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

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

Quantum Inf Process (2018) 17:174
https://doi.org/10.1007/s11128-018-1944-4

CrossMark

Shorter unentangled proofs for ground state connectivity

Libor Caha[1] · **Daniel Nagaj**[1] · **Martin Schwarz**[2]

Received: 22 February 2018 / Accepted: 29 May 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

✉ Libor Caha
libor.caha@savba.sk

Daniel Nagaj
daniel.nagaj@savba.sk

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

2 Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany

Published online: 08 June 2018

Caha, Nagaj, Schwarz

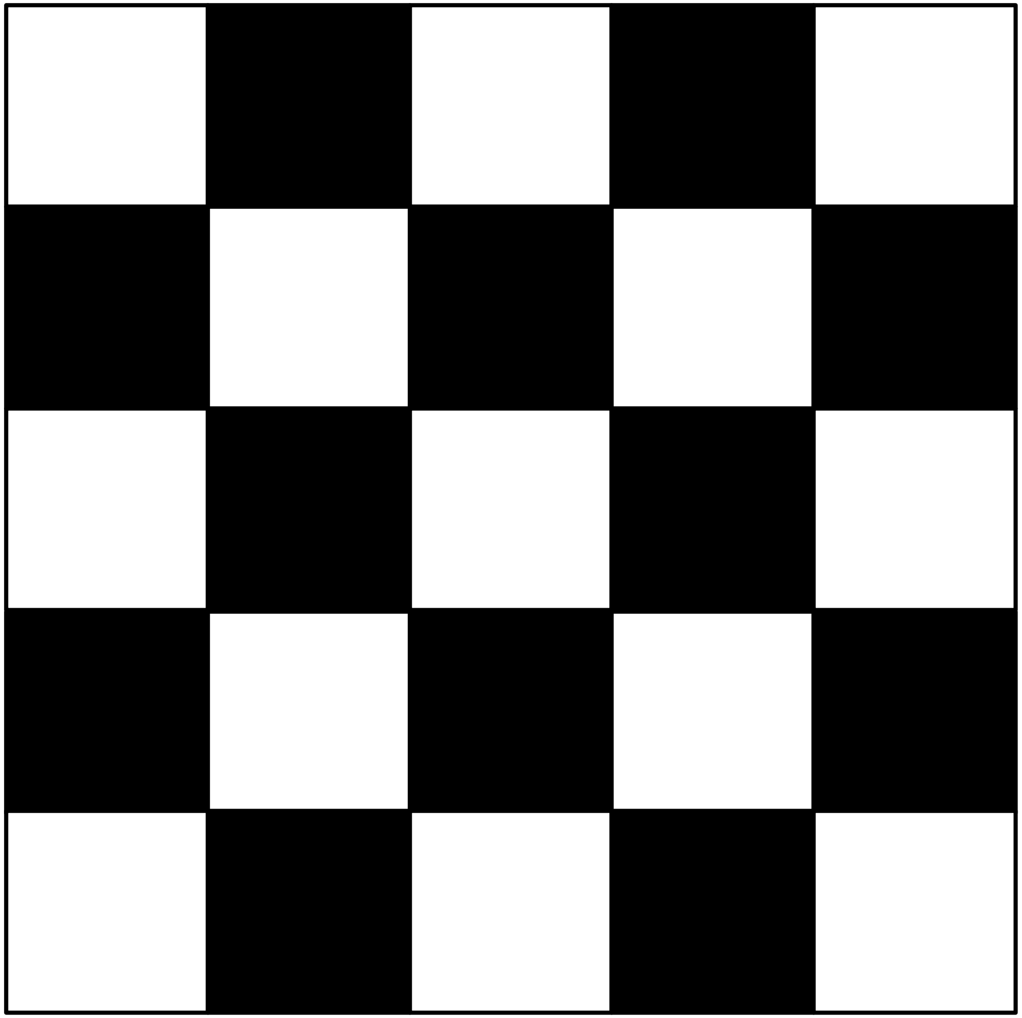
Quantum Information Processing 17:174 (2018)

1712.07400

DN's research has received funding from the People Programme (Marie Curie Actions) EU's 7th Framework Programme under REA grant agreement No. 609427. This research has been further co-funded by the Slovak Academy of Sciences. LC & DN have also received support from the Slovak Research & Development Agency grant QETWORK APVV-14-0878. MS thanks the Alexander von Humboldt Foundation for support.

- Puzzles and proofs

- 5 queens, > 10 solutions?

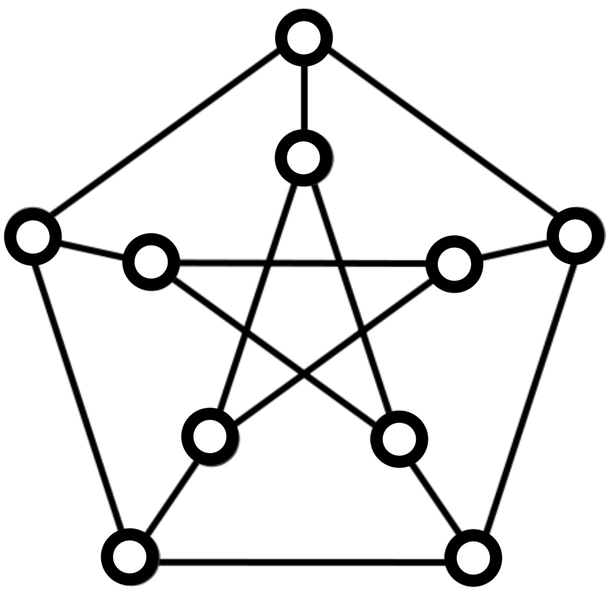


- NP: checkable proofs

traveling salesman: a list of cities

sudoku: fill the boxes with numbers

graph 3-coloring: vertex colors

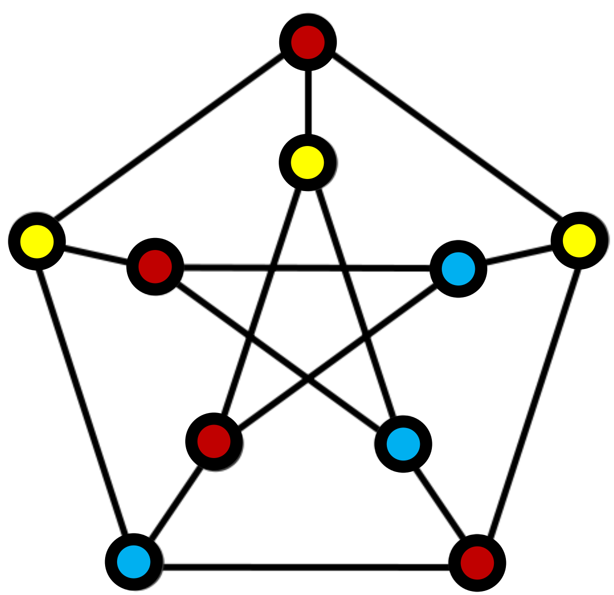


- NP: checkable proofs

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?

