QIP 2013
Beijing

QIP 2013
Beijing

towards perfect completeness in QMA

Stephen P. Jordan
NIST Gaithersburg

Hirotada Kobayashi
NII Tokyo

François Le Gall
University of Tokyo

Harumichi Nishimura
Nagoya University

Daniel Nagaj
University of Vienna

QIP 2013
Beijing

arXiv: 1111.5306v2
arXiv: 1210.1290

towards perfect completeness in QMA

QIP 2013
Beijing

1 what it means to be really convincing

2 classical witnesses $QCMA_1$

3 a few EPR's

$QMA_1^{c.EPR}$

$QIP_1(2)$

1 The MA protocol

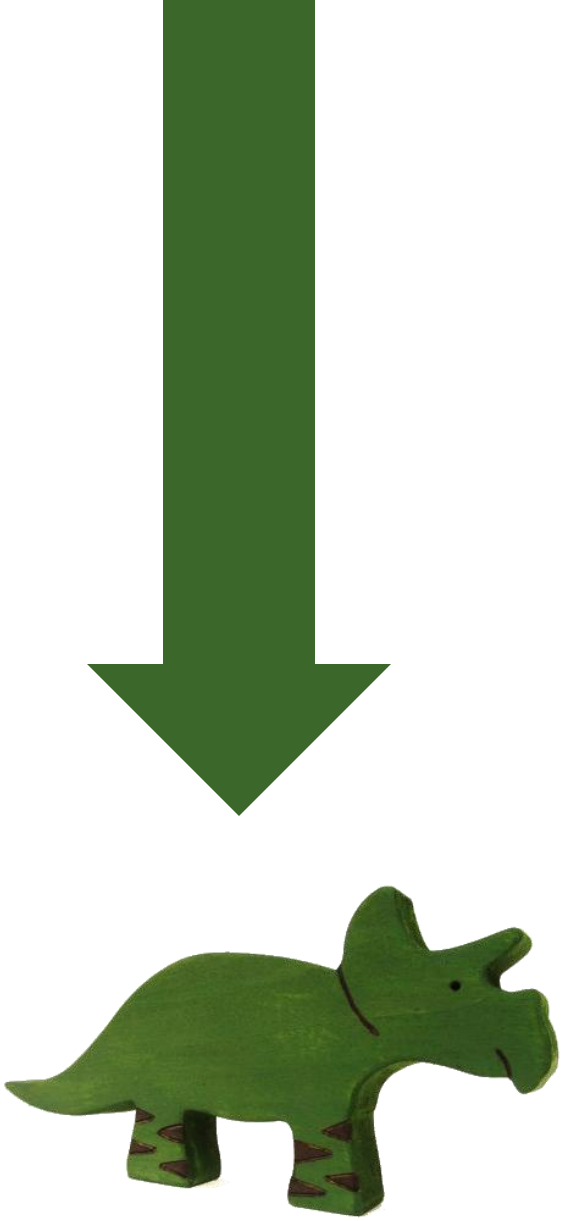
Did dinosaurs exist?

triceratops

?

1 The MA protocol

Did dinosaurs exist?

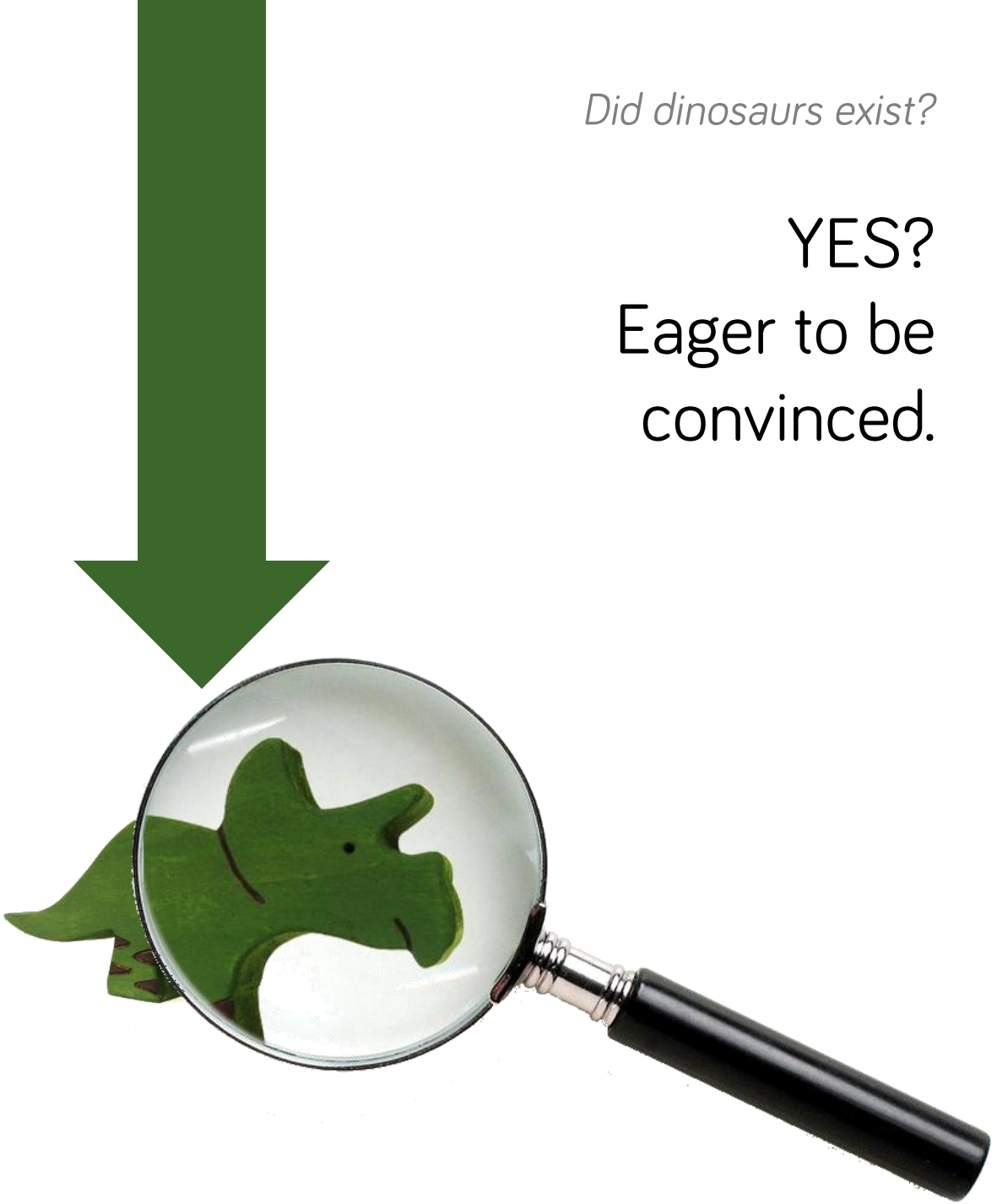


[wooden animals: Imagination Kids Toys]

1 The MA protocol

Did dinosaurs exist?

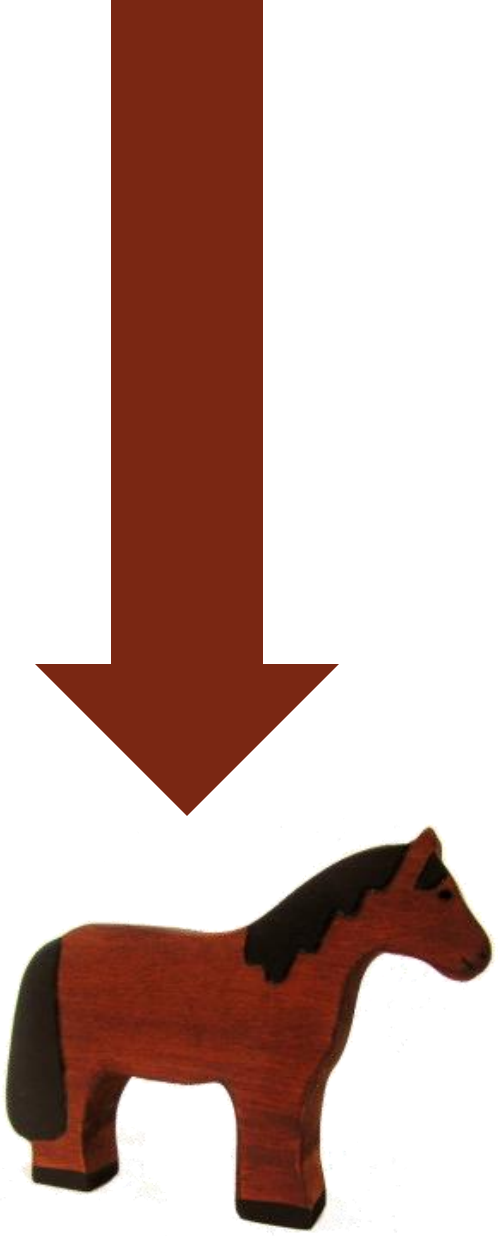
YES?
Eager to be convinced.



[magnifying glass: hillllllall]

1 The MA protocol

Recognizing fakes?



1 The MA protocol

Recognizing fakes?

NO?
Don't be
fooled
easily.

1 Probabilistic checks

Sometimes reject a genuine proof?

Accept a fake?

1 Perfect completeness

Never reject
a genuine proof?

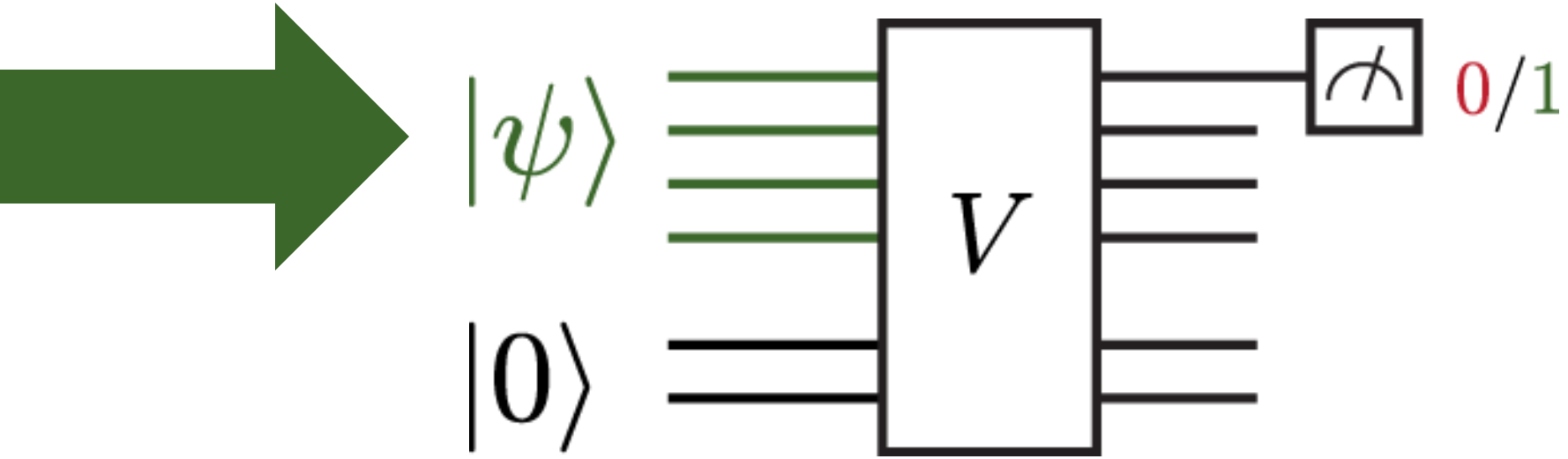
YES?
Accept some
proof without
any doubt.

