Most quantum states are useless for measurement-based quantum computation

Steve Flammia

Perimeter Institute

QIP 2009, Santa Fe

D. Gross, SF, J. Eisert 0810.4331

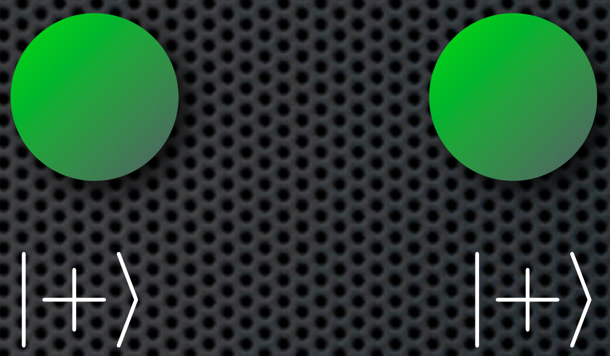
M. Bremner, C. Mora, A. Winter 0812.3001

Measurement-based QC

Raussendorf & Briegel PRL 2001

Measurement-based QC

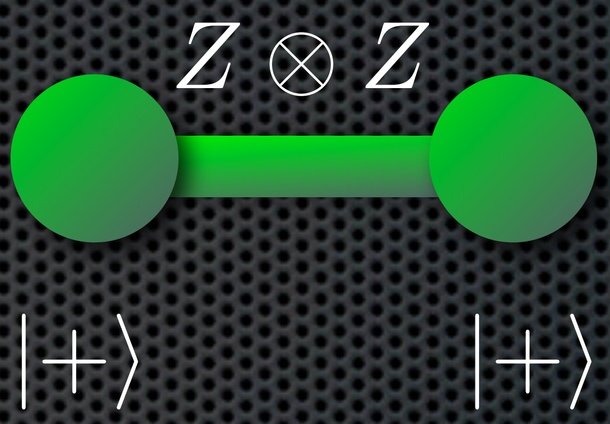
- prepare X eigenstates



Raussendorf & Briegel PRL 2001

Measurement-based QC

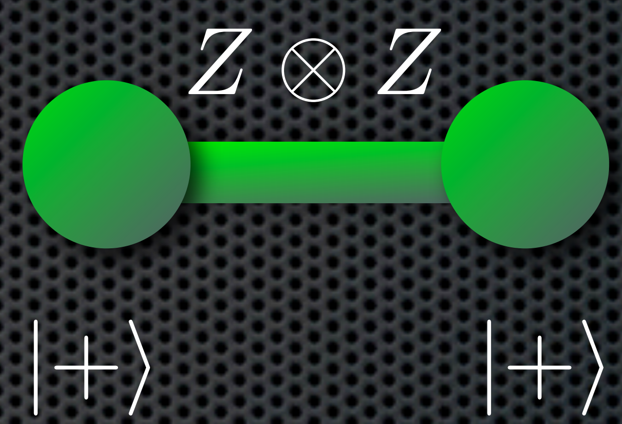
- prepare X eigenstates
- entangle neighbors with a Z-Z coupling

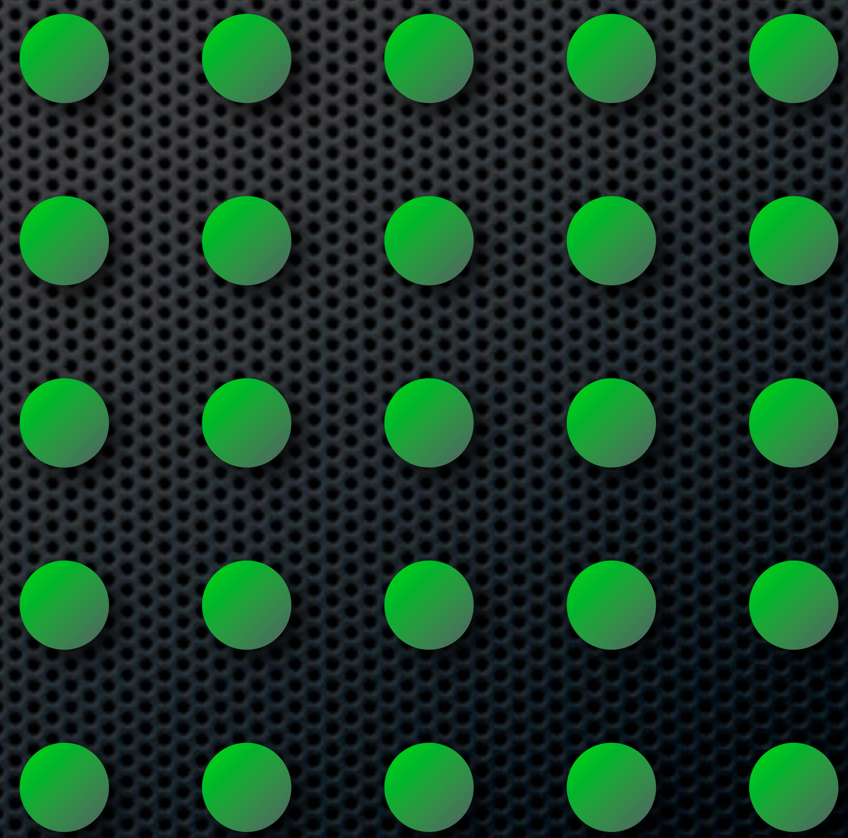


Raussendorf & Briegel PRL 2001

Measurement-based QC

- prepare X eigenstates
- entangle neighbors with a Z-Z coupling
- Build a large lattice for universality:
  the CLUSTER STATE