completeness (YES)

convince me

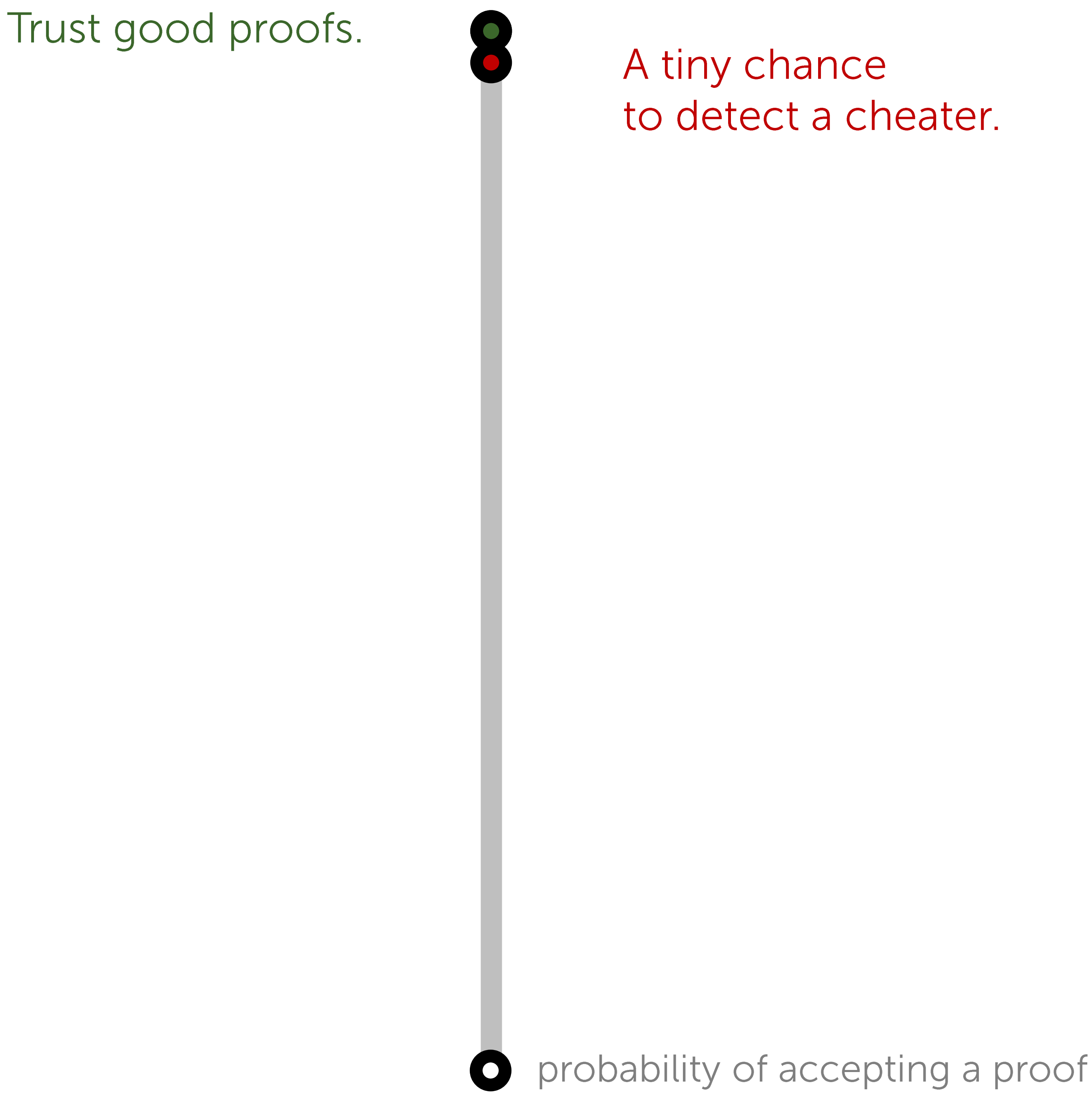
stay skeptical

soundness (NO)

Carefully verify!

MA

probability of accepting a proof


Trust good proofs.
A tiny chance
to detect a cheater.
probability of accepting a proof

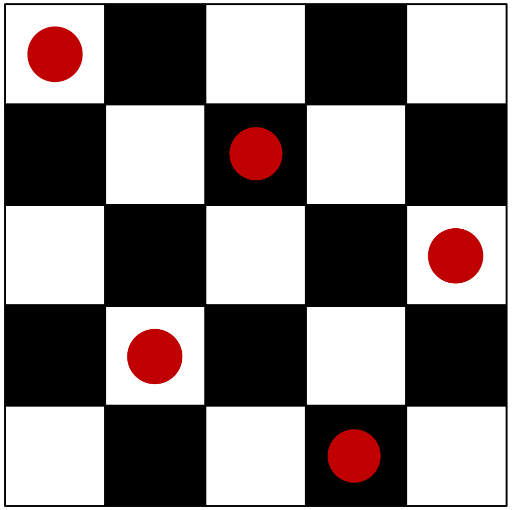
Proofs and checks

deterministic / randomized

full / partial

classical / quantum

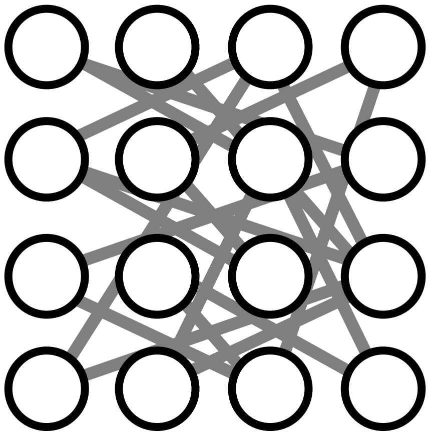
general / with promises



+ symmetries = 10.