NO?
Still don't get fooled easily.

YES?
Accept some proof without any doubt.

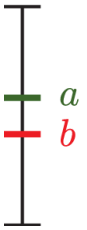
perfect completeness

1 The QMA protocol

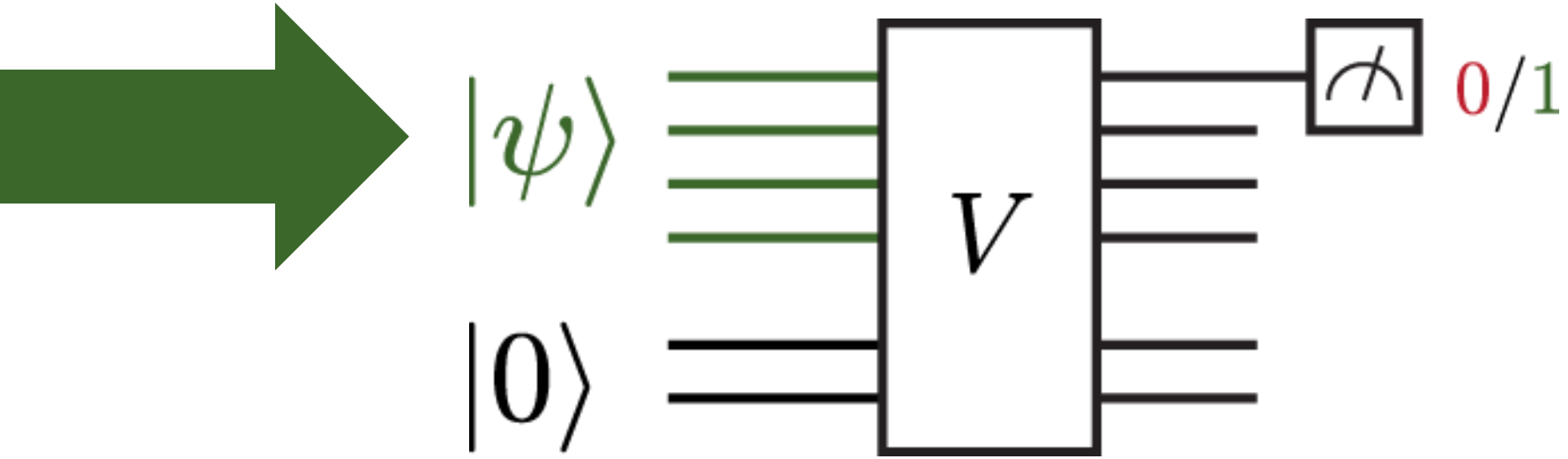


YES? Accept a good proof with $p > a$.

NO? Probability of accepting $p < b$.

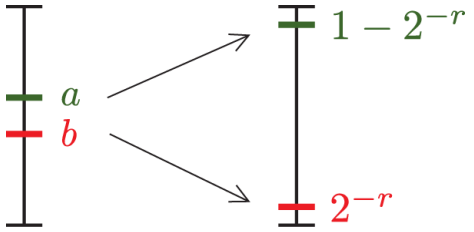


1 The QMA protocol: amplification

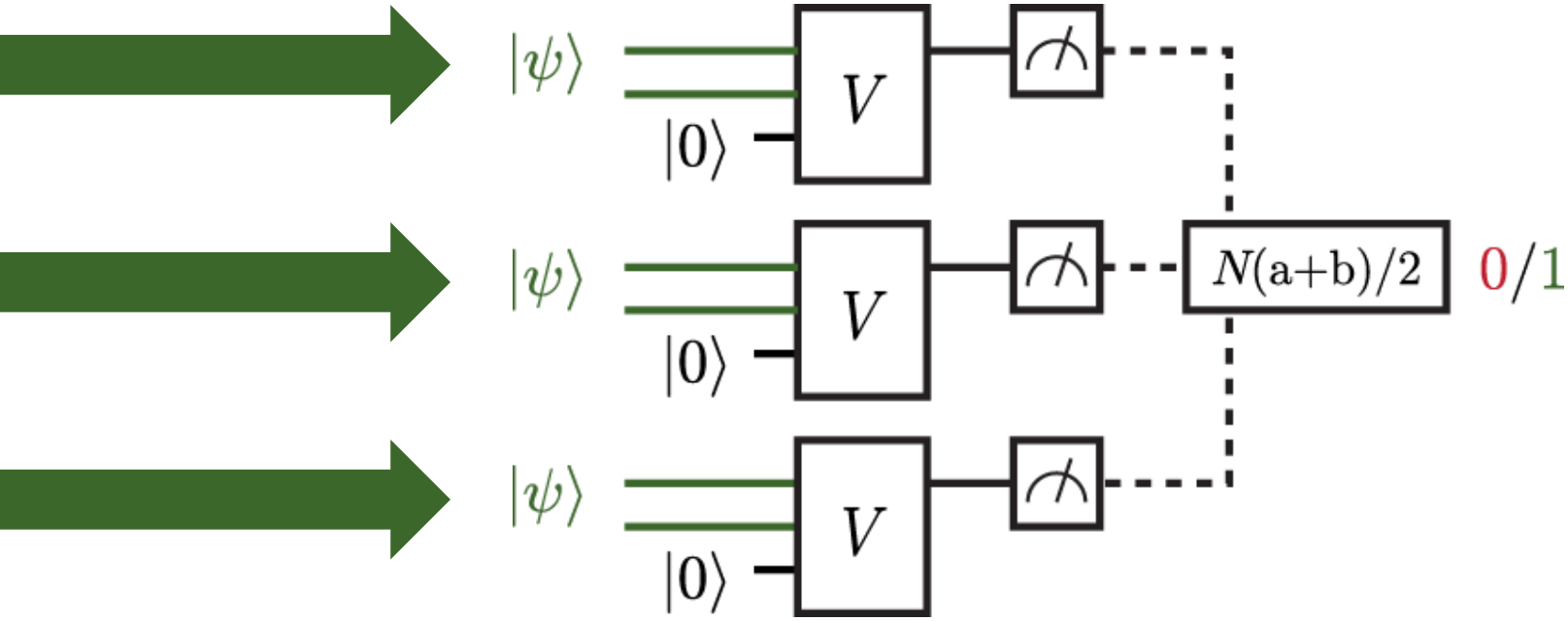


YES? Accept a good proof with $p > a$.

NO? Probability of accepting $p < b$.

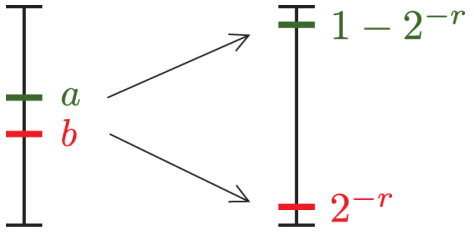


1 The QMA protocol: amplification [Kitaev]



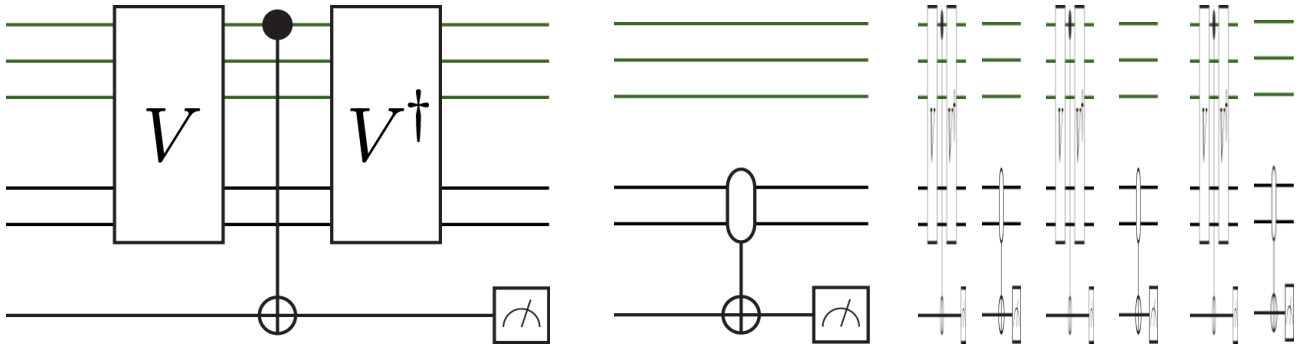
YES? Accept a good proof with $p > a$.

NO? Probability of accepting $p < b$.



