i \frac{1}{\sqrt{2m}} |i+1\rangle \langle i+1| U_i | \psi_i \rangle$$

check invariance

SWAP with the other copy  
1/poly success probability  
for honest Merlins

### 3 state of the art

Aaronson et al., Chen & Drucker,  
LeGall et al., Nakagawa & Nishimura

the tradeoffs  
proof length, prover #,  
& the completeness gap

constant gap

$\frac{1}{\sqrt{n}}$

$1/n$  gap

$\frac{\log n}{n}$

$\text{QMA}_{\log(2)} = \text{NP}^{\text{QP}}$   
no easy search

the quantum ETH  
 $\text{QMA}_n(2) \subseteq \text{QMA}_{n(\alpha^2)}$

### 7 a lot of testing

consistency (SWAP)  
do the witnesses match?

unique/uniform gates  
are all gates encoded?

sequence  
is the sequence invariant  
under probabilistic  
gate application?  
for the tests to pass well,  
the whole sequence  
must be represented

initialization/readout  
proper traversal start/end?  
low energy  
for all intermediate states?

the weakest test, which  
requires a frustration-free  
variant of GSCON

a pretty bad 1/poly gap  
between completeness  
and soundness

1712.07400

Blier & Tapp, A Quantum Characterization Of NP Complete Problems, Complexity, 21(2):499–510 (2012)  
Beigi, On QMA(2), Communications in Computer and Information Science, Part I, 426–436 (2013)  
Gharibian & Sikora, Ground State Connectivity of Local Hamiltonians, Communications in Computer and Information Science, Part I, 426–436 (2013)  
Aaronson et al., The Complexity of Approximating Local Hamiltonians, Communications in Computer and Information Science, Part I, 426–436 (2013)  
Jordan et al., Achieving perfect completeness in classical witness quantum computation, Quantum Information and Computation 12(9&10), 466–471 (2012)

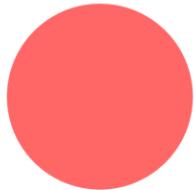
LeGall et al., On QMA protocols with 2 short quantum proofs, Quantum Information & Computation 12(9&10), 469–480 (2012)

Gharibian & Sikora, Ground State Connectivity of Local Hamiltonians, Communications in Computer and Information Science, Part I, 426–436 (2013)  
Gharibian, Mehta, & Vaidya, The Complexity of Ground State Connectivity for Commuting Hamiltonians, Communications in Computer and Information Science, Part I, 426–436 (2013)  
Aaronson et al., The Complexity of Approximating Local Hamiltonians, Communications in Computer and Information Science, Part I, 426–436 (2013)  
Jordan et al., Achieving perfect completeness in classical witness quantum computation, Quantum Information and Computation 12(9&10), 466–471 (2012)  
LeGall et al., On QMA protocols with 2 short quantum proofs, Quantum Information & Computation 12(9&10), 469–480 (2012)

A better low energy test?  
A better gap?

Counting  
problems?

Something  
QMA hard?



**Blier & Tapp, A Quantum Characterization Of NP**

Computational complexity, 21(3):499–510 (2012)

**Beigi, NP vs QMAlog(2)**

Quantum Information & Computation, 10(1&2):2 (2010)

**Aaronson et al., The power of unentanglement**

Theory of Computing, 5(1):1–42 (2009)

**LeGall et al., On QMA protocols with 2 short quantum proofs**

Quantum Information & Computation 12 (7/8), 589–600 (2012)



**Gharibian & Sikora, Ground State Connectivity of Local Hamiltonians**

ICALP 2015 Proceedings, Part I, 617–628 (2015)

**Gosset, Mehta, & Vidick, QCMA hardness**

**of ground space connectivity for commuting Hamiltonians**

Quantum 1, 16 (2017)