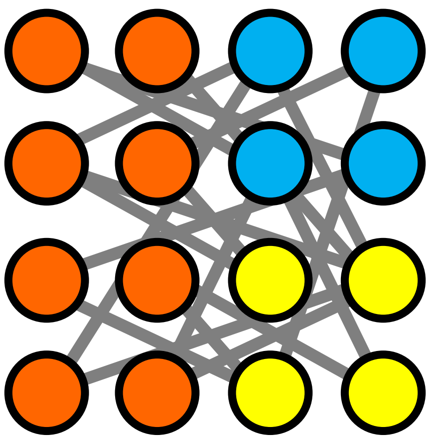
Quantum proofs for G3C

a “long” classical
proof: the colors



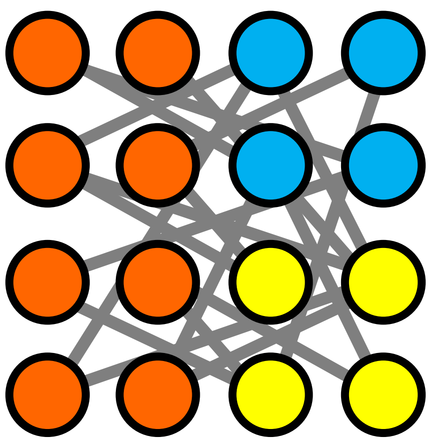
Quantum proofs for G3C

a "long" classical proof: the colors



Quantum proofs for G3C

a “long” classical proof: the colors

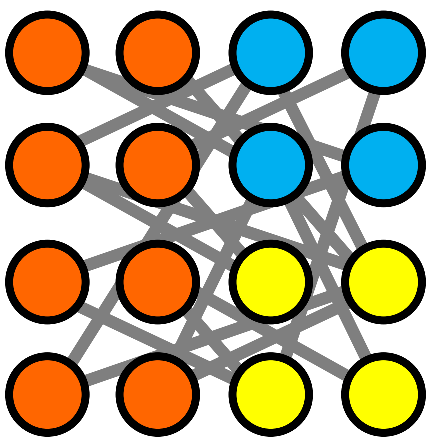


a “short” quantum proof: superpose

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

Quantum proofs for G3C

a "long" classical proof: the colors



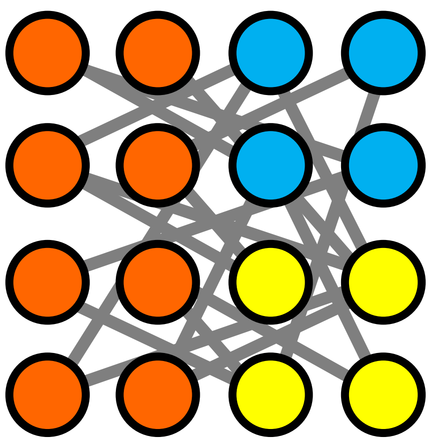
a "short" quantum proof: superpose

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

How short is it?

Quantum proofs for G3C

a “long” classical proof: the colors



a “short” quantum proof: superpose

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

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

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

$$\updownarrow$$

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

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

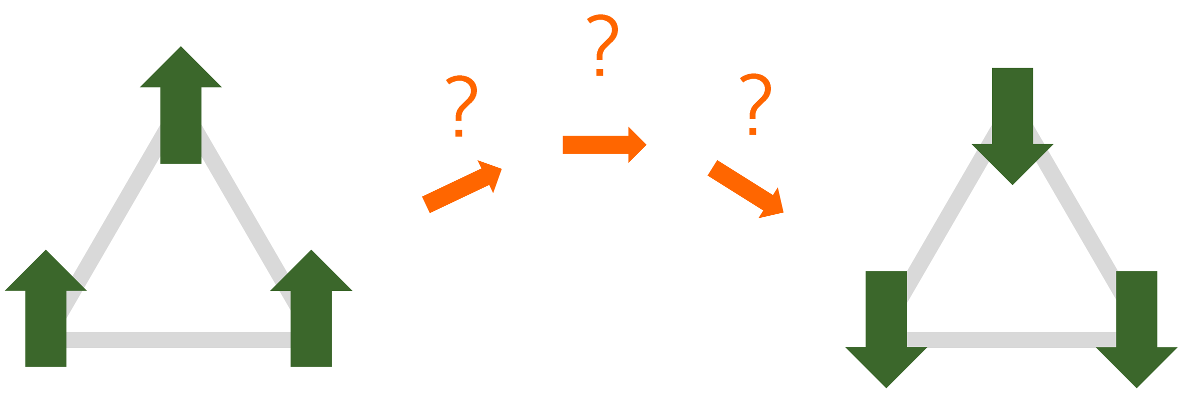
Shorter proofs for a quantum problem

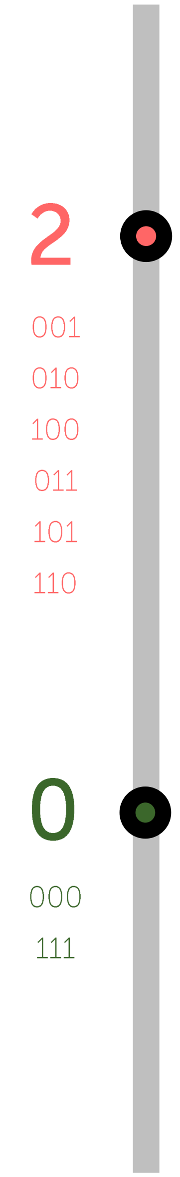
encode some quantum proof
in a verifiable superposition?

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

A low energy traversal

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





1 & 2-local gates, keep E < 1.5

GSCON traversing a ground space

[Sikora & Gharibian]

H, in, out, bounds

a sequence of 1 & 2-local gates?

GSCON traversing a ground space

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

H, in, out, bounds

a sequence of 1 & 2-local gates?