1 The QMA protocol: amplification [Mariott-Watrous]

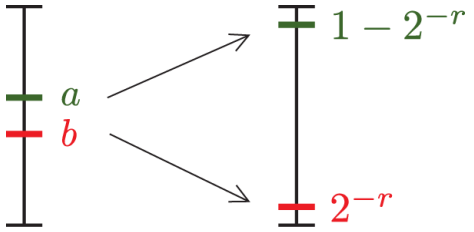
alternating projections P, Q



1, 0, 0, 0, 1, 1, 0, 1 …

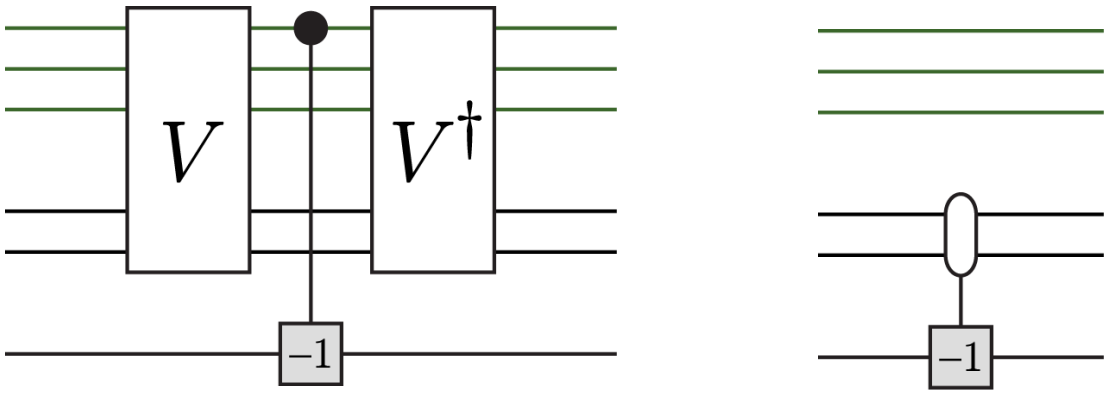
Life in a 2D subspace. [Jordan]

How many 00's and 11's?

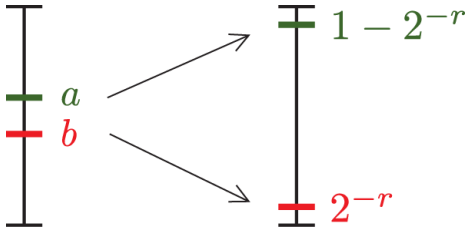


1 The QMA protocol: fast amplification [N.-Wocjan-Zhang]

alternating reflections R, S

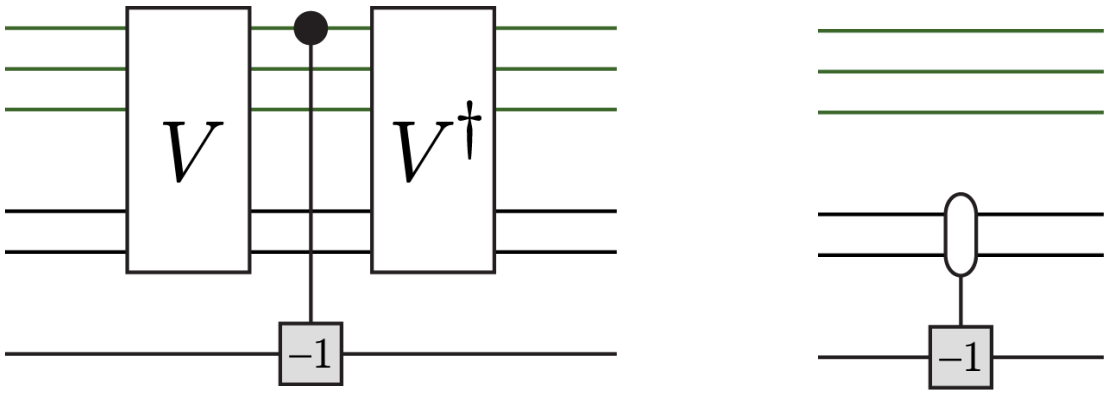


Together: a rotation.
Phase estimation of RS.



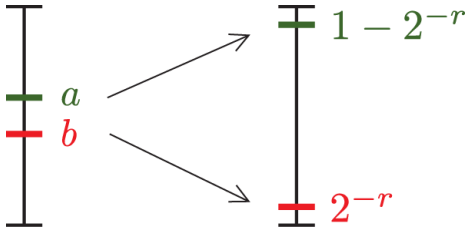
1 The QMA protocol: fast amplification [N.-Wocjan-Zhang]

alternating reflections *R*, *S*



Together: a rotation.

Perfect phase estimation of *RS*?

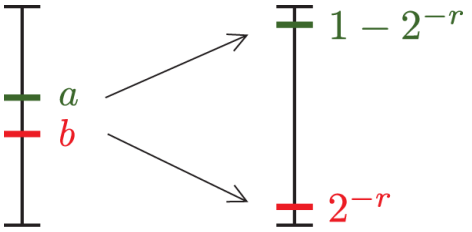


1 Amplification for MA & QMA.

amplification

YES? Accept with p almost 1.

NO? Get fooled with small p.

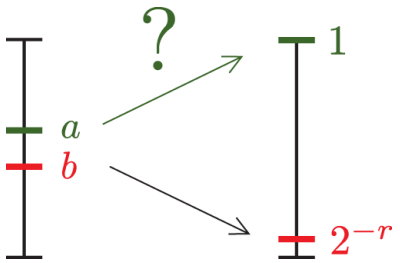


1 Perfect amplification for MA & QMA?

perfect
amplification

YES? Accept a good proof.

NO? Get fooled with small p.



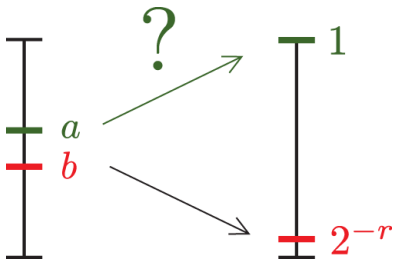
1 Perfect amplification for MA.

perfect classical amplification

$$\mathrm{MA} = \mathrm{MA}_1$$ [Zachos & Fürer]

YES? Accept a good proof.

NO? Get fooled with small *p*.



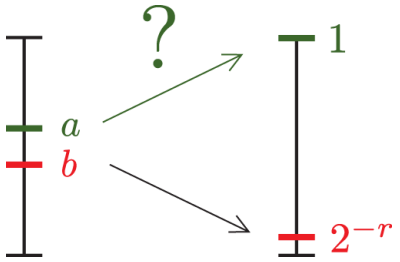
1 Perfect amplification for QMA?

perfect quantum amplification

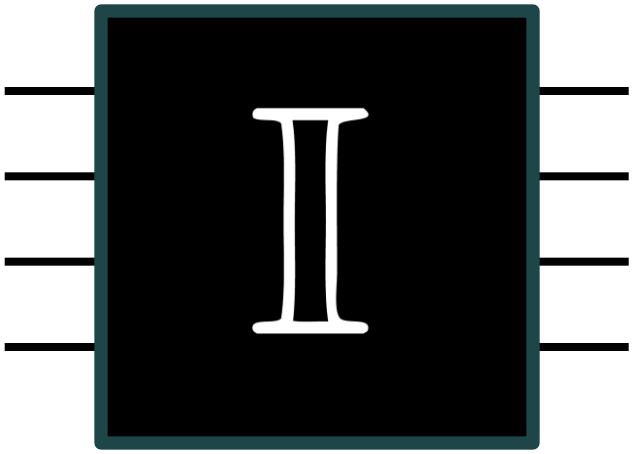
$$\text{QMA} \overset{?}{\to} \text{QMA}_1$$

YES? Accept a good proof.

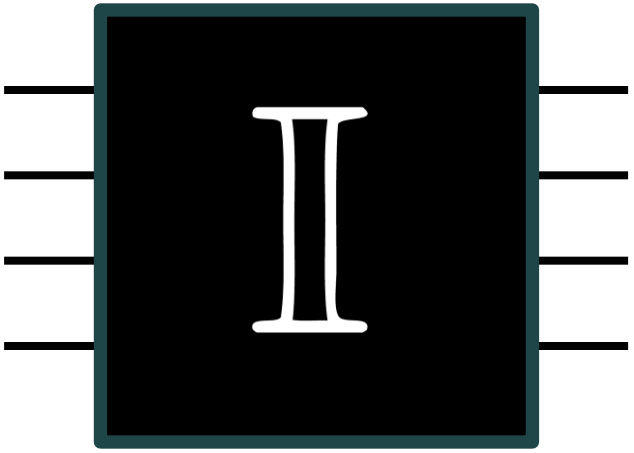
NO? Get fooled with small *p*.



An oracle separation of QMA & QMA_1



An oracle separation of QMA & QMA_1



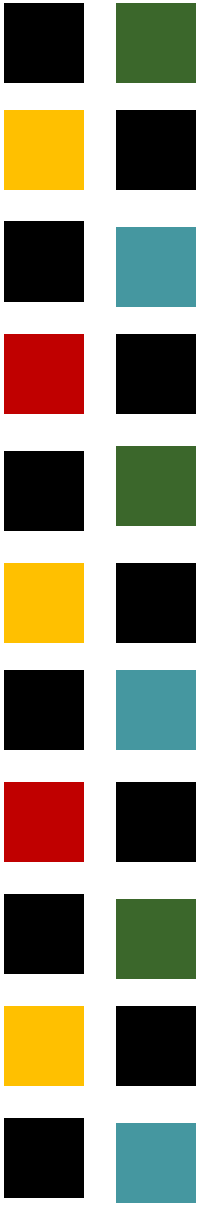
a continuous range of angles

Accept something without a doubt?

=

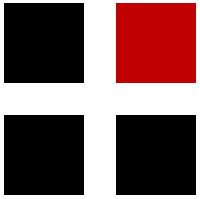
Accept everything…
[Aaronson '08]

Quantum Computing



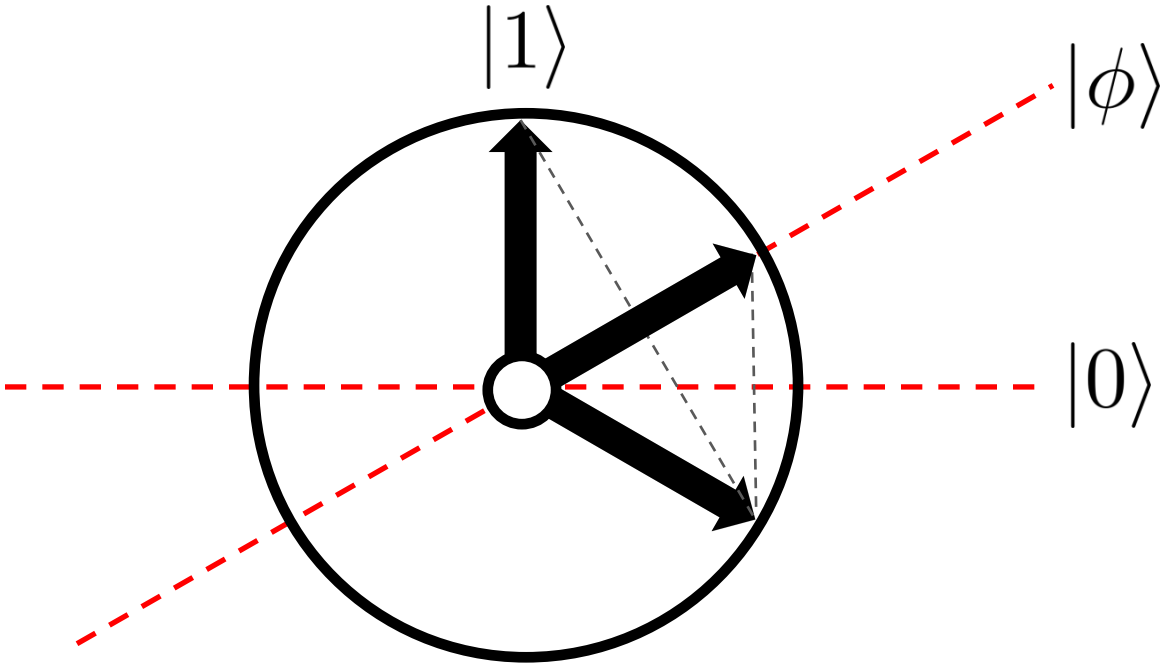
Exact

Quantum Computing



Exact Grover's search [L. Grover]