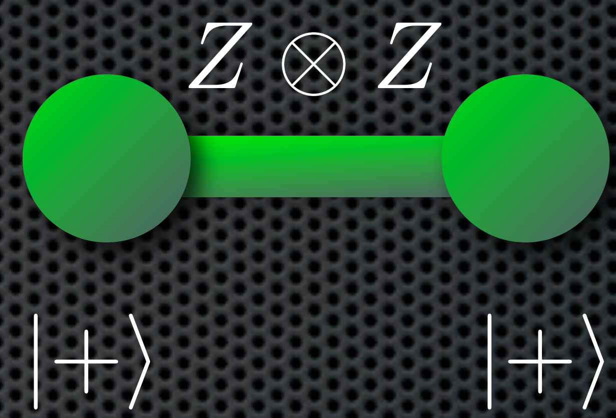


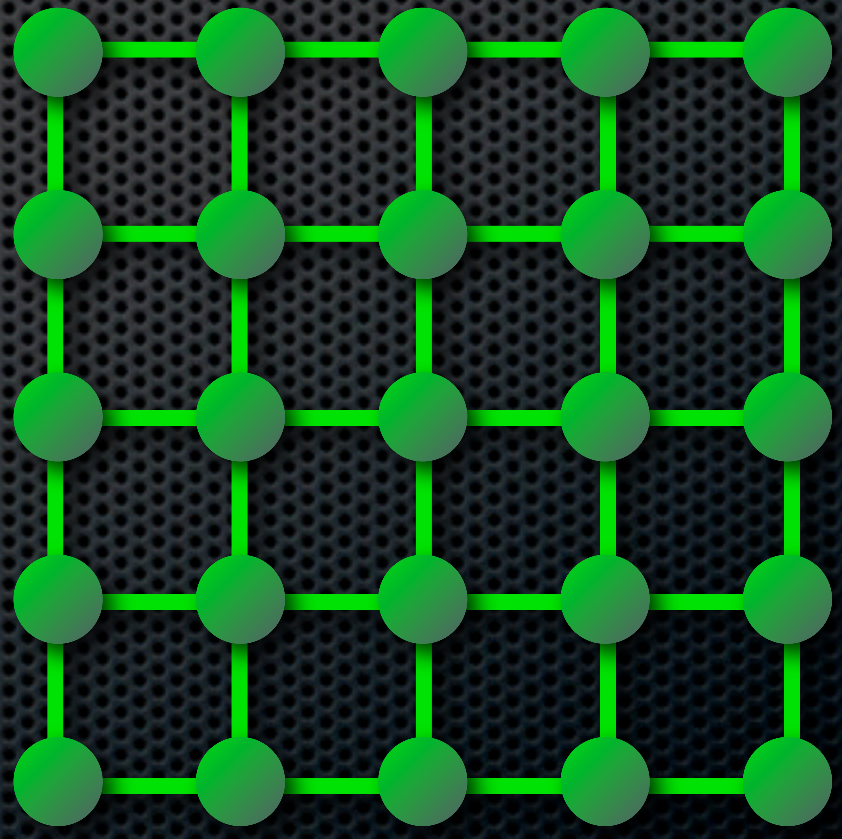


Raussendorf & Briegel PRL 2001

Measurement-based QC

- prepare X eigenstates
- entangle neighbors with a Z-Z coupling
- Build a large lattice for universality:
  the CLUSTER STATE



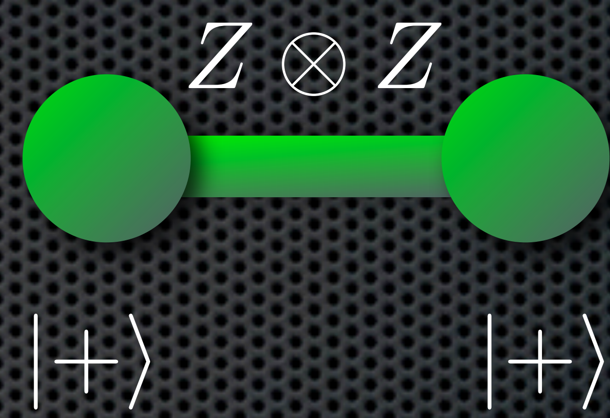


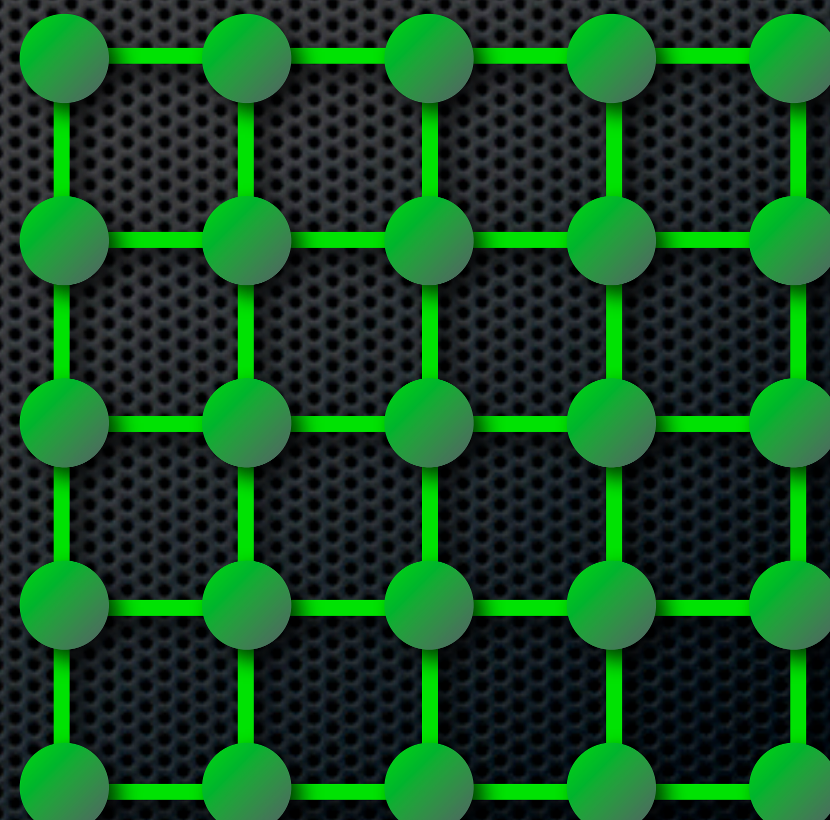
$|\psi_0\rangle$

Raussendorf & Briegel PRL 2001

Measurement-based QC

- prepare X eigenstates
- entangle neighbors with a Z-Z coupling
- Build a large lattice for universality: the CLUSTER STATE
- arbitrary single-qubit measurements with feedforward to compute



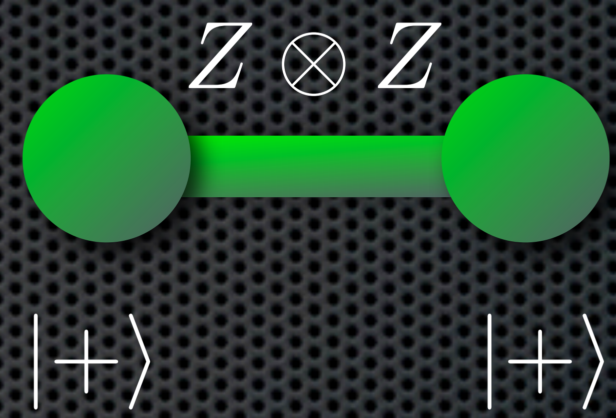


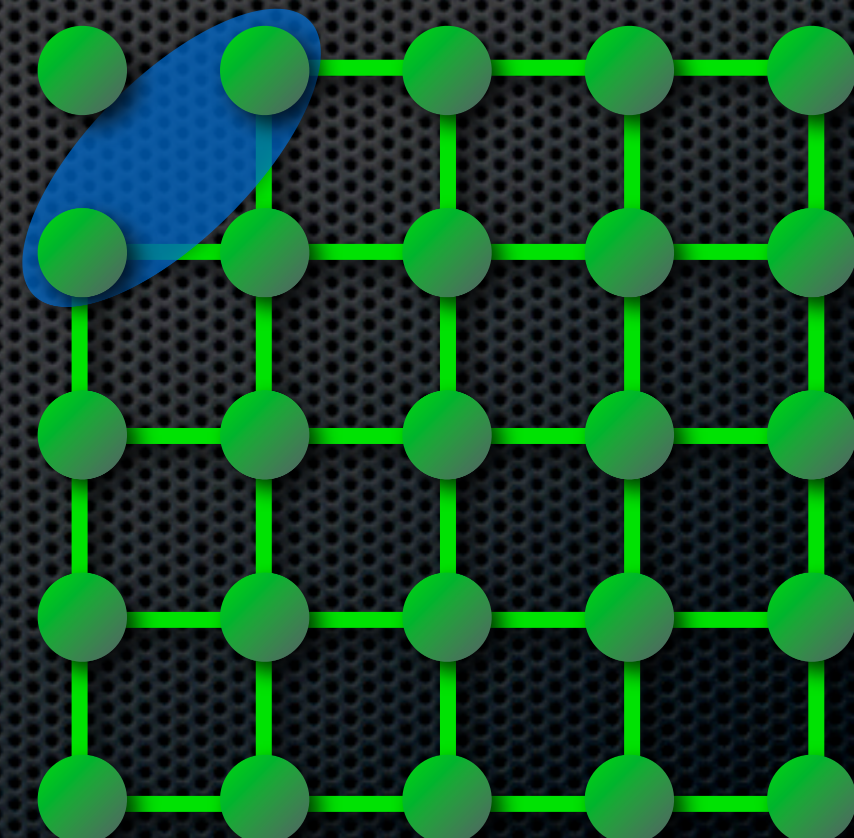
$|\psi_0\rangle$

Raussendorf & Briegel PRL 2001

Measurement-based QC

- prepare X eigenstates
- entangle neighbors with a Z-Z coupling
- Build a large lattice for universality:
  the CLUSTER STATE
- arbitrary single-qubit measurements with feedforward to compute