classical description

state of the art

QCMA complete

commuting Hamiltonians

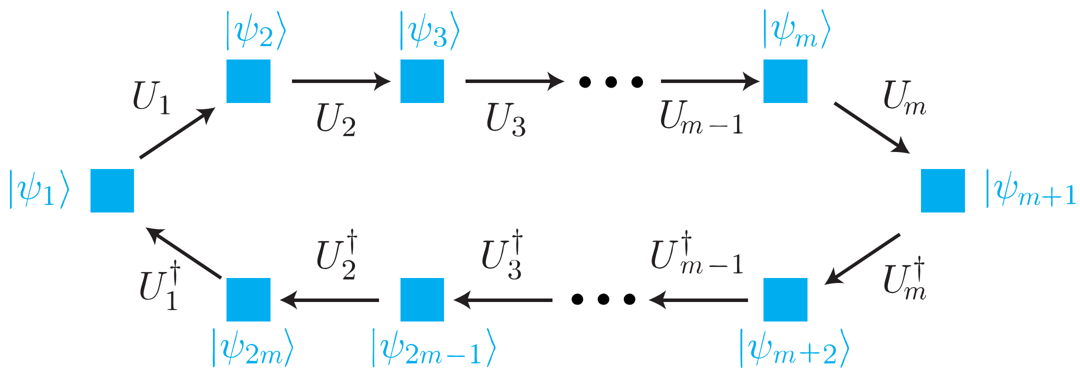
Shorter proofs for a quantum problem

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

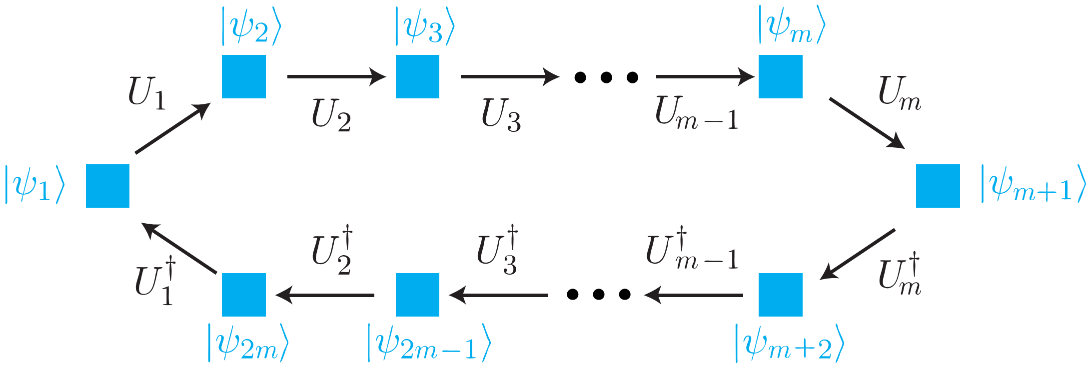


of states

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

A GSCON traversal path encoded in superpositions

a cycle

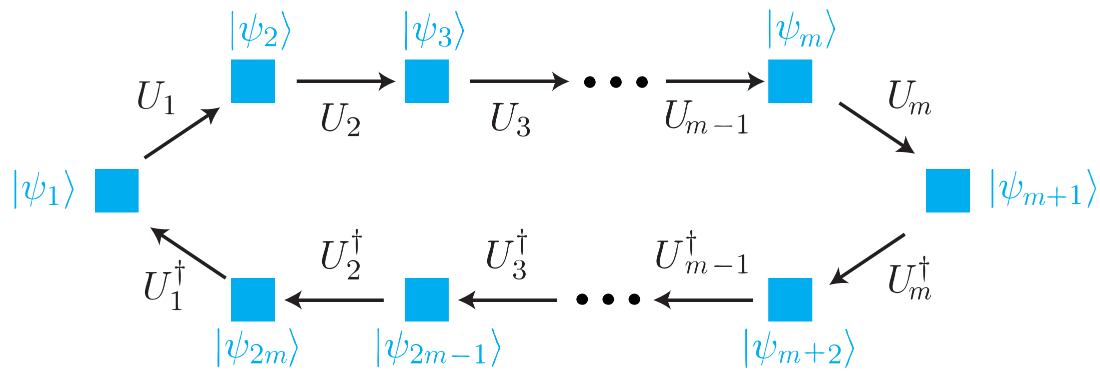


of states $\frac{1}{\sqrt{2m}} \sum_{i=1}^{2m} |i\rangle |\psi_i\rangle$

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

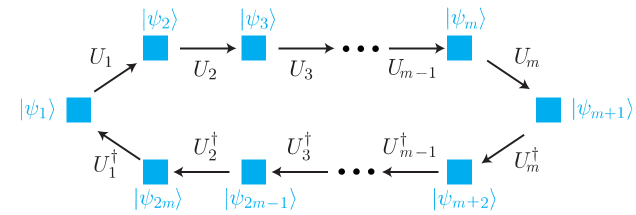
$$\sum_{i=1}^{2m} |i+1\rangle\langle i| \otimes U_i$$

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



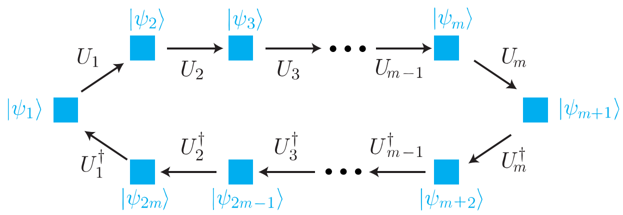
$$\frac{1}{\sqrt{2m}}\sum_{i=1}^{2m}|i\rangle|\psi_i\rangle \qquad \frac{1}{\sqrt{2m}}\sum_{i=1}^{2m}|i\rangle|u_i\rangle$$

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

consistency of U's

The testing of the path

2 copies of the cycle states & gates



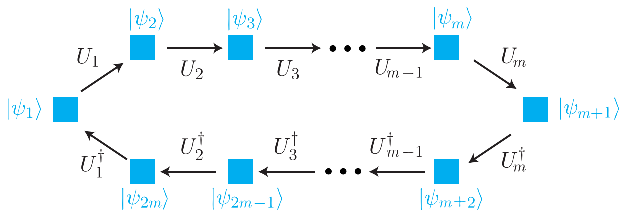
$$\frac{1}{\sqrt{2m}}\sum_{i=1}^{2m}|i\rangle|\psi_i\rangle \qquad \frac{1}{\sqrt{2m}}\sum_{i=1}^{2m}|i\rangle|u_i\rangle$$

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

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

The testing of the path

2 copies of the cycle states & gates



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

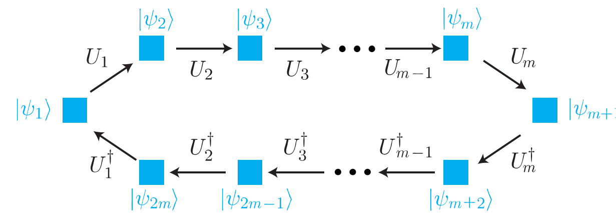
$$\frac{1}{\sqrt{2m}}\sum_{i=1}^{2m}|i\rangle|\psi_i\rangle \qquad \frac{1}{\sqrt{2m}}\sum_{i=1}^{2m}|i\rangle|u_i\rangle$$