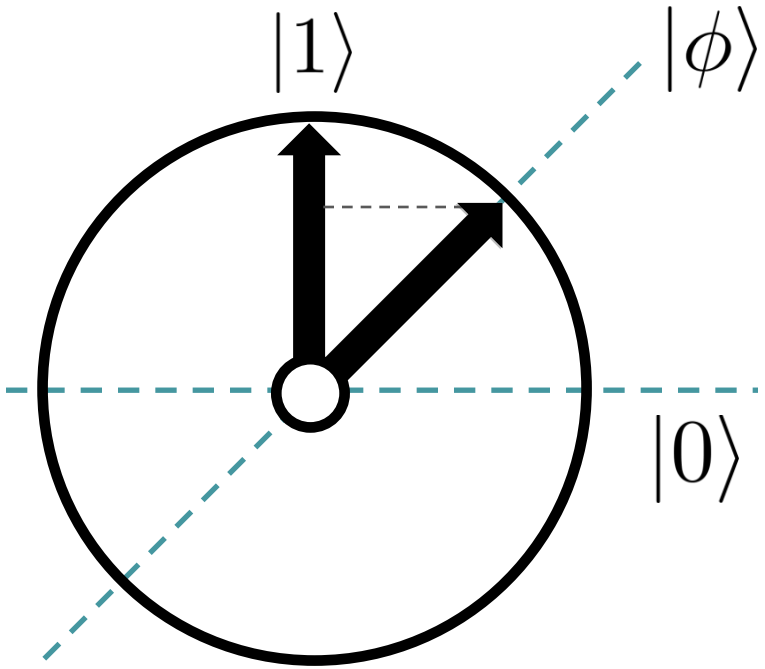
$$|\phi\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$$

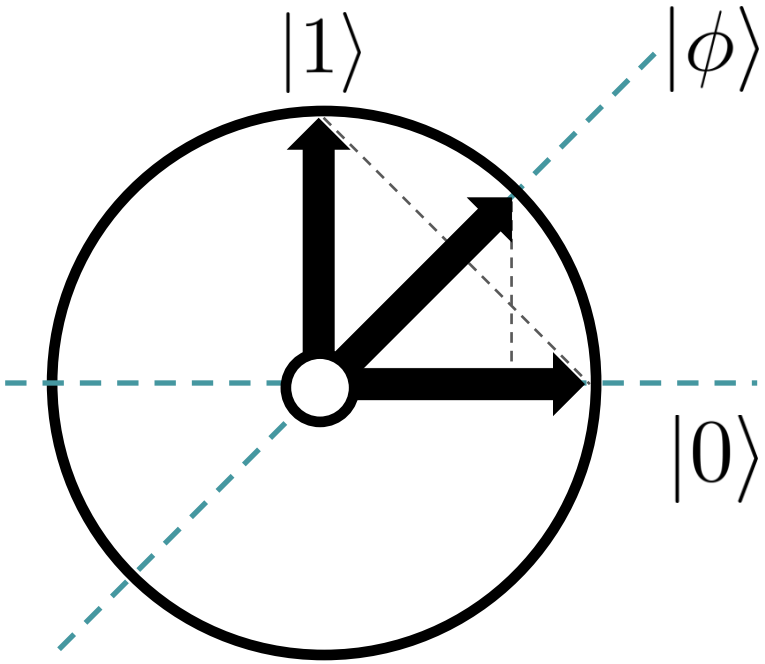


Exact quantum rewinding

[J. Watrous]

$$|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

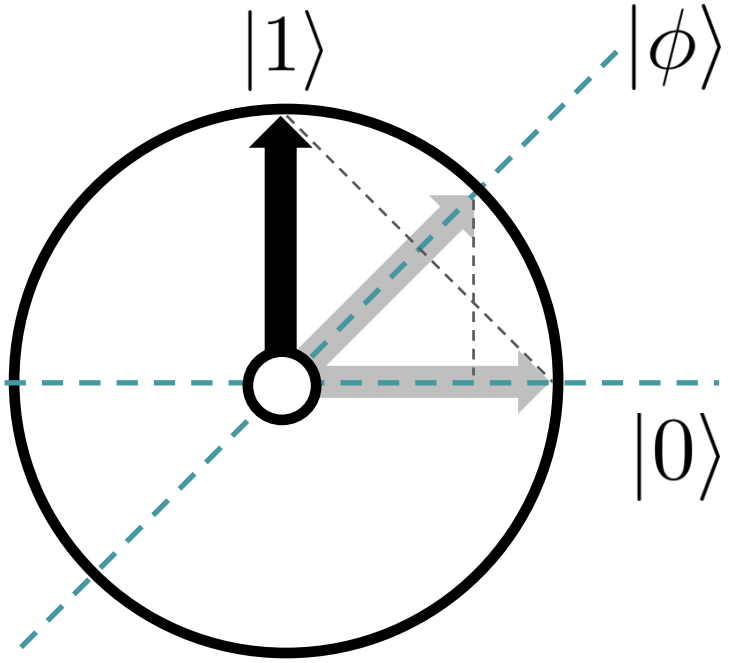




Exact quantum rewinding

$$|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

- test acceptance
- reflect about $|\phi\rangle$
- test acceptance



Exact quantum rewinding

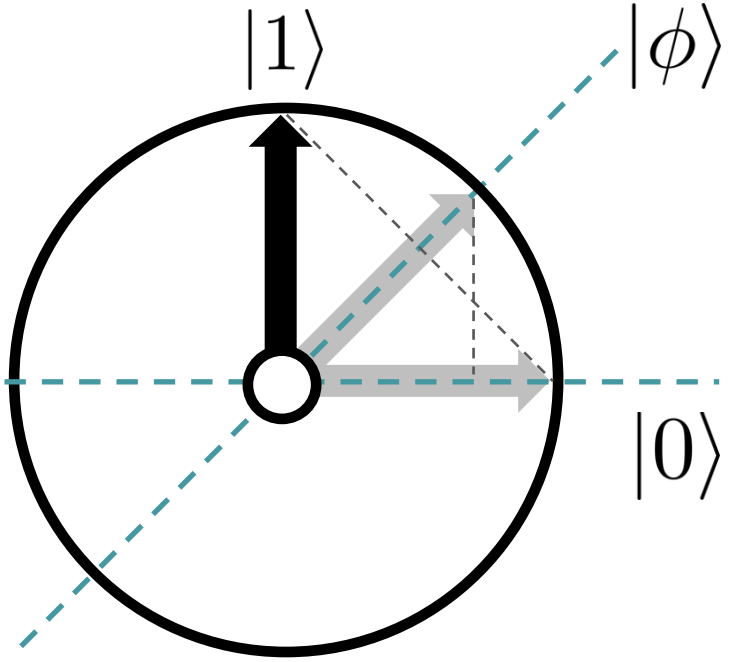
$$|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