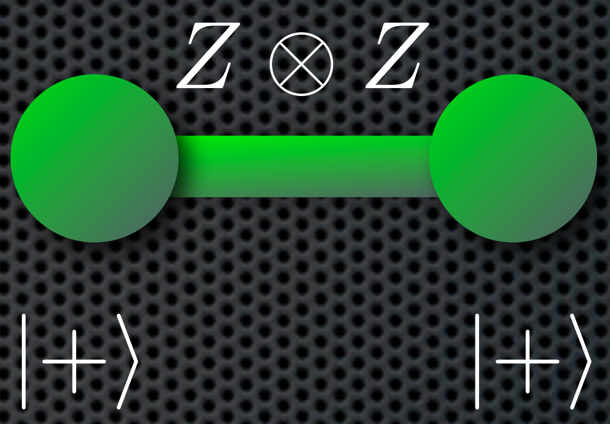


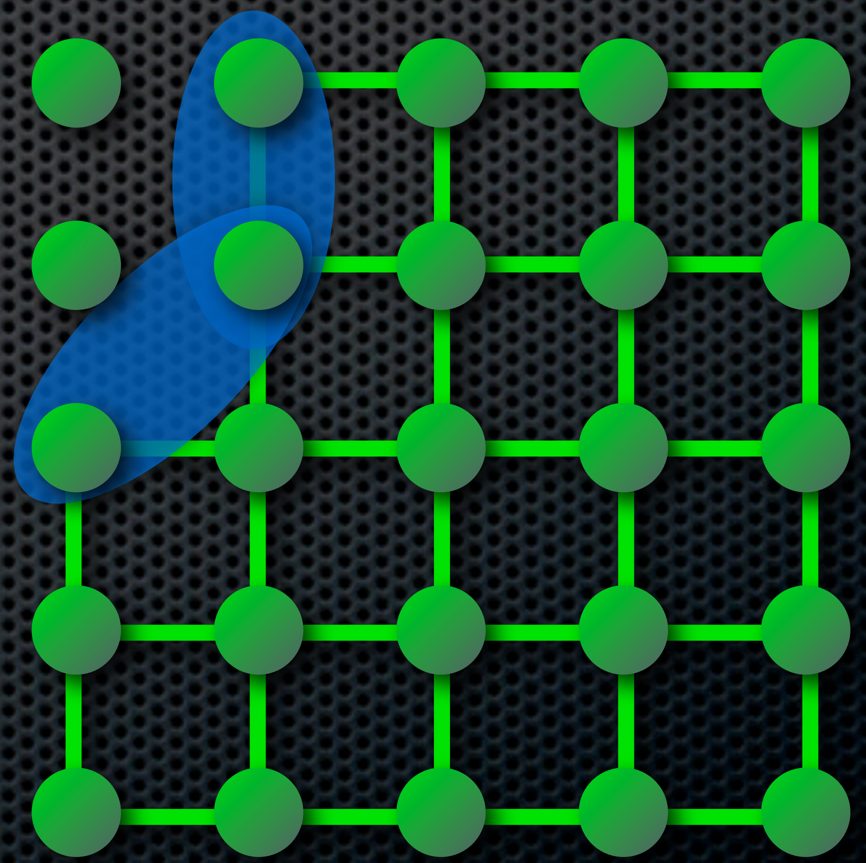
$$|\psi_1\rangle$$

Raussendorf & Briegel PRL 2001

Measurement-based QC

- prepare X eigenstates
- entangle neighbors with a Z-Z coupling
- Build a large lattice for universality: the CLUSTER STATE
- arbitrary single-qubit measurements with feedforward to compute



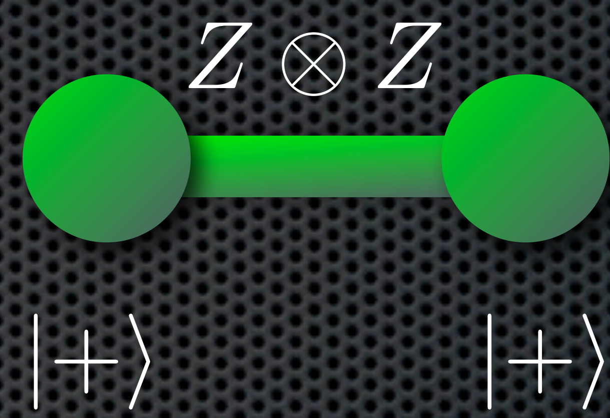


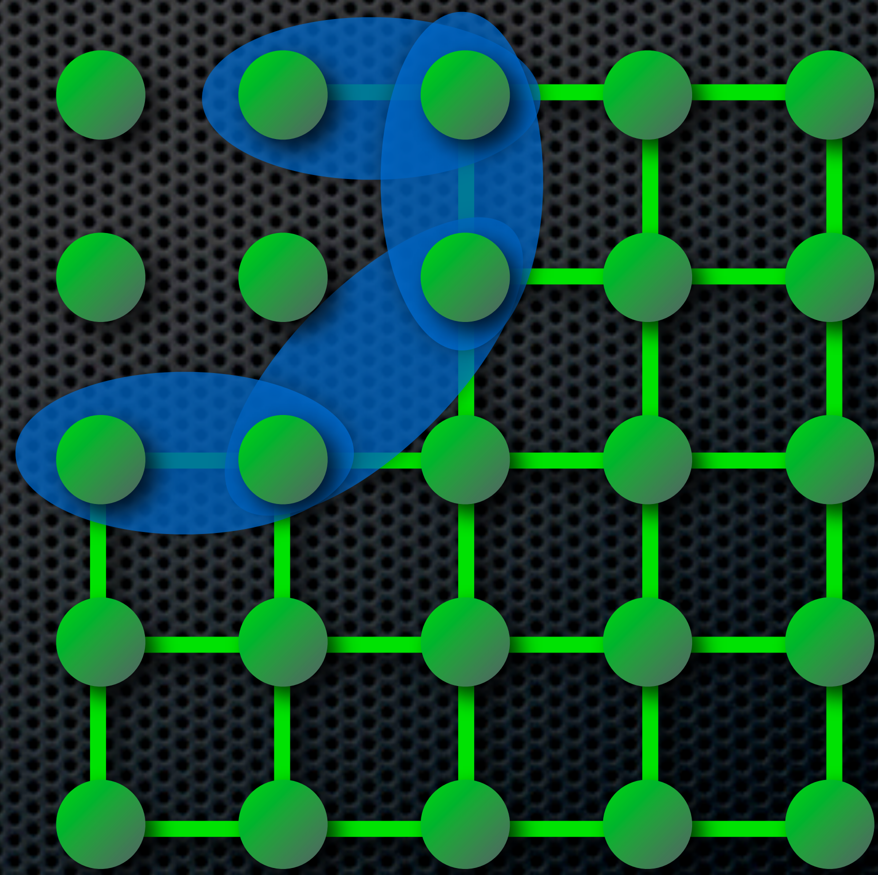
$|\psi_2\rangle$

Raussendorf & Briegel PRL 2001

Measurement-based QC

- prepare X eigenstates
- entangle neighbors with a Z-Z coupling
- Build a large lattice for universality: the CLUSTER STATE
- arbitrary single-qubit measurements with feedforward to compute