**Jordan et al., Achieving perfect completeness in**

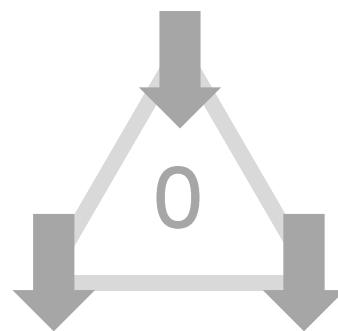
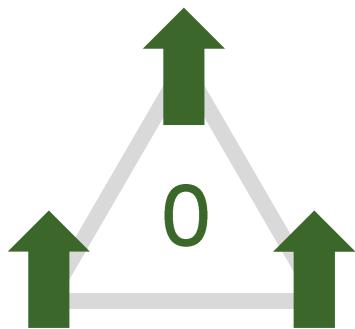
**classical-witness quantum Merlin-Arthur proof systems**

Quantum Information and Computation 12 (5/6), 461-471 (2012)z





# A low energy traversal



2

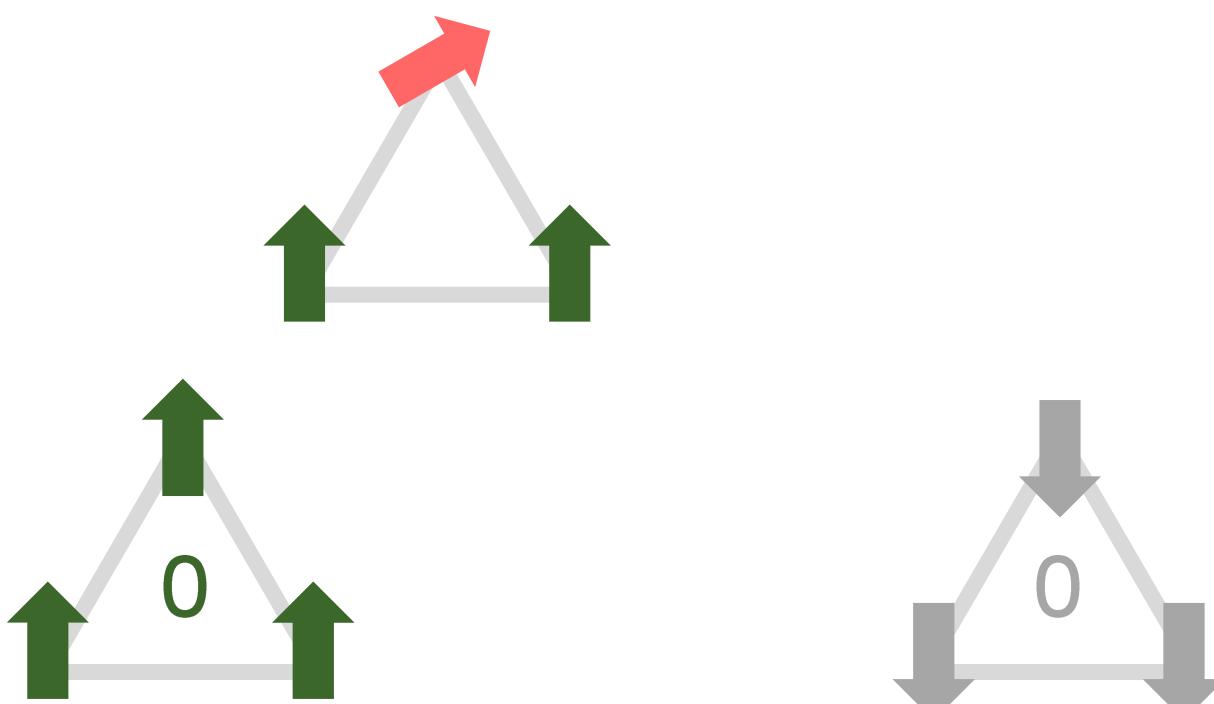
001  
010  
100  
011  
101  
110

0

000  
111



# A low energy traversal



2

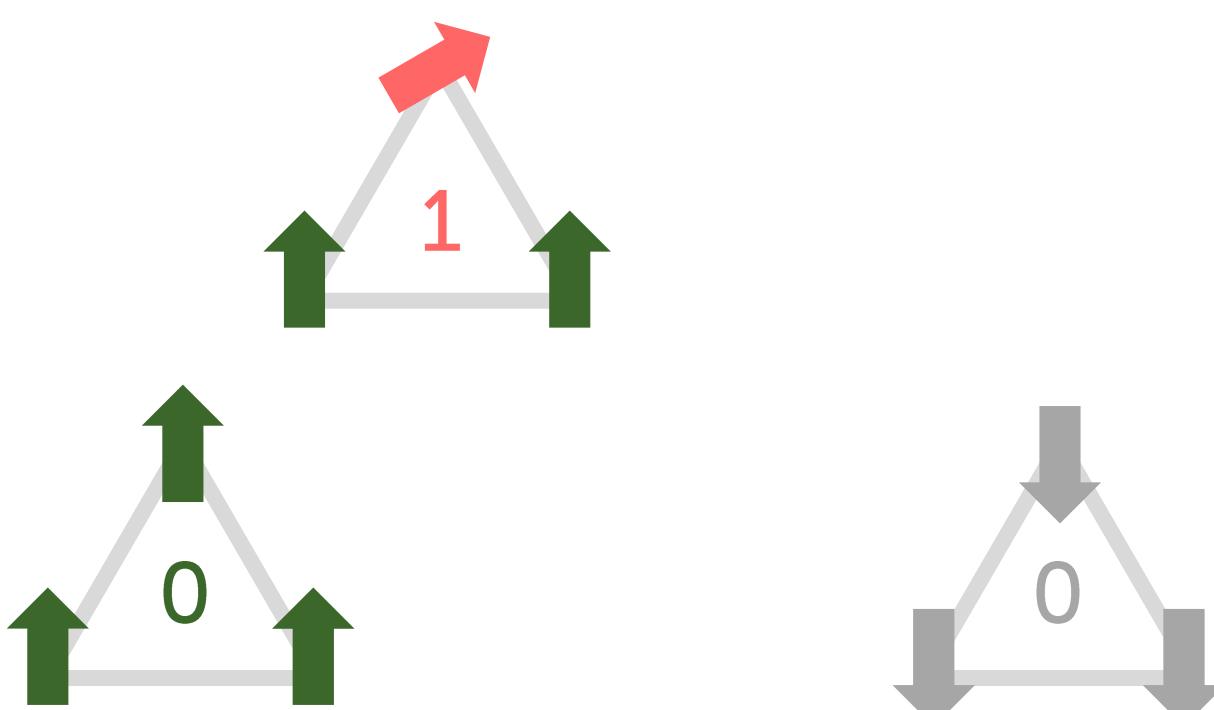
001  
010  
100  
011  