a state with a "nice" *p*

test acceptance

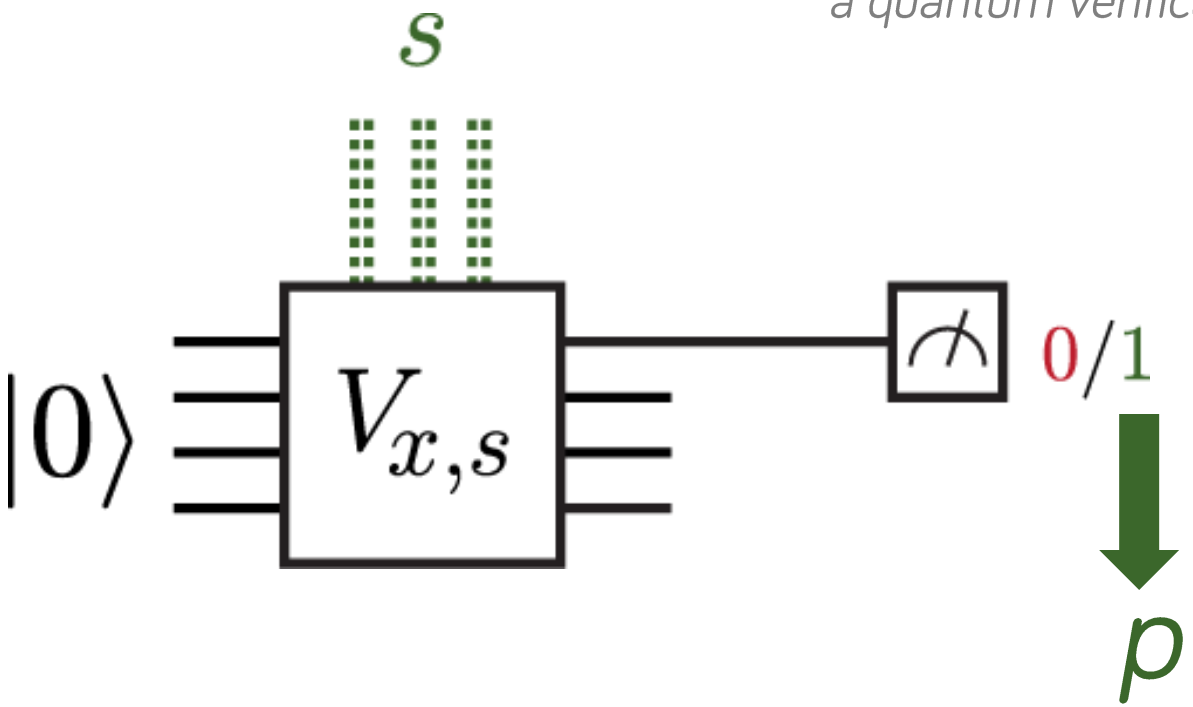
reflect about $|\phi\rangle$

test acceptance



2 QCMA (MQA)

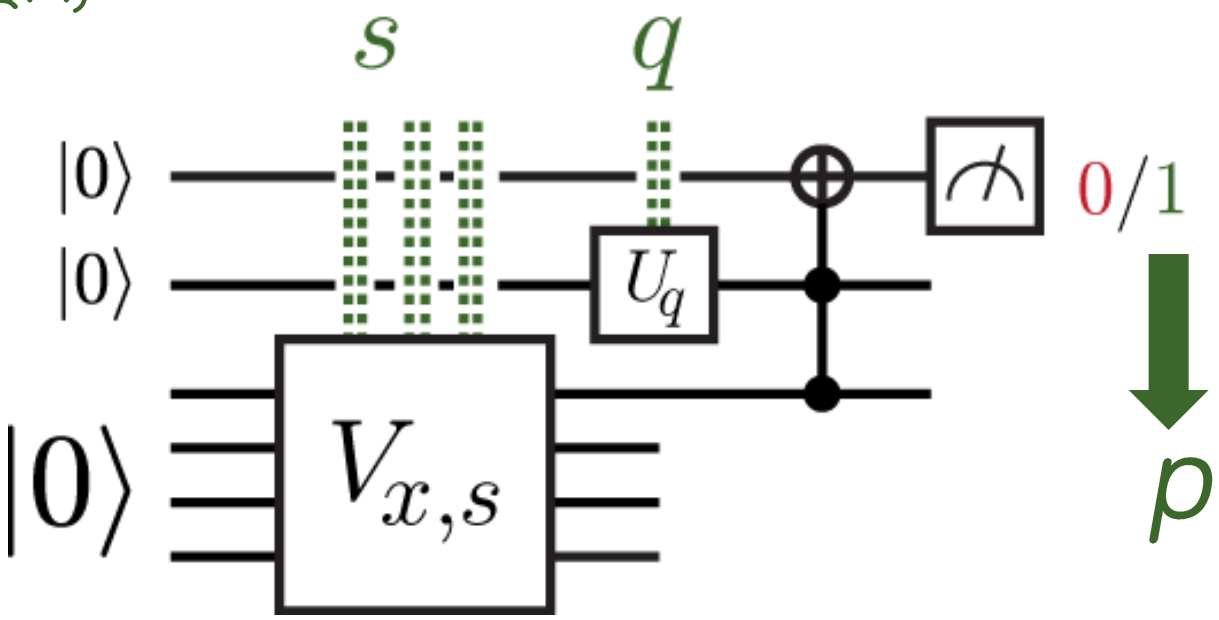
A classical witness,
a quantum verification.



Knowing how to prepare the witness...
we can reflect about it.

$$\sqrt{1-p}|\cdots 0\rangle + \sqrt{p}|\cdots 1\rangle$$

2 QCMA (MQA)

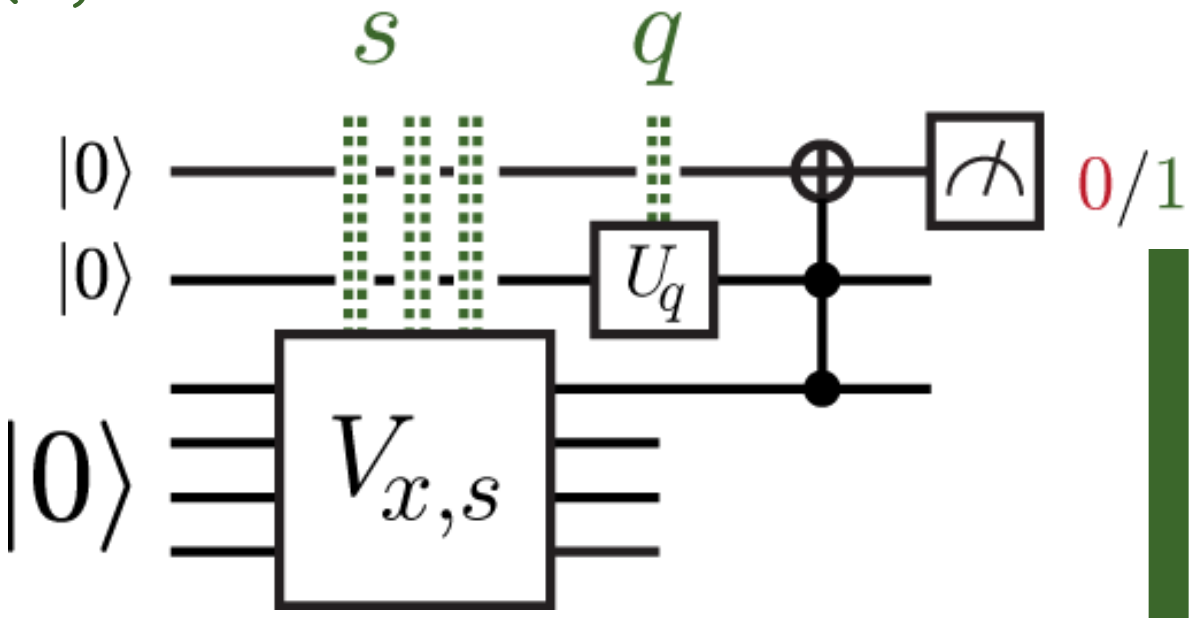


Knowing the acceptance probability...
add a rotated ancilla.

$$\sqrt{1-q}|0\rangle + \sqrt{q}|1\rangle$$

$$\sqrt{1-p}|\cdots 0\rangle + \sqrt{p}|\cdots 1\rangle$$

2 QCMA (MQA)



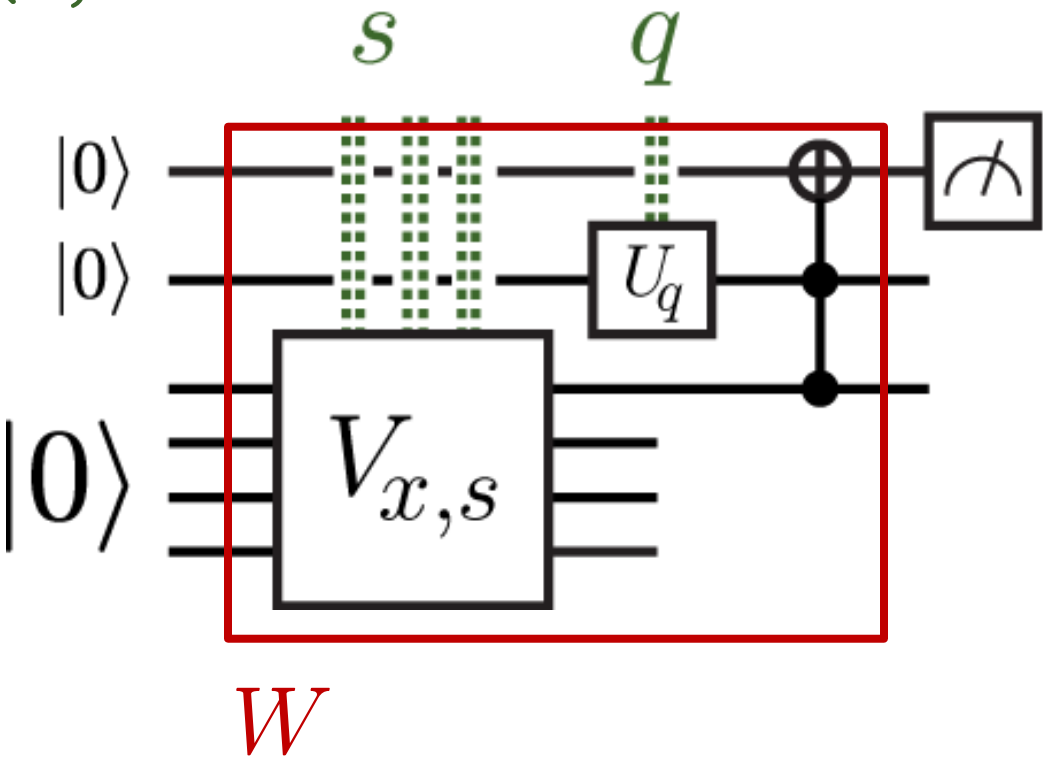
Knowing the acceptance probability...
add a rotated ancilla, get ¼ or ½.

$p'=pq=¼$

$$\sqrt{1-q}|0\rangle + \sqrt{q}|1\rangle$$

$$\sqrt{1-p}|\cdots 0\rangle + \sqrt{p}|\cdots 1\rangle$$

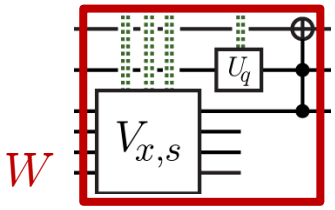
2 QCMA (MQA)