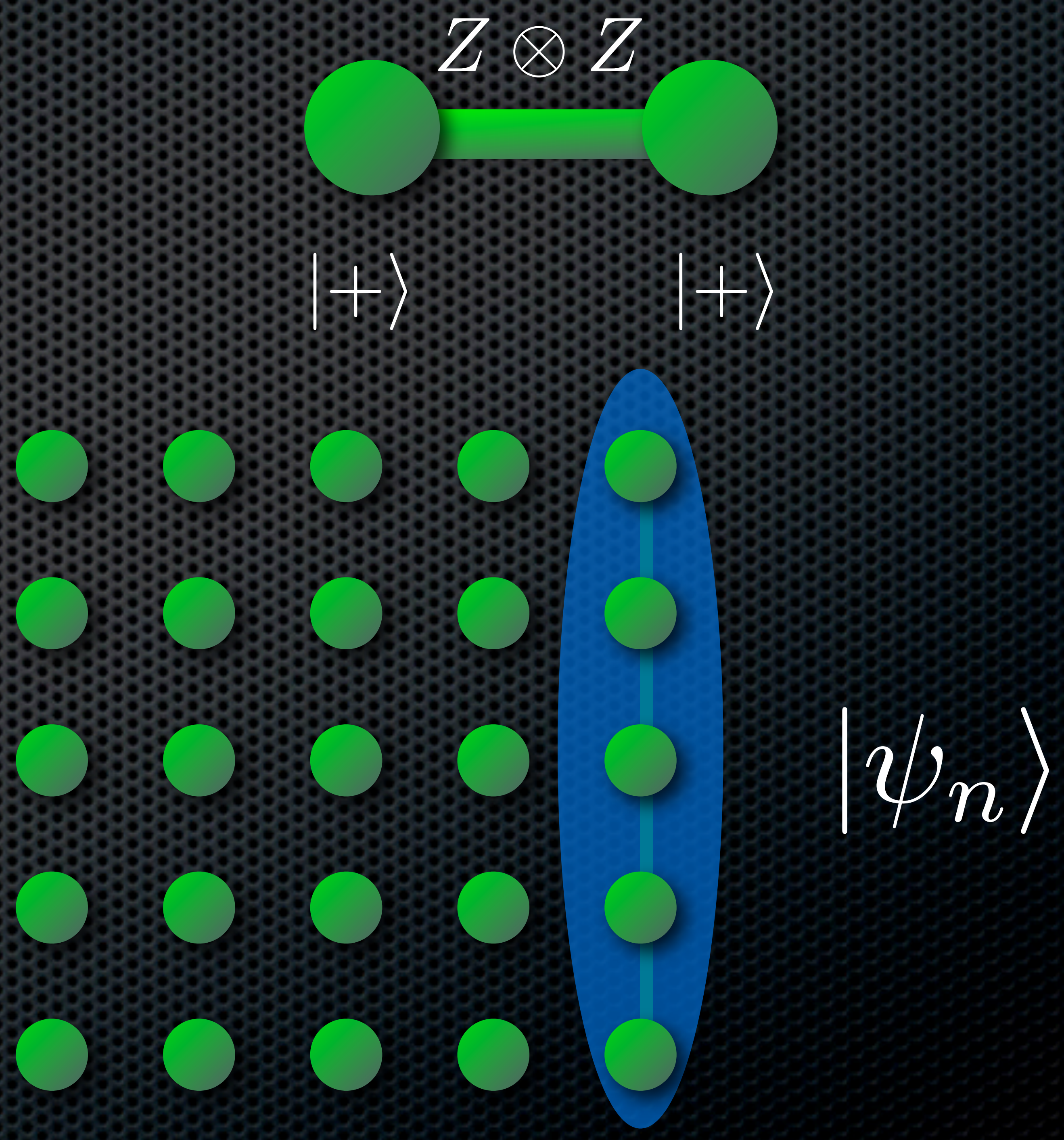


$$|\psi_3\rangle$$

Raussendorf & Briegel PRL 2001

Measurement-based QC

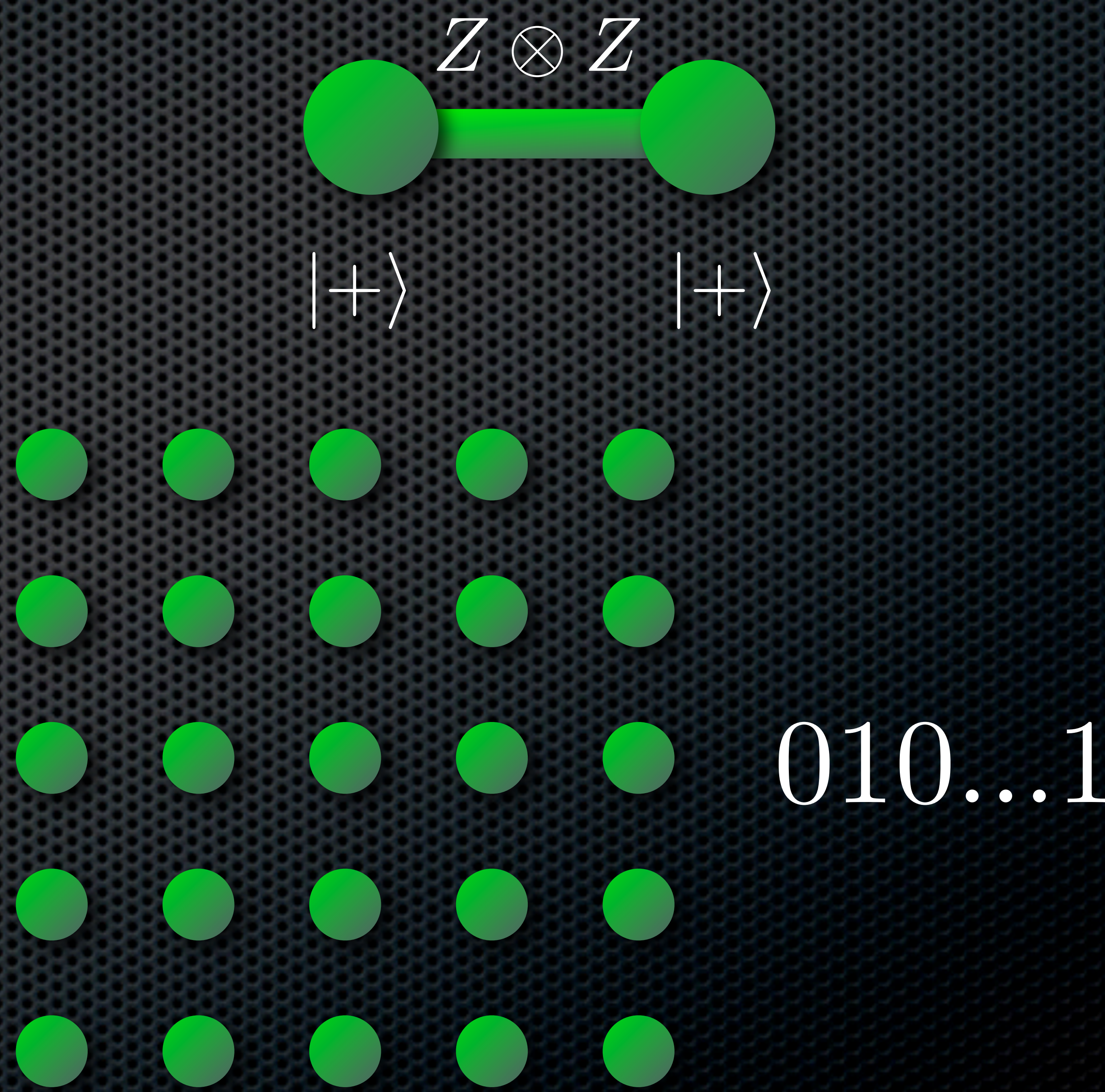
- prepare X eigenstates
- entangle neighbors with a Z-Z coupling
- Build a large lattice for universality:
  the CLUSTER STATE
- arbitrary single-qubit measurements with feedforward to compute