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

consistency of states

The testing of the path

2 copies of the cycle states & gates



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

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

shift invariant

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

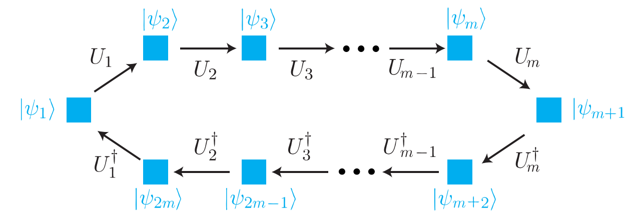
consistency of U's, all of the U's

consistency of states

shift invariance

The testing of the path

2 copies of the cycle states & gates



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

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

shift invariant

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

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

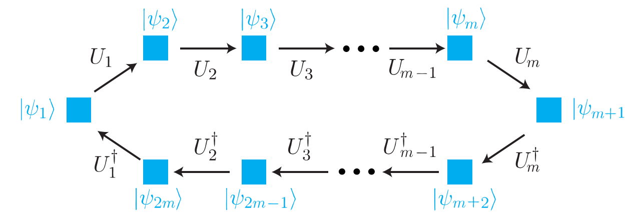
consistency of states

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



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

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

shift invariant

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

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

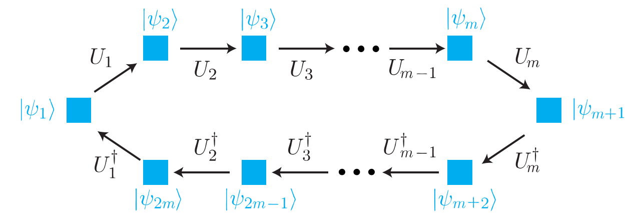
consistency of states

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



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

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

shift invariant

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

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

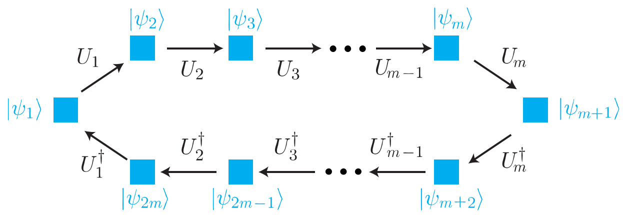
consistency of states

shift invariance

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

The testing of the path

2 copies of the cycle states & gates



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

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

shift invariant

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

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

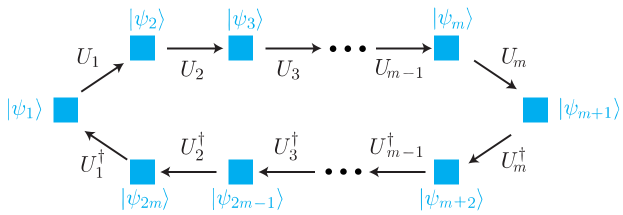
consistency of states

shift invariance

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

The testing of the path

2 copies of the cycle states & gates



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

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

shift invariant

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

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

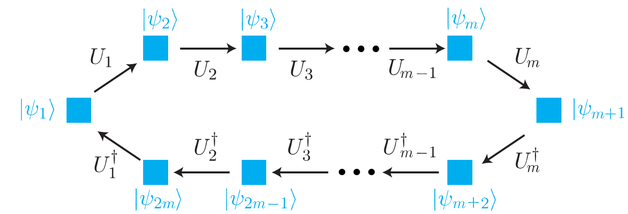
consistency of states

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



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

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

shift invariant

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

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

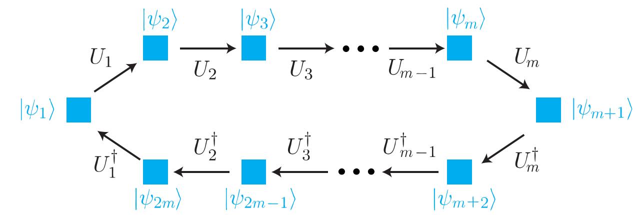
consistency of states

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



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

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

shift invariant

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

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

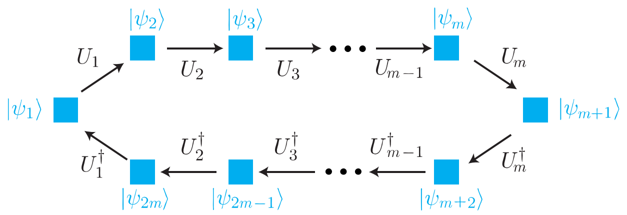
consistency of states

shift invariance

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

The testing of the path

2 copies of the cycle
states & gates



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

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

shift invariant

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

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

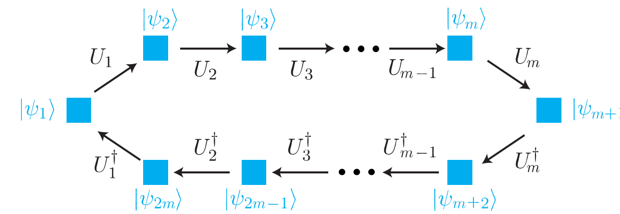
consistency of states

shift invariance

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

The testing of the path

2 copies of the cycle states & gates



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

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

shift invariant

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

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

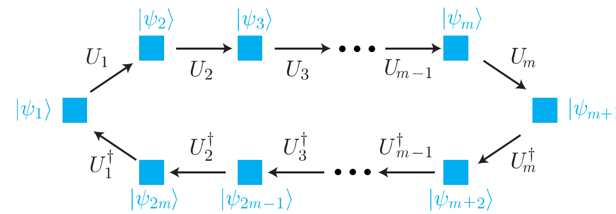
consistency of states

shift invariance

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

The testing of the path

2 copies of the cycle states & gates



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

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

shift invariant

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

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

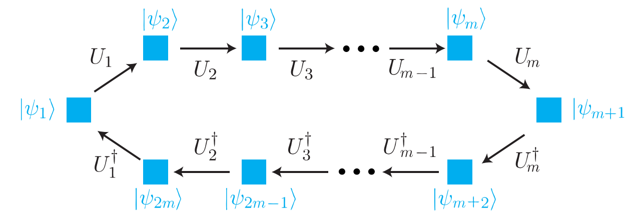
consistency of states

shift invariance

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

The testing of the path

2 copies of the cycle states & gates



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

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

shift invariant

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

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

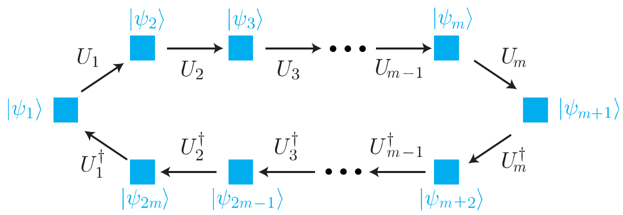
consistency of states

shift invariance

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

The testing of the path

2 copies of the cycle states & gates



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

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

shift invariant

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

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

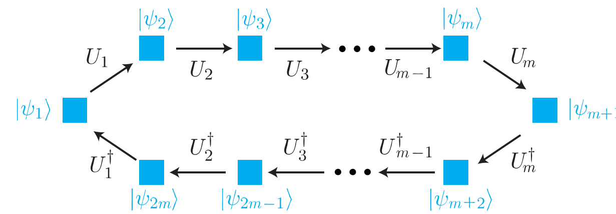
consistency of states

shift invariance

low energy

The testing of the path

2 copies of the cycle states & gates



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

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

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
$n \log m$
of the short
unentangled
proofs?