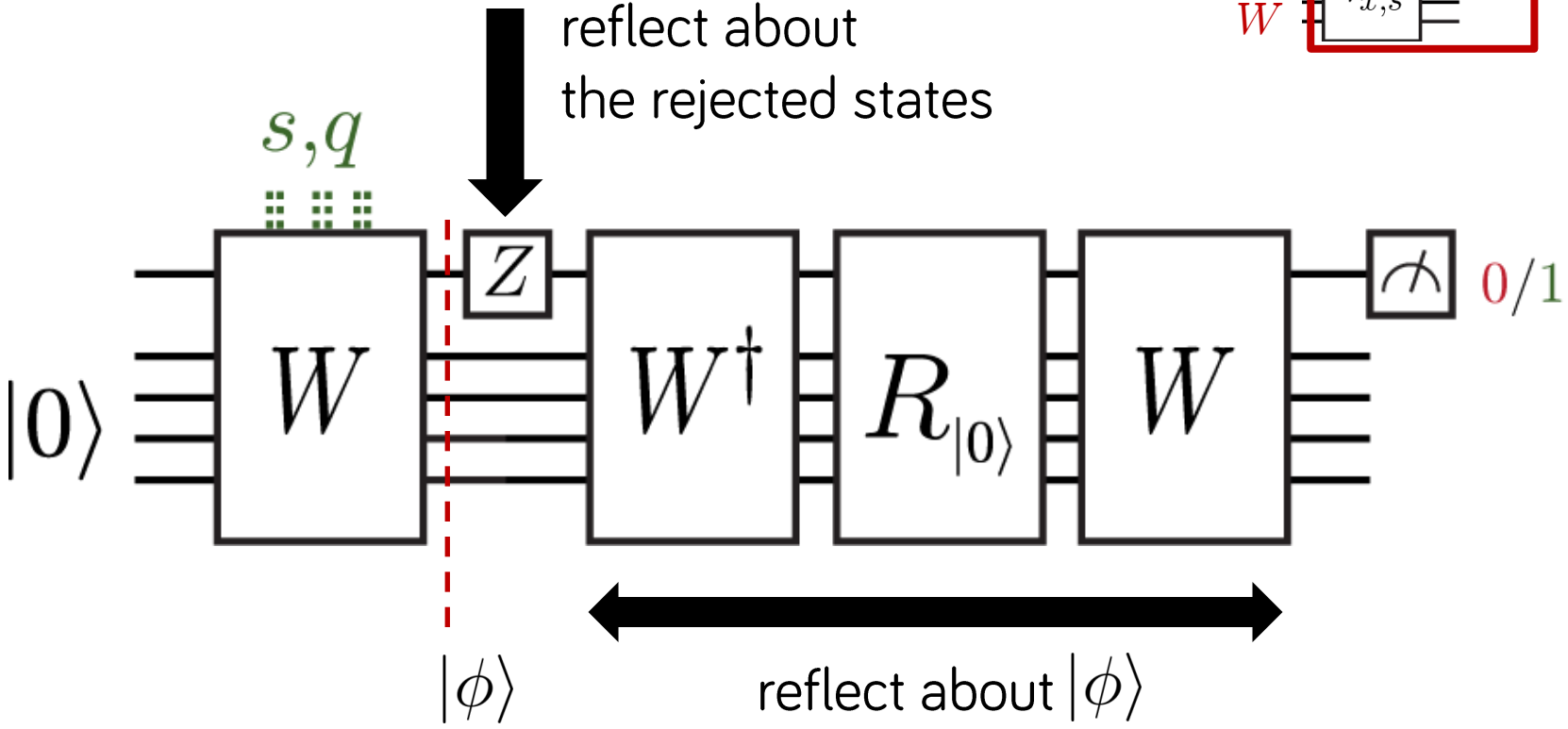


$p'=pq=¼$

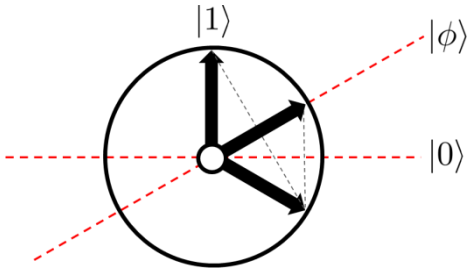
Gates with rational-number elements are universal.
Both p and q are rational.
It's doable.

2 QCMA (MQA) with perfect completeness

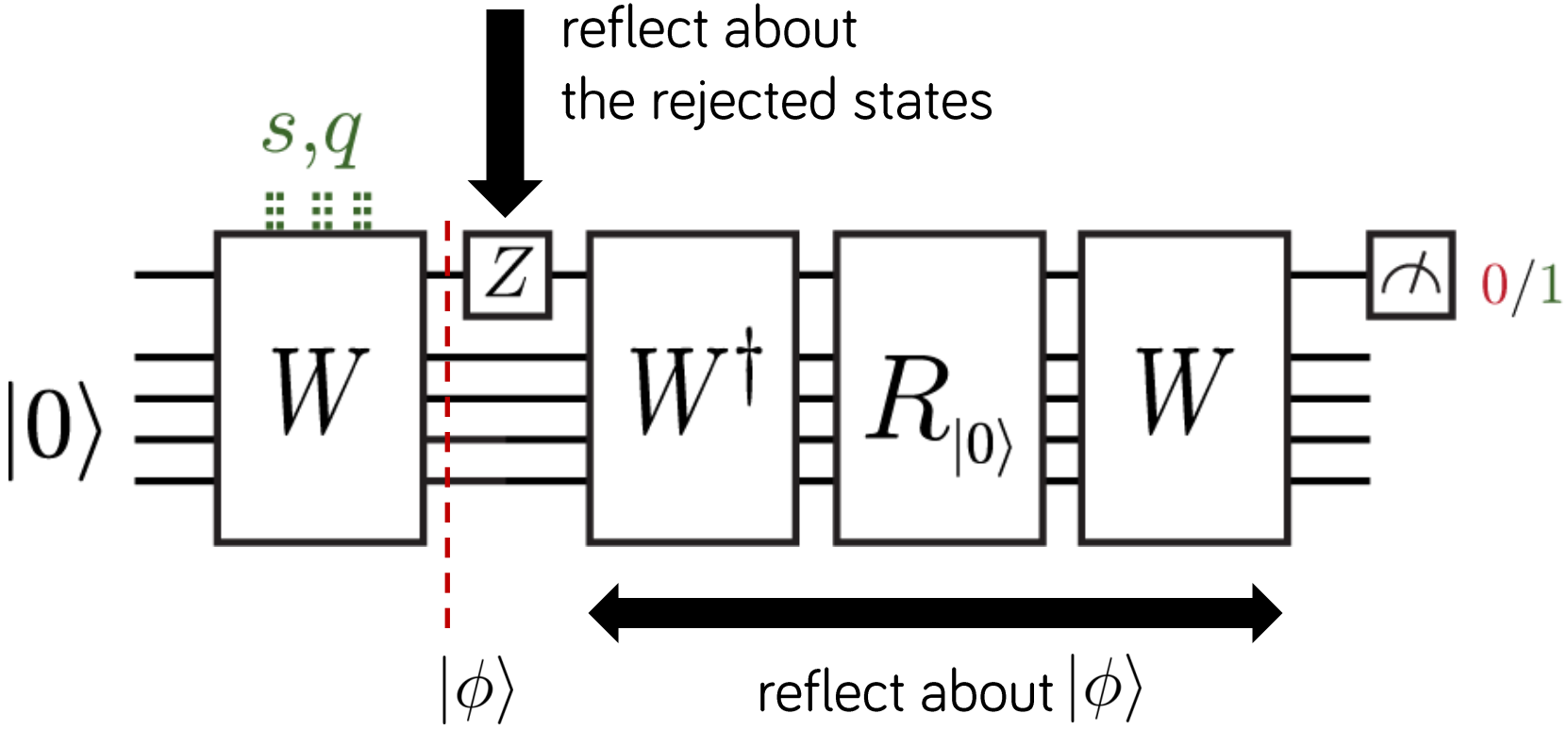




Perfectly accepts solid proofs.

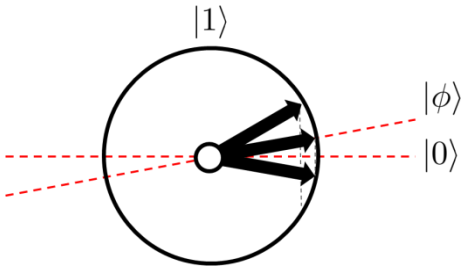


2 QCMA (MQA) with perfect completeness

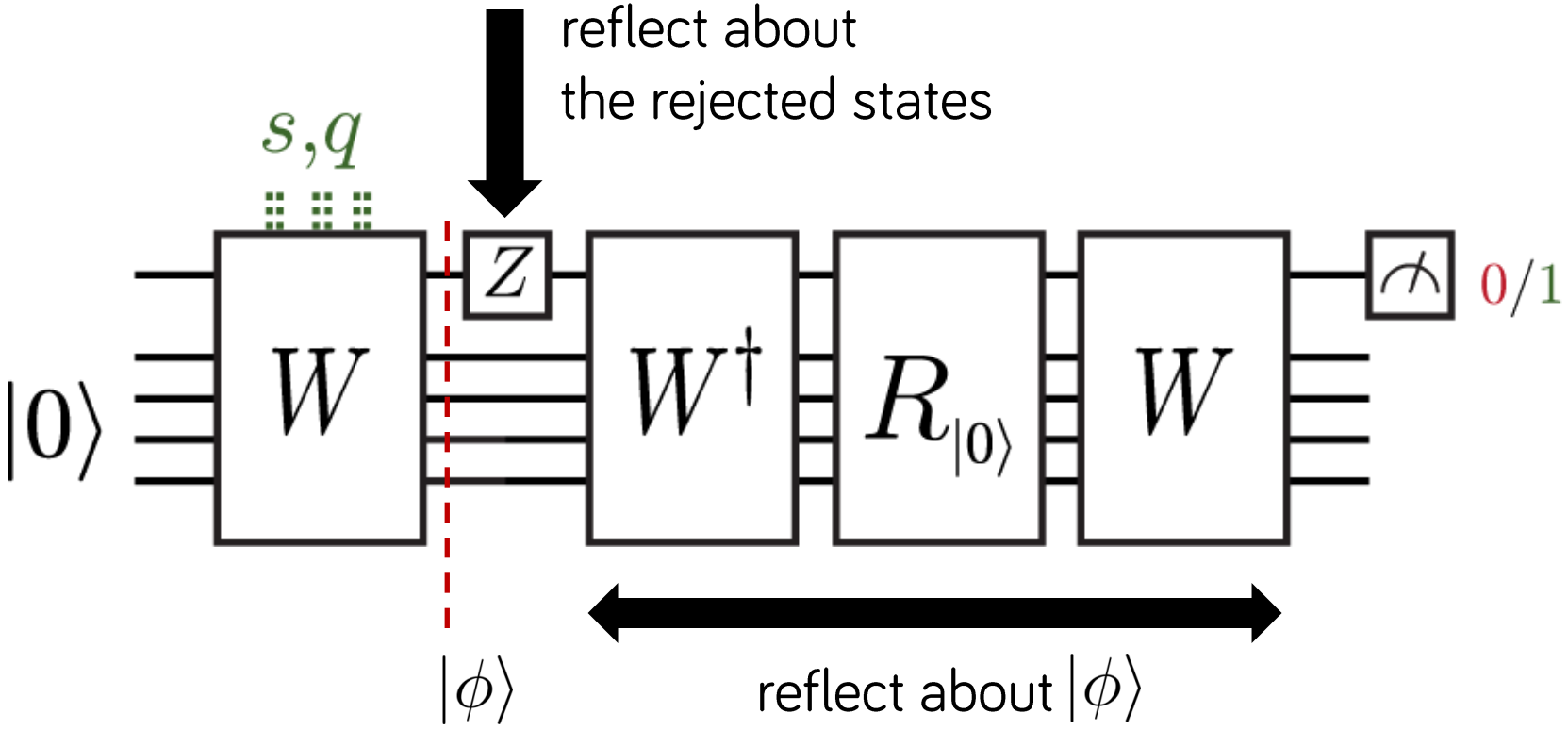


Perfectly accepts solid proofs.