Raussendorf & Briegel PRL 2001

Measurement-based QC

- prepare X eigenstates
- entangle neighbors with a Z-Z coupling
- Build a large lattice for universality:
  the CLUSTER STATE
- arbitrary single-qubit measurements with feedforward to compute



Raussendorf & Briegel PRL 2001

- In general, MBQC requires:

- In general, MBQC requires:
  - A family of n qubit quantum states

- In general, MBQC requires:
  - A family of n qubit quantum states

- In general, MBQC requires:
  - A family of n qubit quantum states

$$|\Psi\rangle$$

- In general, MBQC requires:
  - A family of n qubit quantum states
  - A classical control computer determines where to measure, the measurement basis and how to interpret the measurement outcomes

$$|\Psi\rangle$$

- In general, MBQC requires:
  - A family of n qubit quantum states
  - A classical control computer determines where to measure, the measurement basis and how to interpret the measurement outcomes

$$|\Psi\rangle$$

- In general, MBQC requires:
  - A family of n qubit quantum states
  - A classical control computer determines where to measure, the measurement basis and how to interpret the measurement outcomes

1

$|\Psi\rangle$

- In general, MBQC requires:
  - A family of n qubit quantum states
  - A classical control computer determines where to measure, the measurement basis and how to interpret the measurement outcomes

1

$|\Psi'\rangle$

- In general, MBQC requires:
  - A family of n qubit quantum states
  - A classical control computer determines where to measure, the measurement basis and how to interpret the measurement outcomes

$$|\Psi'\rangle$$

- In general, MBQC requires:
  - A family of n qubit quantum states
  - A classical control computer determines where to measure, the measurement basis and how to interpret the measurement outcomes

$$|\Psi'\rangle$$

- Without initial entanglement, it’s clear you can’t do better than BPP.

Universality and entanglement

Question:

What are the necessary and sufficient conditions for a family of n qubit quantum states to be universal for MBQC?

Universality and entanglement

Question:

What are the necessary and sufficient conditions for a family of n qubit quantum states to be universal for MBQC?

Necessary conditions:

van den Nest, Miyake, Dür, Briegel 2006

find entanglement measures that must grow “quickly” with n.

Universality and entanglement

Question:

What are the necessary and sufficient conditions for a family of n qubit quantum states to be universal for MBQC?

Sufficient conditions:

Gross, Eisert, Schuch, Pérez-García 2007

find states with special structure in the many-body correlations.

Brennen & Miyake 2008, Doherty & Bartlett 2008

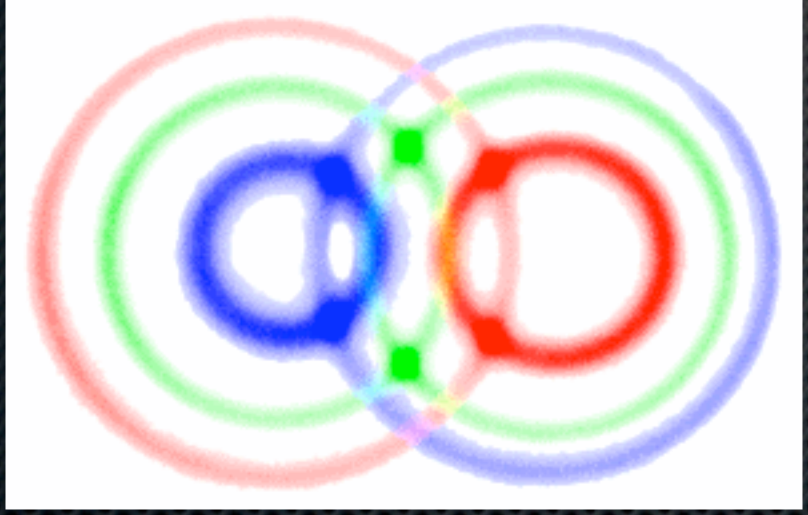
find *ground states* with special structure.

Bridging the divide

Quantum world	Classical world

Bridging the divide

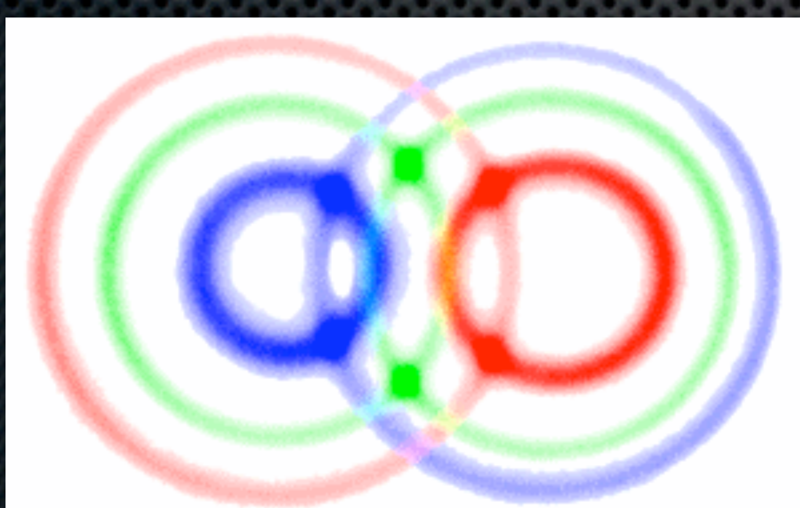
Quantum world	Classical world
Entanglement and correlations	