101  
110

0

000  
111



# A low energy traversal



2

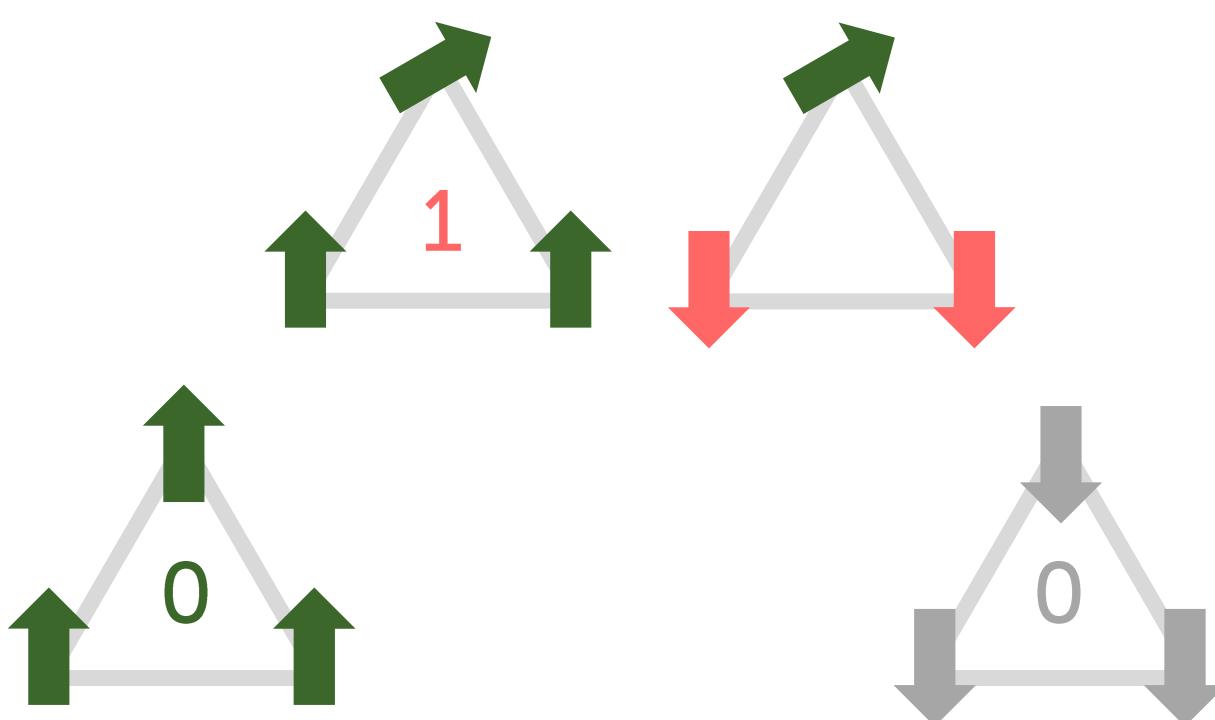
001  
010  
100  
011  
101  
110

0

000  
111



# A low energy traversal



2

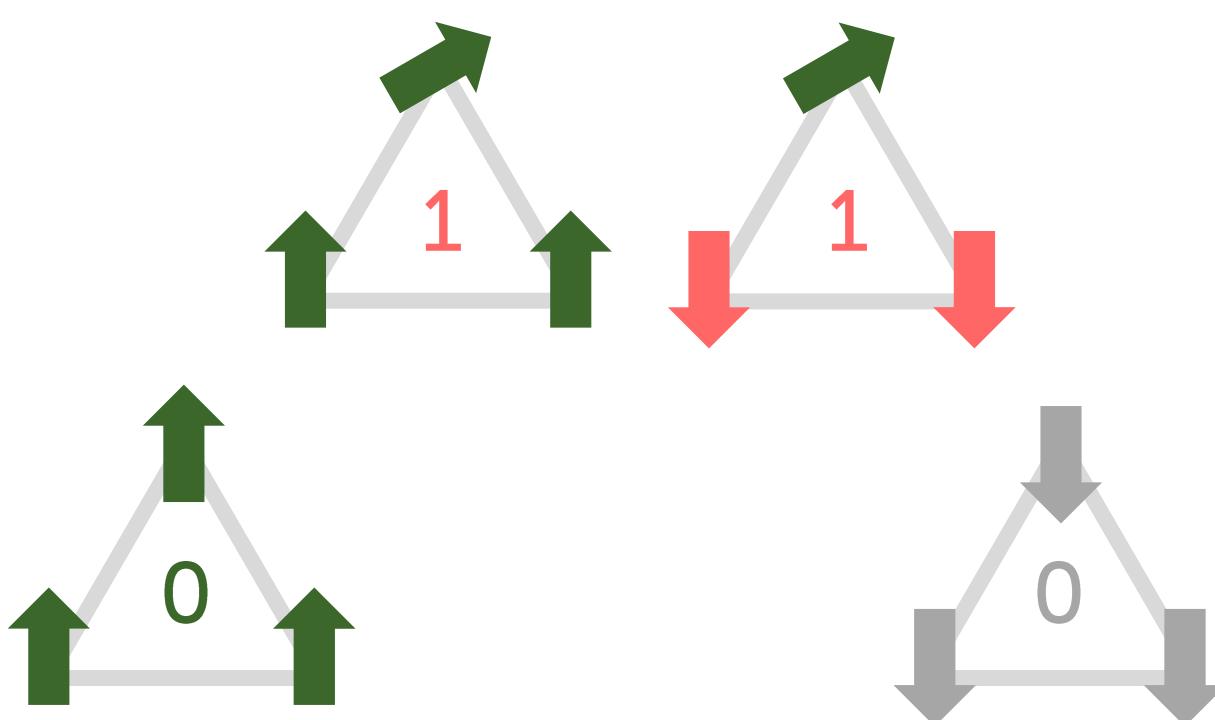
001  
010  