1/poly(n)

A tiny
chance
to detect
a cheater.

probability of accepting a proof

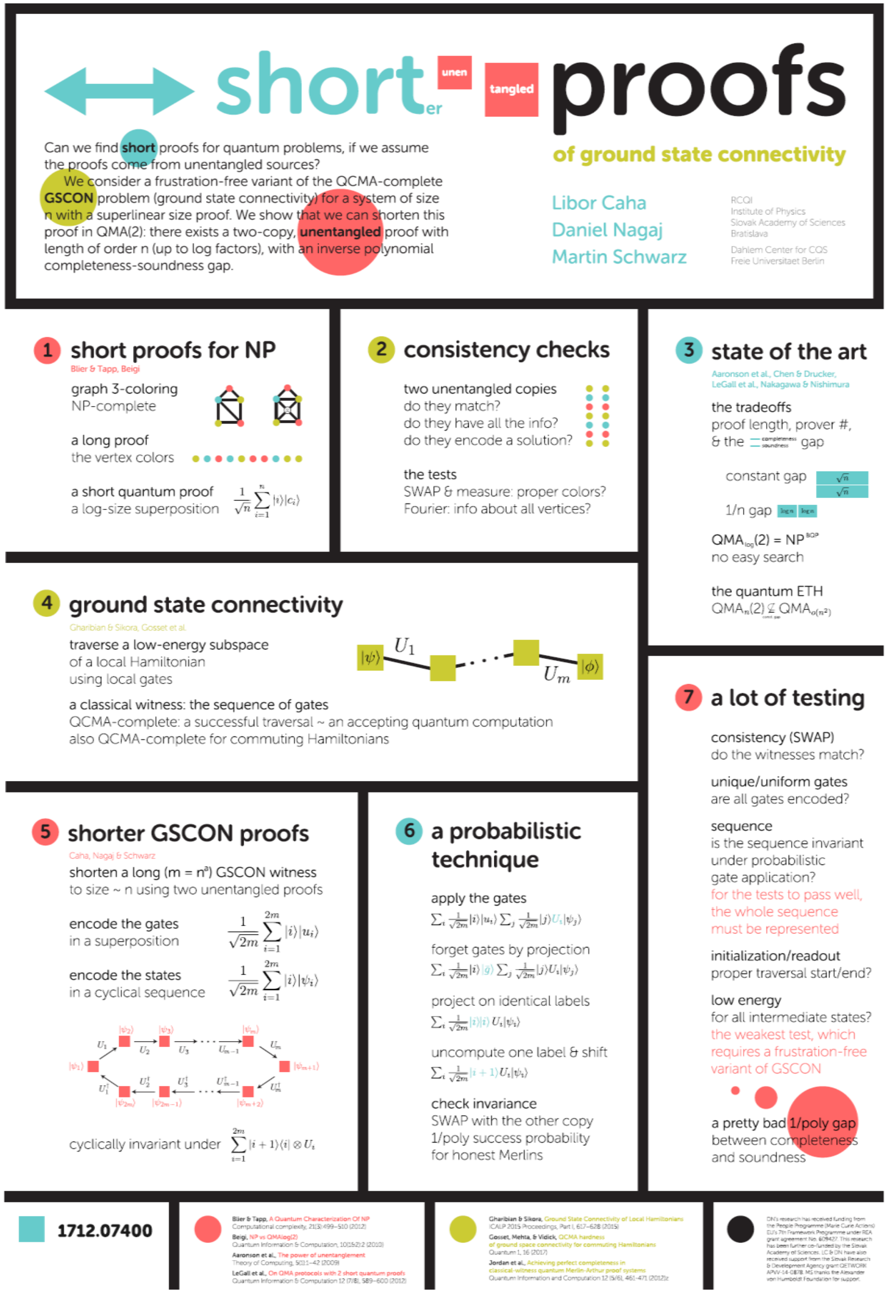
Reliability of the short ($n \log m$) unentangled proofs?

Is it cool?

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

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

probability of accepting a proof



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)

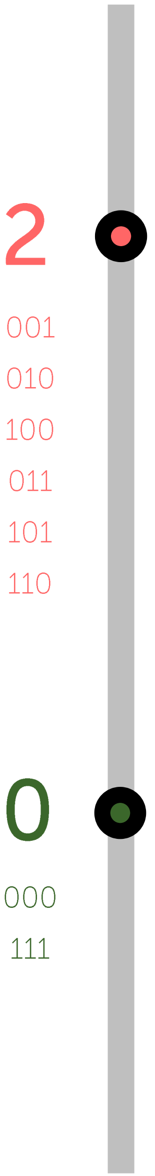
LeGall et al., On QMA protocols with 2 short quantum proofs
Quantum Information & Computation 12 (7/8), 589–600 (2012)

Gharibian & Sikora, Ground State Connectivity of Local Hamiltonians
ICALP 2015 Proceedings, Part I, 617–628 (2015)

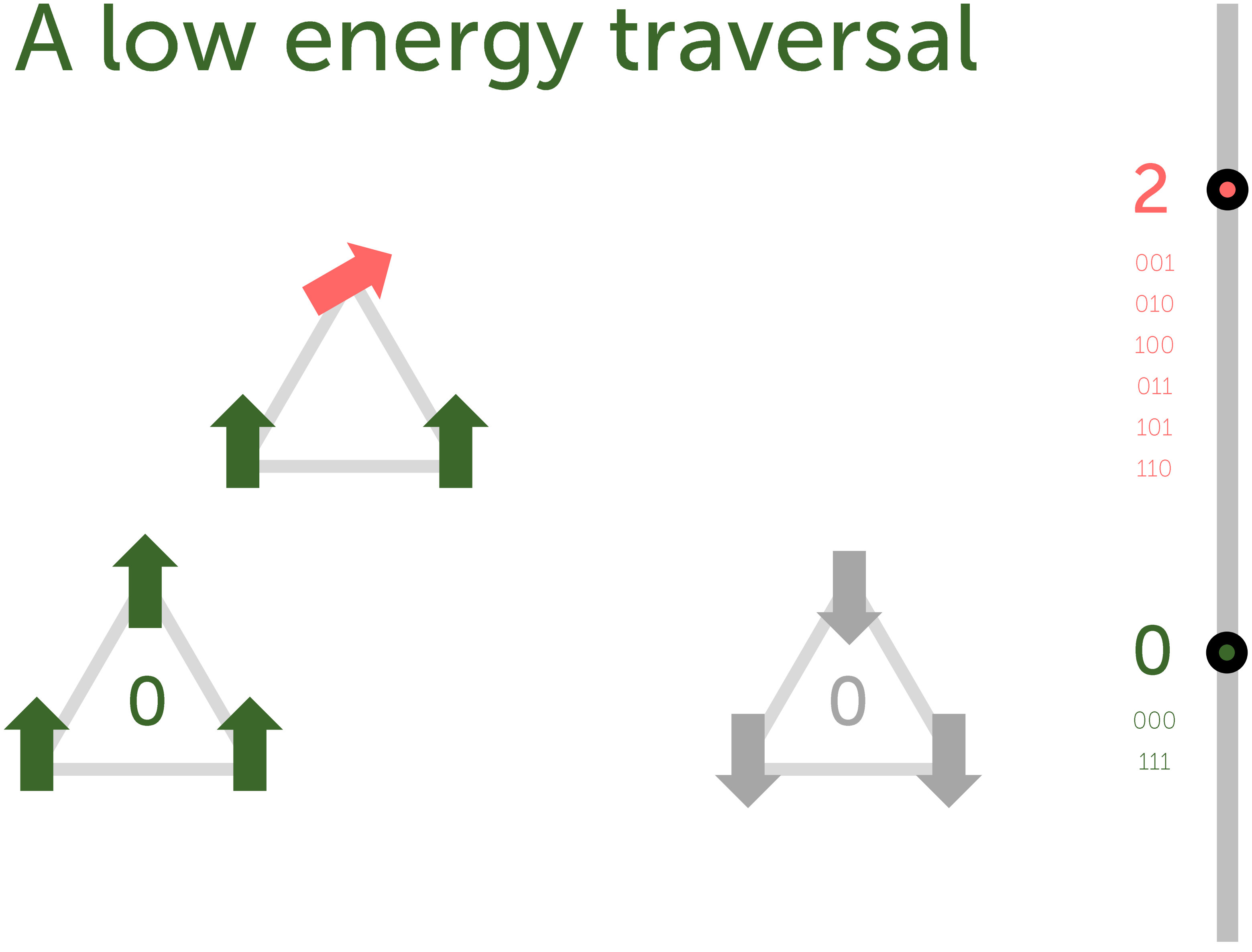
Gosset, Mehta, & Vidick, QCMA hardness
of ground space connectivity for commuting Hamiltonians
Quantum 1, 16 (2017)