Bridging the divide

Quantum world

Entanglement
and
correlations

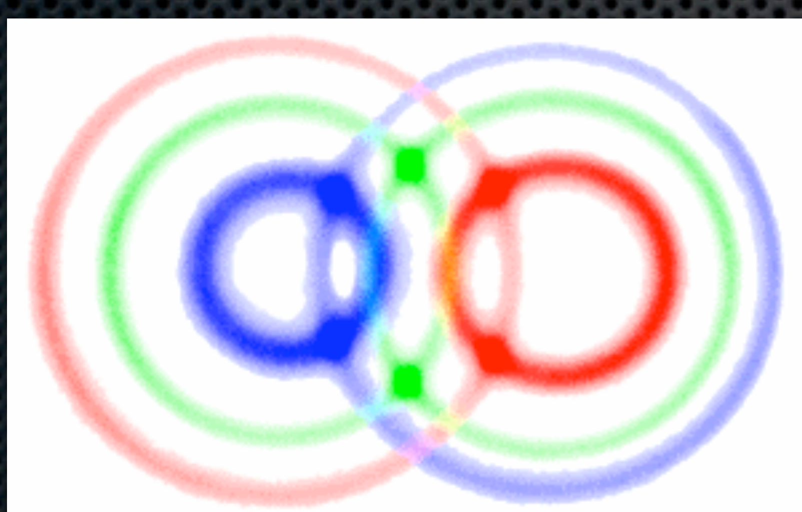


Classical world

Local bases,
Limited processing
power.

Bridging the divide

Quantum world	Classical world
Entanglement and correlations	Local bases, Limited processing power.



MBQC

Local bases, geometric measure

$$E_g(\Psi) = -\log_2 \sup_{\alpha \in \mathcal{P}} |\langle \alpha | \Psi \rangle|^2$$

the set of product states

Answers the question:
How far is the nearest
collection of local bases
$\alpha_1, \alpha_2, \ldots, \alpha_n$?

Large geometric measure

⇕

Far from all product states

Local bases, geometric measure

$$E_g(\Psi) = -\log_2 \sup_{\alpha \in \mathcal{P}} |\langle \alpha | \Psi \rangle|^2$$

the set of product states

Answers the question:
How far is the nearest collection of local bases $\alpha_1, \alpha_2, \ldots, \alpha_n$?

Large geometric measure

⇕

Far from all product states

Theorem 1 (GFE): n qubit states with $E_g > n - O(\log n)$ are useless for MBQC.

Local bases, geometric measure

For concreteness, a state is useless if it fails to provide a polynomial-time MBQC algorithm for Factoring.

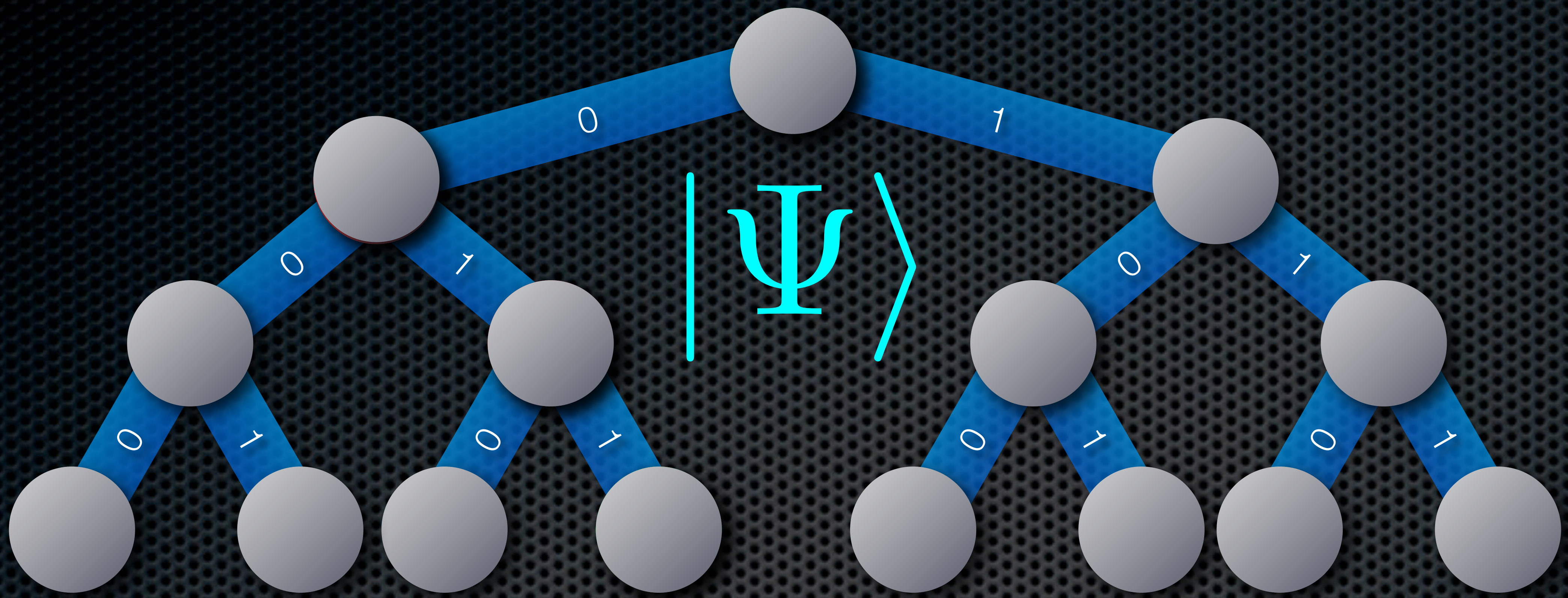
Theorem 1 (GFE): n qubit states with $E_g > n - O(\log n)$ are useless for MBQC.

Local bases, geometric measure

For concreteness, a state is useless if it fails to provide a polynomial-time MBQC algorithm for Factoring.

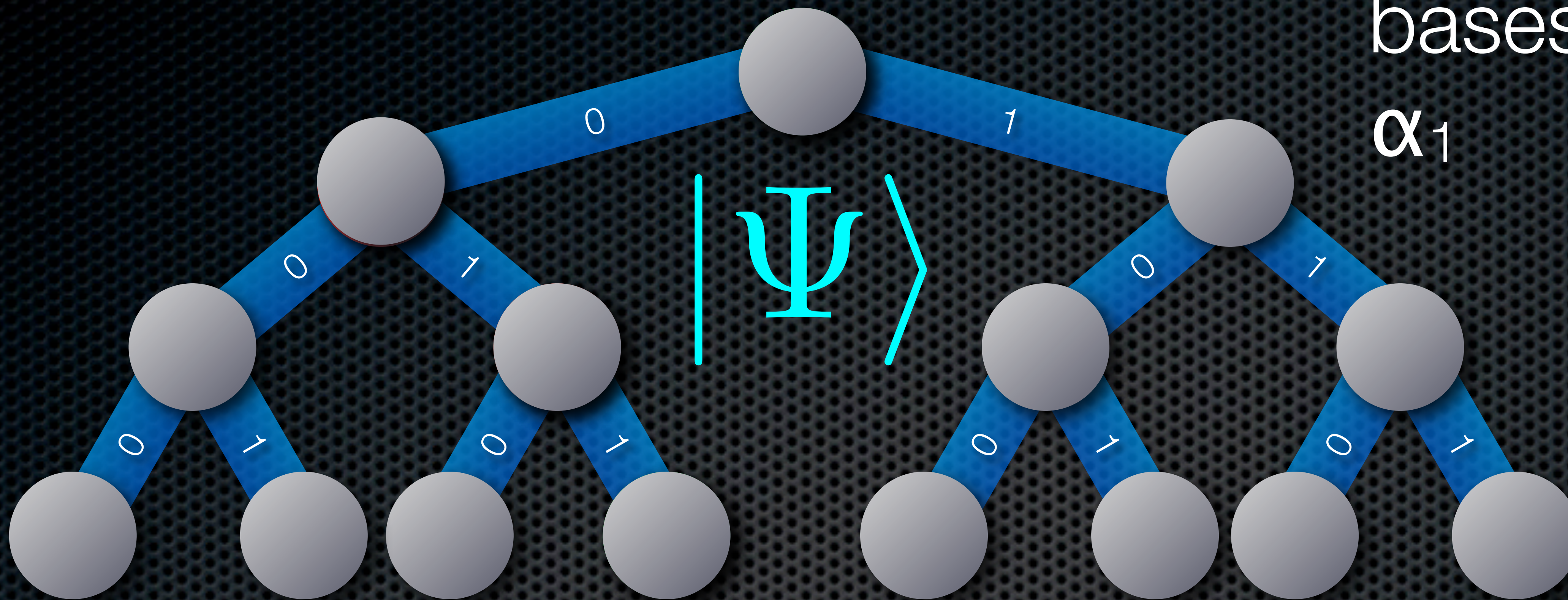
Proof strategy: replace ψ with a classical coin and show there exists a classical algorithm that factors just as well (within poly factors).