The soundness doesn't break.



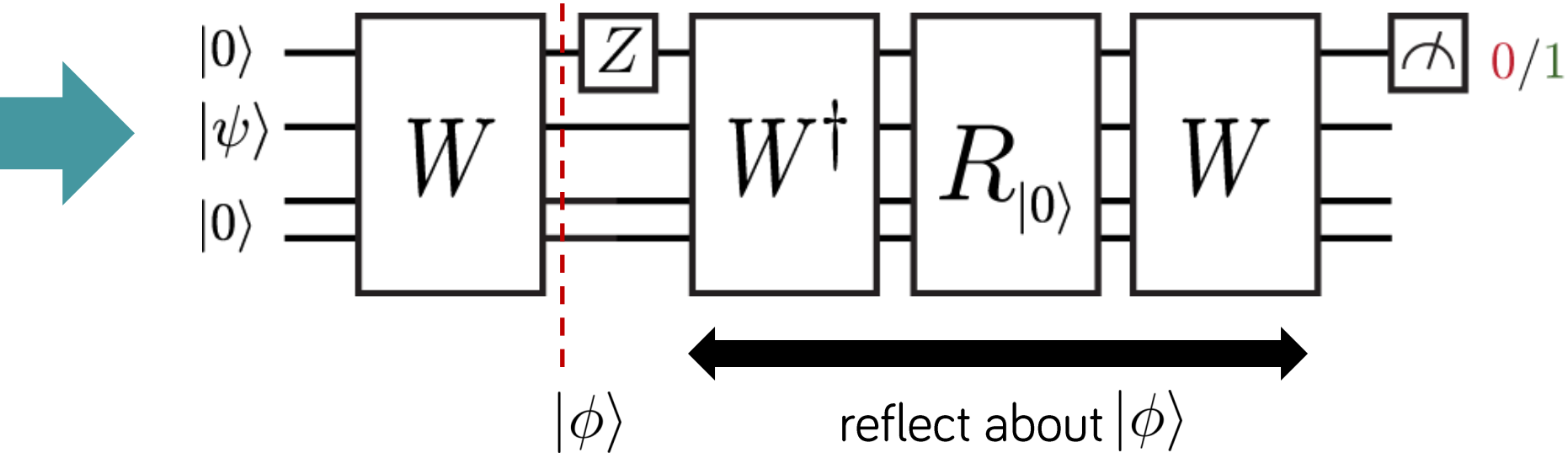
2 QCMA (MQA) with perfect completeness



$$\mathrm{QCMA}_1 = \mathrm{QCMA}$$

3 Towards perfect completeness in QMA...

Let's try the same with a quantum witness.



How to

correct *p* to something nice?

reflect about the unknown witness?

3 Towards perfect completeness in QMA...

Send us the witness.

Send us its acceptance probability p?

a correction q?

How to correct p to something nice?
reflect about the unknown witness?

3 Towards perfect completeness in QMA...

Send us the witness.

Send us its acceptance probability p?

a correction q?

a trustworthy encoding of q?

$$\sqrt{1-q}|0\rangle + \sqrt{q}|1\rangle$$

We'll give you some EPR pairs first.

How to

correct p to something nice?

reflect about the unknown witness?

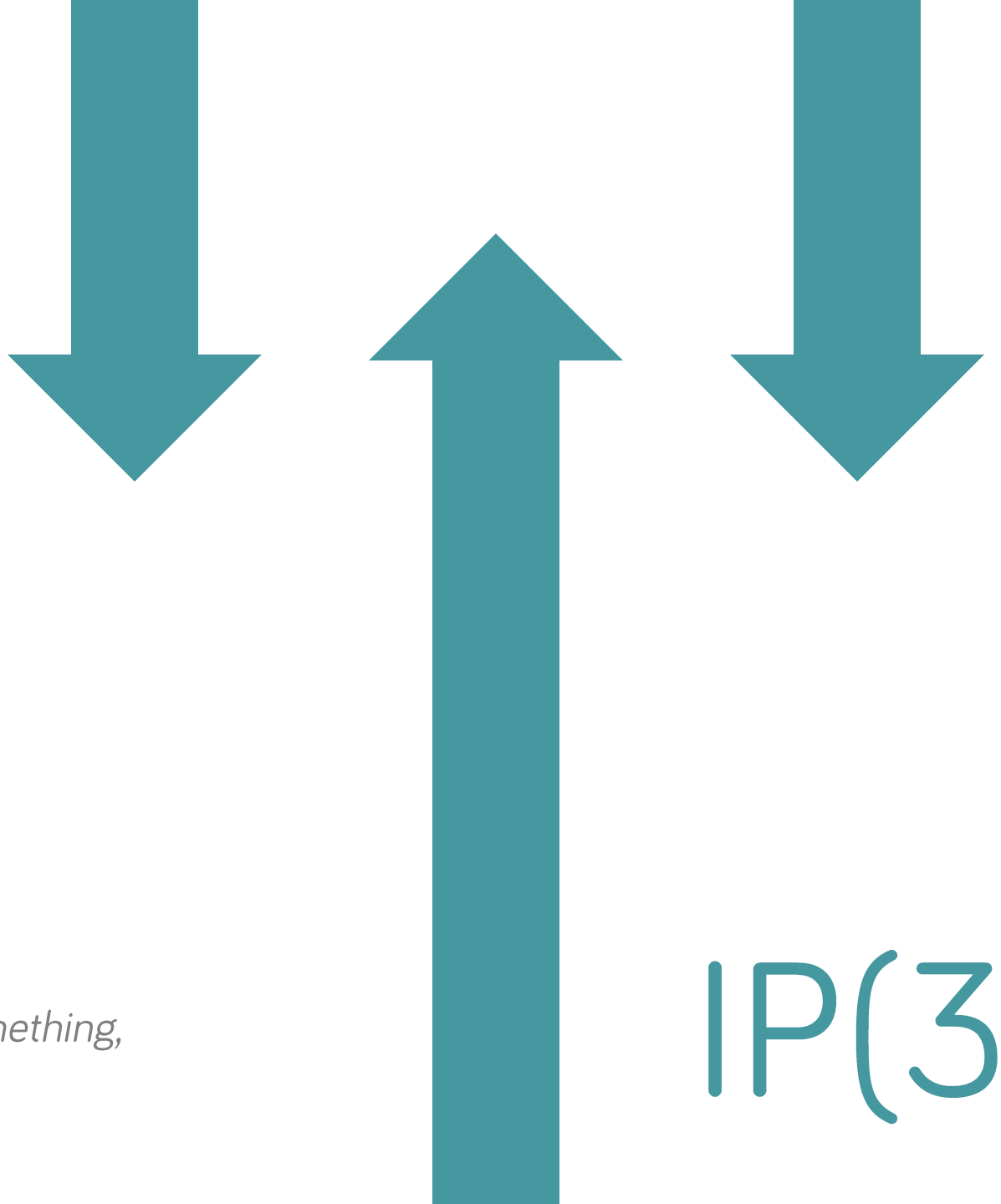
3 Interactive Proofs

Hey, Merlin, could you carve something from this material?

3 Interactive Proofs

Hey, Merlin, could you carve something from this material?

IP(2)

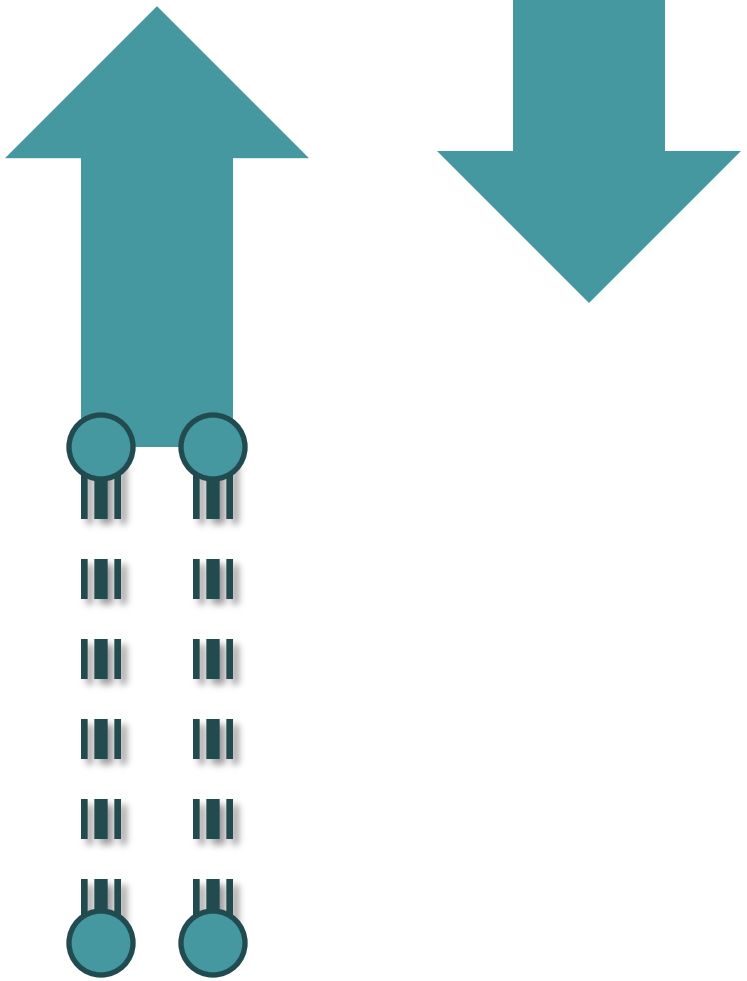


Receive,
compute, ask something,
receive, conclude.

IP(3)


IP(4)

$QIP_1(2)$



QMA_1 const. EPR

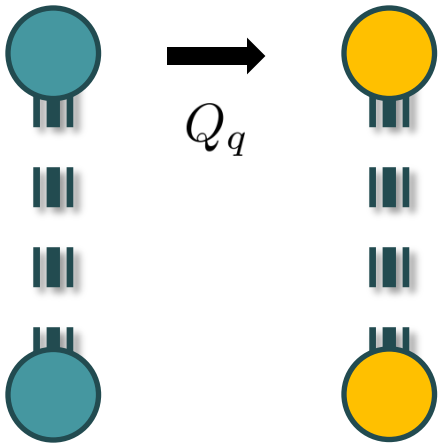
3 Correcting *p* to something "nice".