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

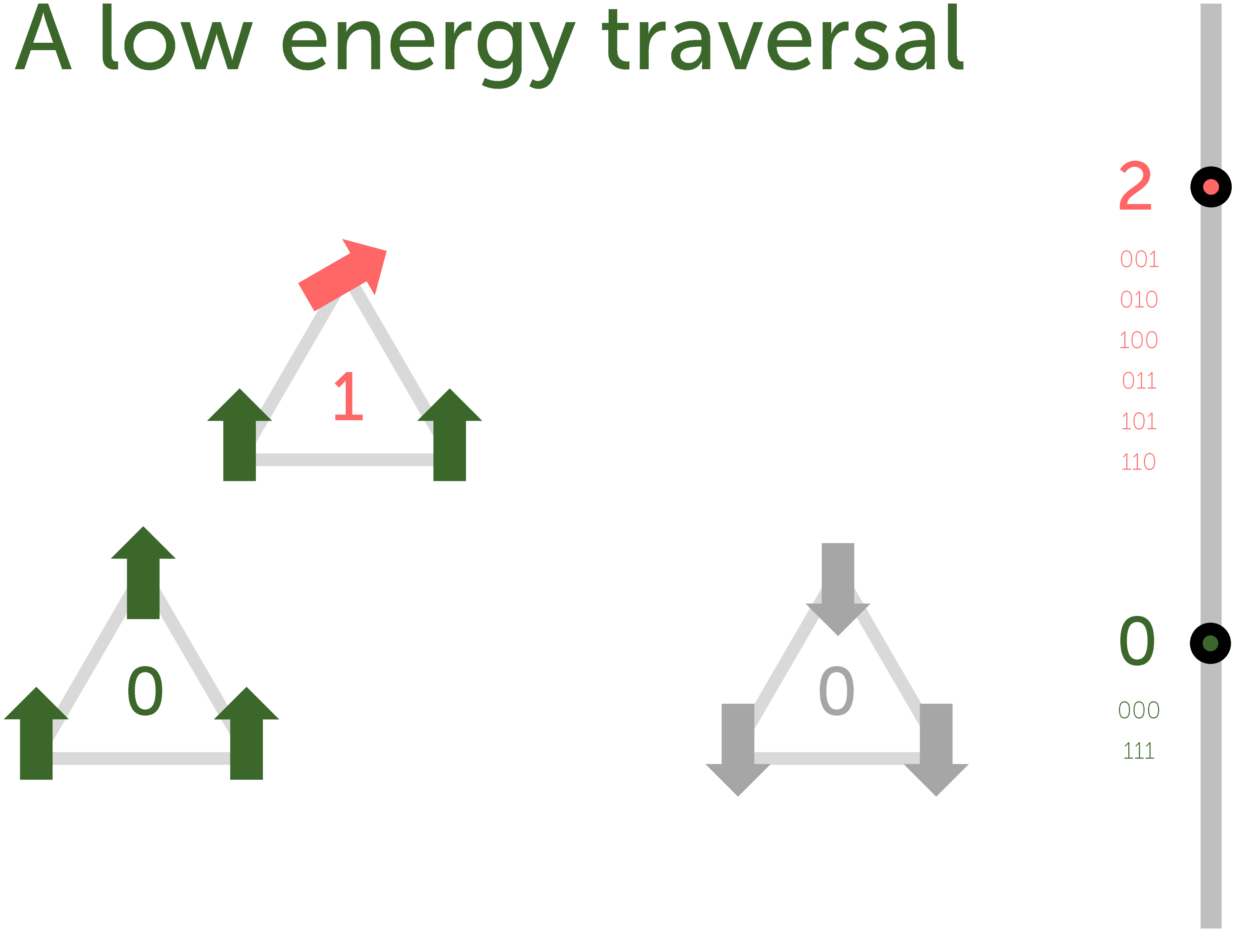
A low energy traversal



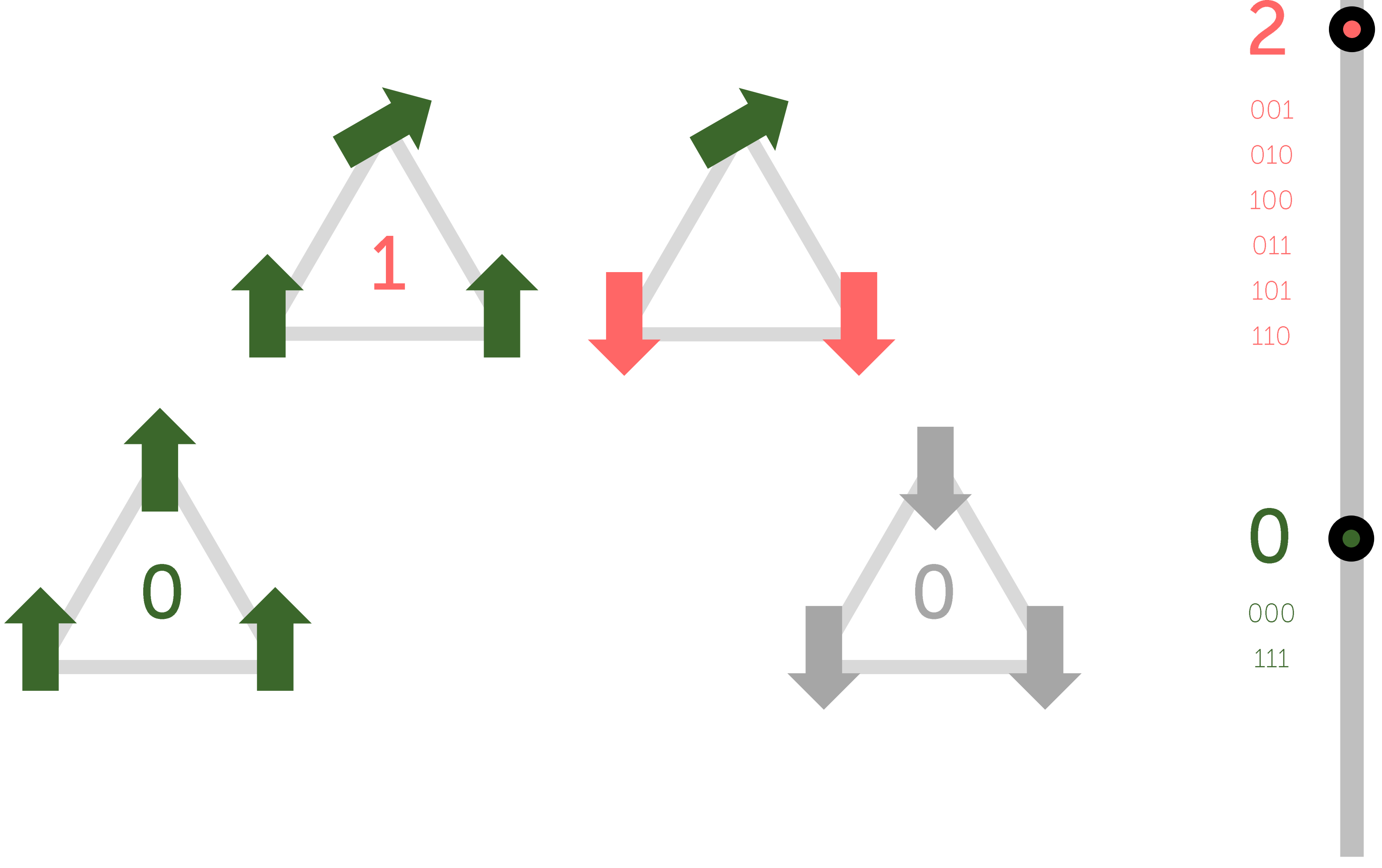