100  
011  
101  
110

0

000  
111



# A low energy traversal



2

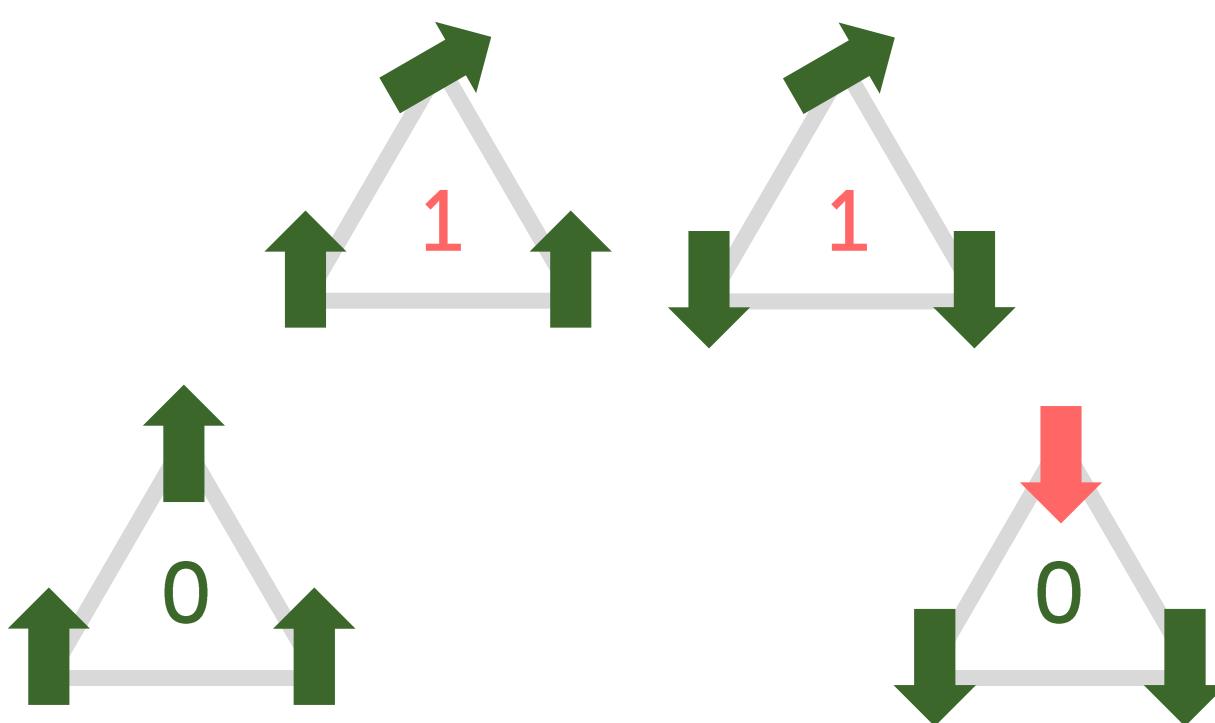
001  
010  
100  
011  
101  
110

0

000  
111



# A low energy traversal



2

001  
010  
100  
011  
101  
110

0

000  
111