A "correcting" state $\sqrt{1-q}|0\rangle + \sqrt{q}|1\rangle$ with $pq = \frac{1}{2}$

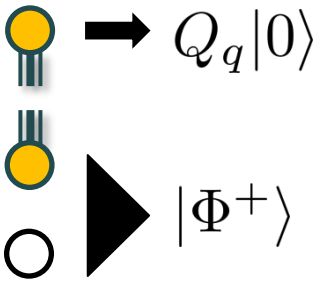
Prepared by Merlin using

$$Q_q = \begin{bmatrix} \sqrt{1-q} & \sqrt{q} \\ \sqrt{q} & -\sqrt{1-q} \end{bmatrix}$$

on a half of an EPR pair



$$\sqrt{1-q}|\Phi^-\rangle + \sqrt{q}|\Psi^+\rangle$$

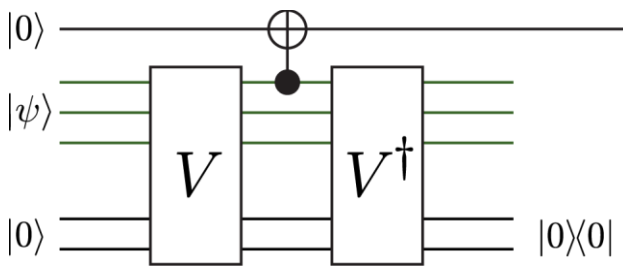


A Choi-Jamiołkowski state… it allows probabilistic (heralded) simulation of Q_q.

3 The soundness is much easier to prove with distillation

Instead of using $\sqrt{1-p}|\cdots 0\rangle + \sqrt{p}|\cdots 1\rangle$

"distill" the state



$\sqrt{1-r}|0\rangle + \sqrt{r}|1\rangle$

with *r* related to *p*

Use it to apply V_r probabilistically

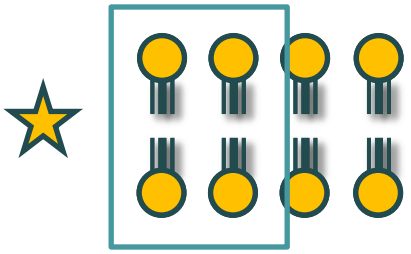
$$V_r = \begin{bmatrix} \sqrt{1-r} & \sqrt{r} \\ \sqrt{r} & -\sqrt{1-r} \end{bmatrix}$$

We can simulate the reflection about $|\phi\rangle = W(|\psi\rangle \otimes |0\rangle)$

3 The combined SOUND protocol

Send Merlin *N* halves of EPR pairs.

He applies Q_q, returns them & a witness.

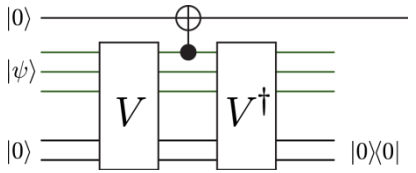


Permute the "EPR pairs".

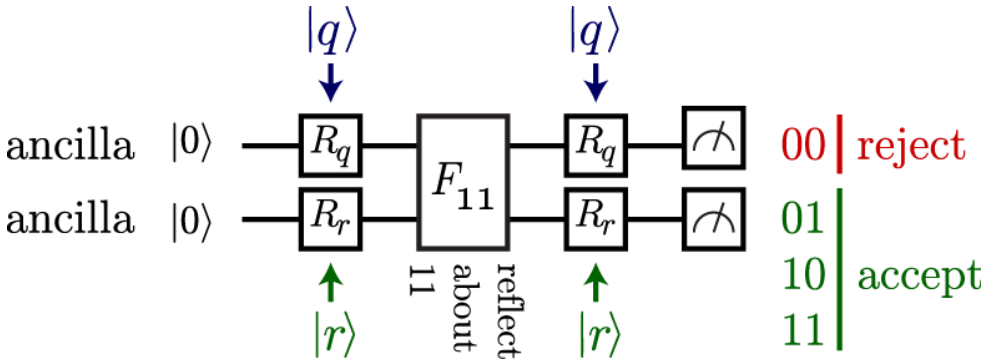
Pick the first two.

SWAP test & Subspace test.

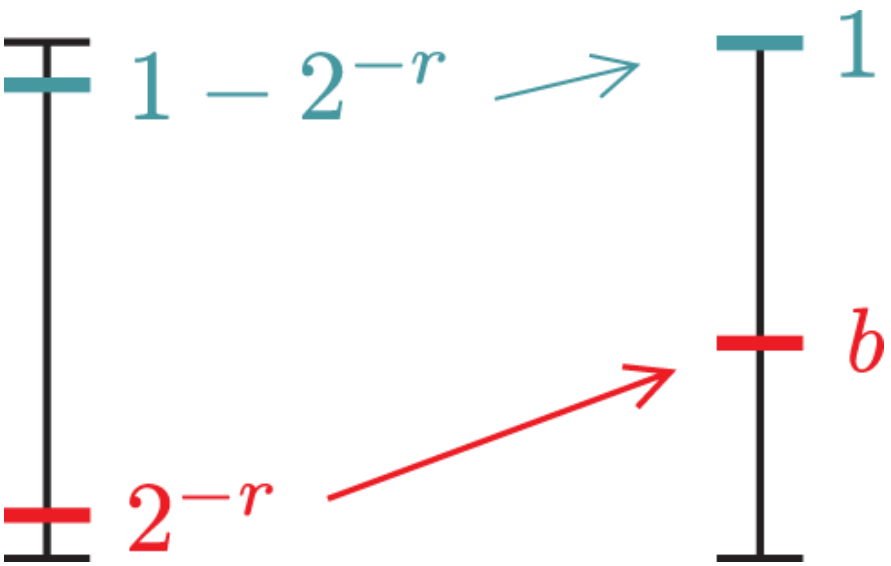
Distill 2 copies of $\sqrt{1-r}|0\rangle + \sqrt{r}|1\rangle$



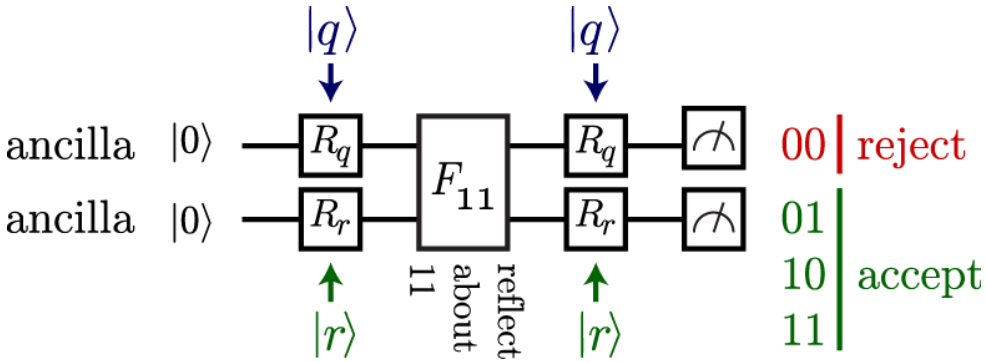
Simulate a modified verification. If the simulation fails, accept.



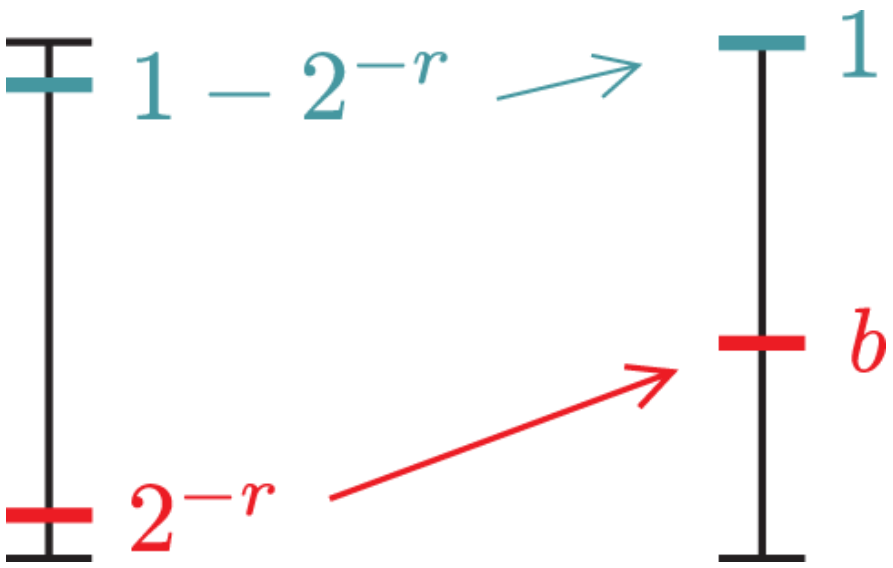
3 The second result



Simulate a modified verification. If the simulation fails, accept.



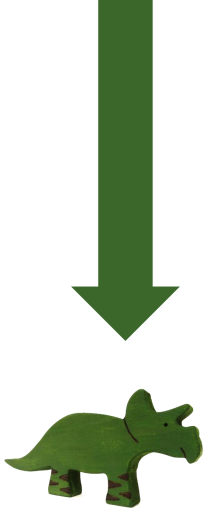
3 The second result



Simulate a modified verification. If the simulation fails, accept.

$$\mathrm{QMA} \subseteq \mathrm{QMA}_1^{\text{const. EPR}}$$

4 Towards perfect completeness for QMA



- It is quite difficult.

  The last, tiny but annoying step.
  An oracle separation to tackle.

- Classical & “nice” witnesses.

  Perfect quantum rewinding.
  Reflection about a known initial state.

$$\mathrm{QCMA} = \mathrm{QCMA}_1$$

- A constant # of EPR pairs.

  Simulating reflections probabilistically.
  Shared EPR pairs give us soundness.

$$\mathrm{QMA} \subseteq \mathrm{QMA}_1^{\mathrm{c.EPR}}$$

QMA

Stephen P. Jordan
NIST Gaithersburg

Hirotada Kobayashi
NII Tokyo

François Le Gall
University of Tokyo

Harumichi Nishimura
Nagoya University

Daniel Nagaj
University of Vienna

QIP 2013
Beijing

arXiv: 1111.5306v2
arXiv: 1210.1290

QMA_1

Stephen P. Jordan
NIST Gaithersburg

Hirotada Kobayashi
NII Tokyo

François Le Gall
University of Tokyo

Harumichi Nishimura
Nagoya University

Daniel Nagaj
University of Vienna

QIP 2013
Beijing

arXiv: 1111.5306v2
arXiv: 1210.1290