A low energy traversal



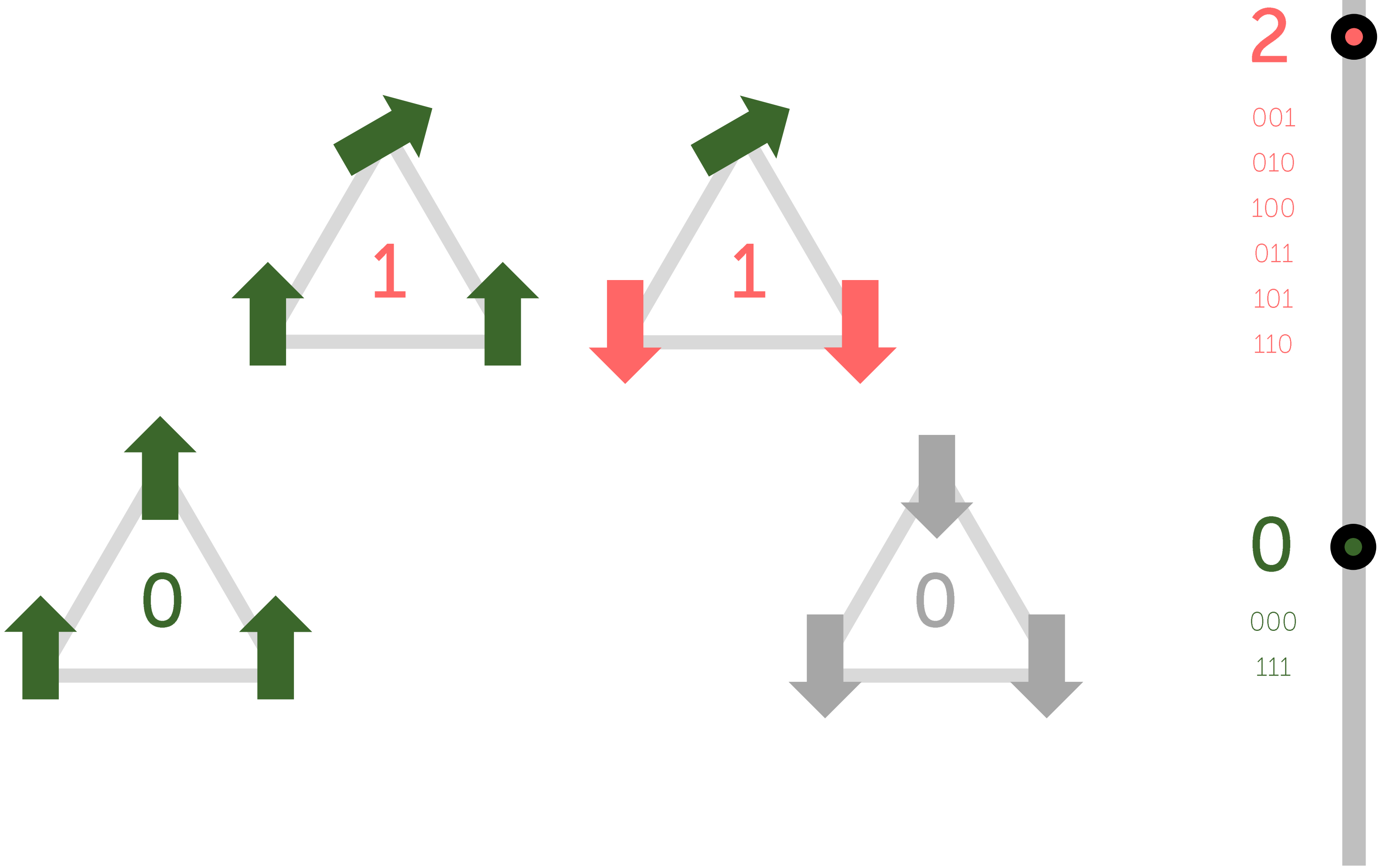
A low energy traversal



A low energy traversal



A low energy traversal



A low energy traversal