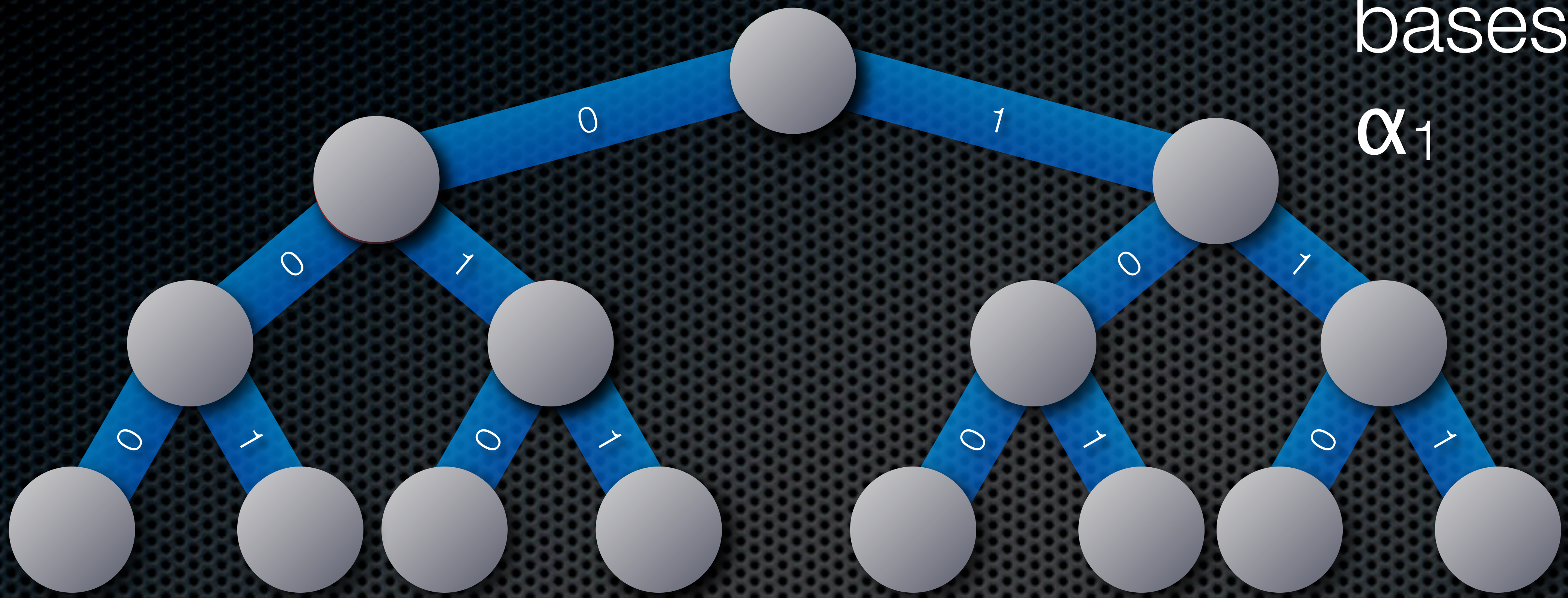
Theorem 1 (GFE): n qubit states with $E_g > n - O(\log n)$ are useless for MBQC.


0
1
0
1
0
1
0
1
0
1
0
1
0
1
$|\Psi\rangle$

bases:

α_1



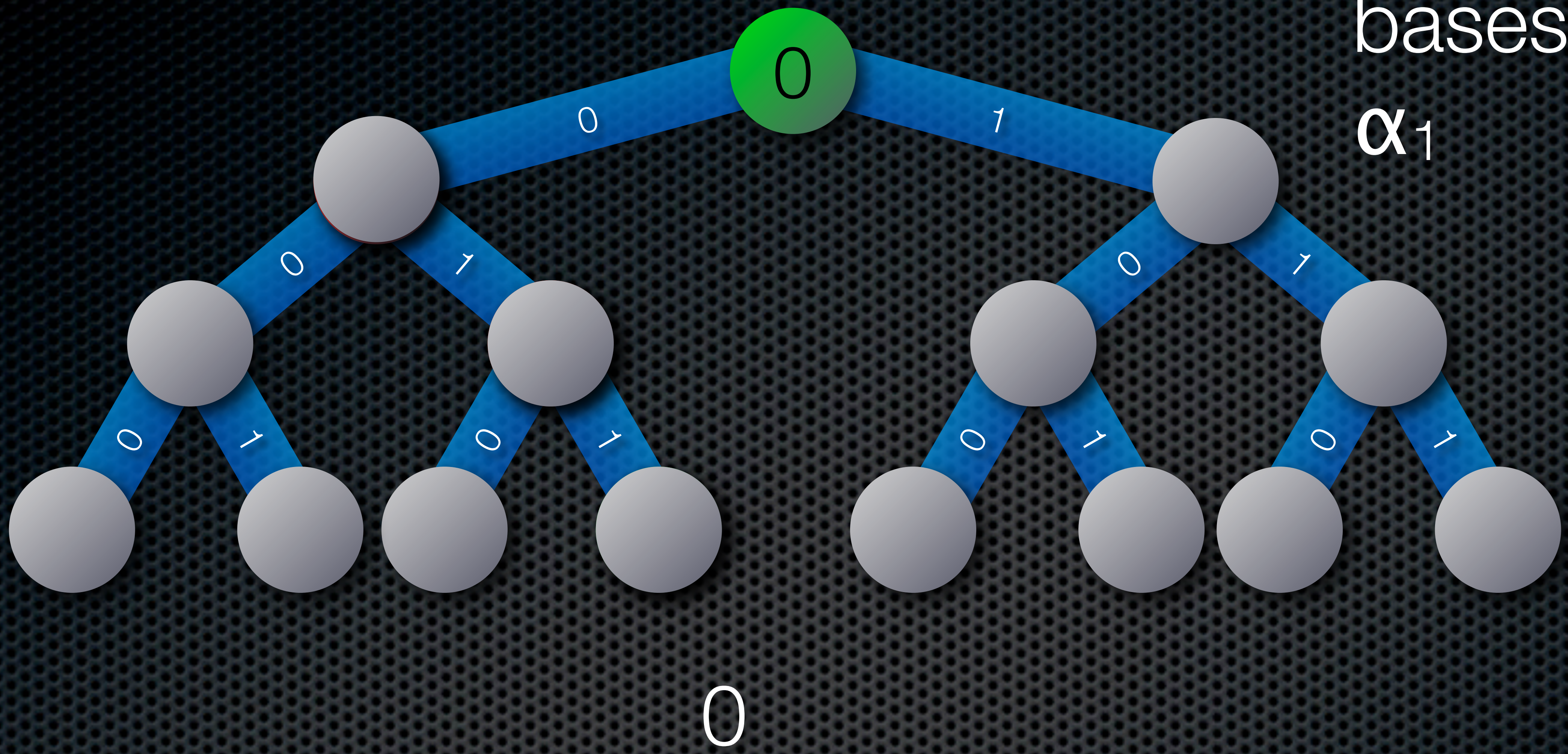


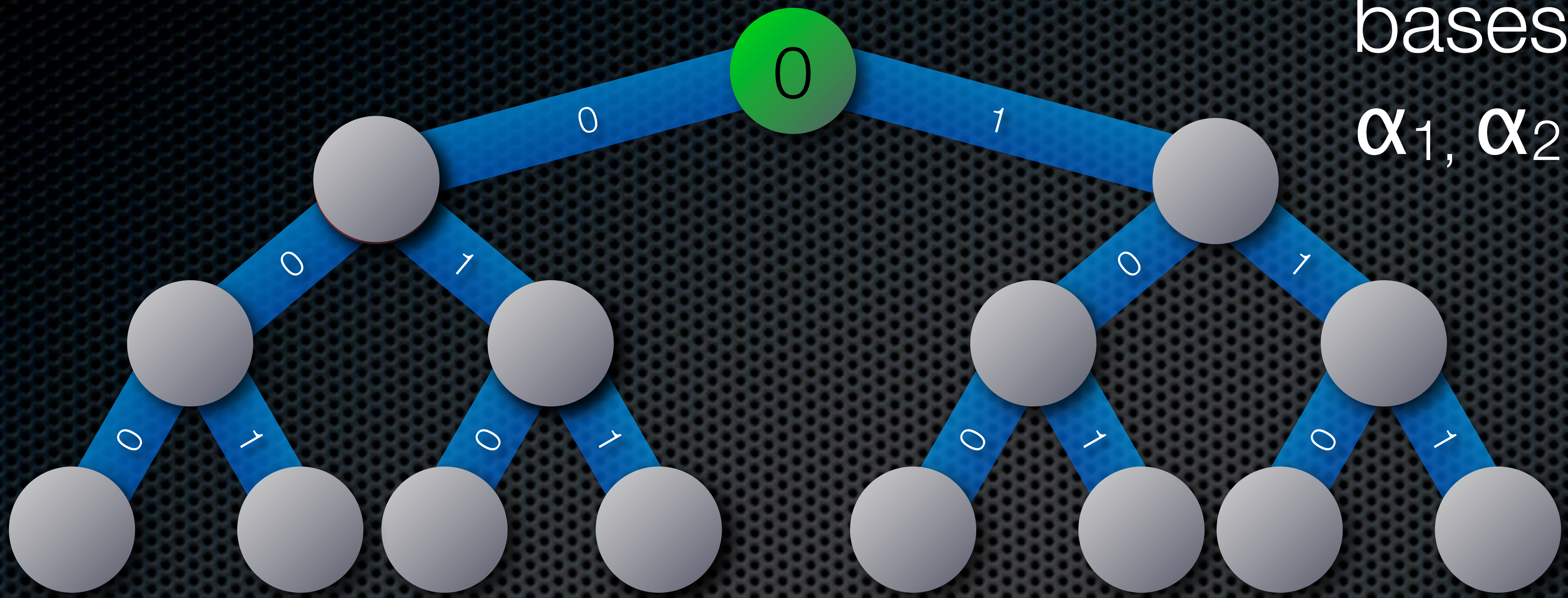
bases:

α_1

bases:

α_1

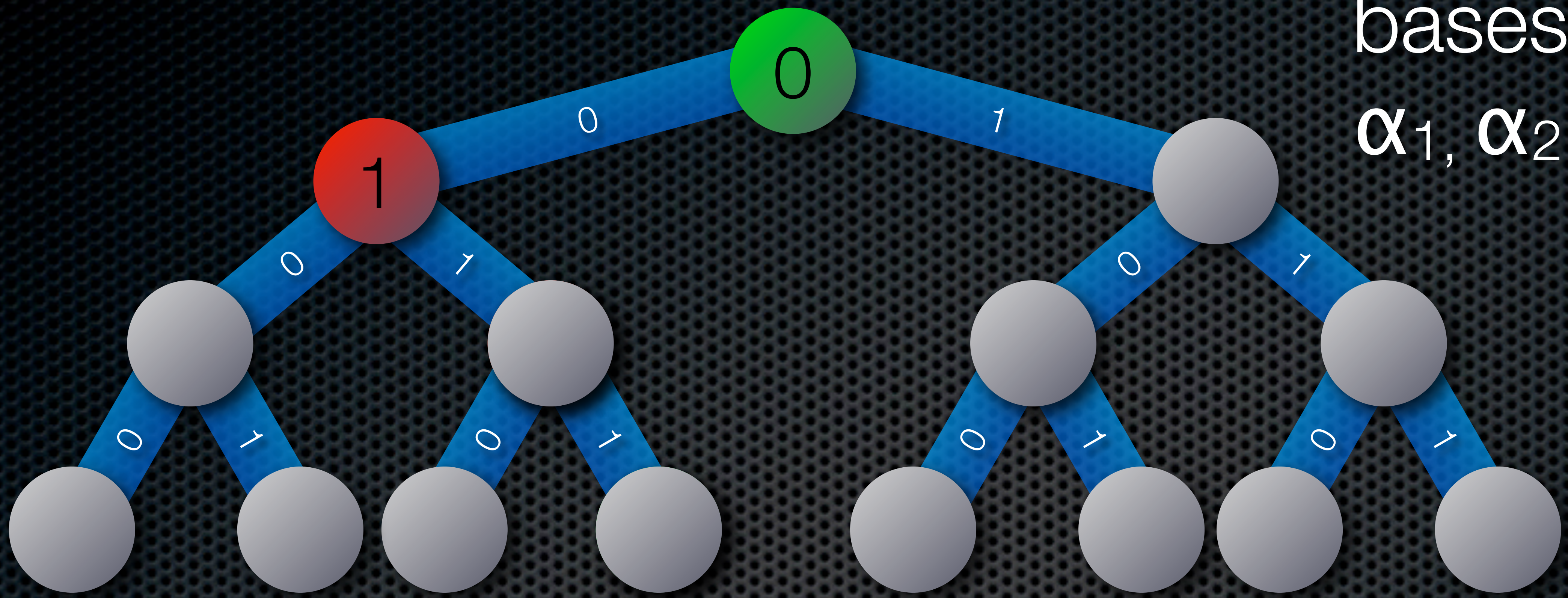




bases:

α_1, α_2

0



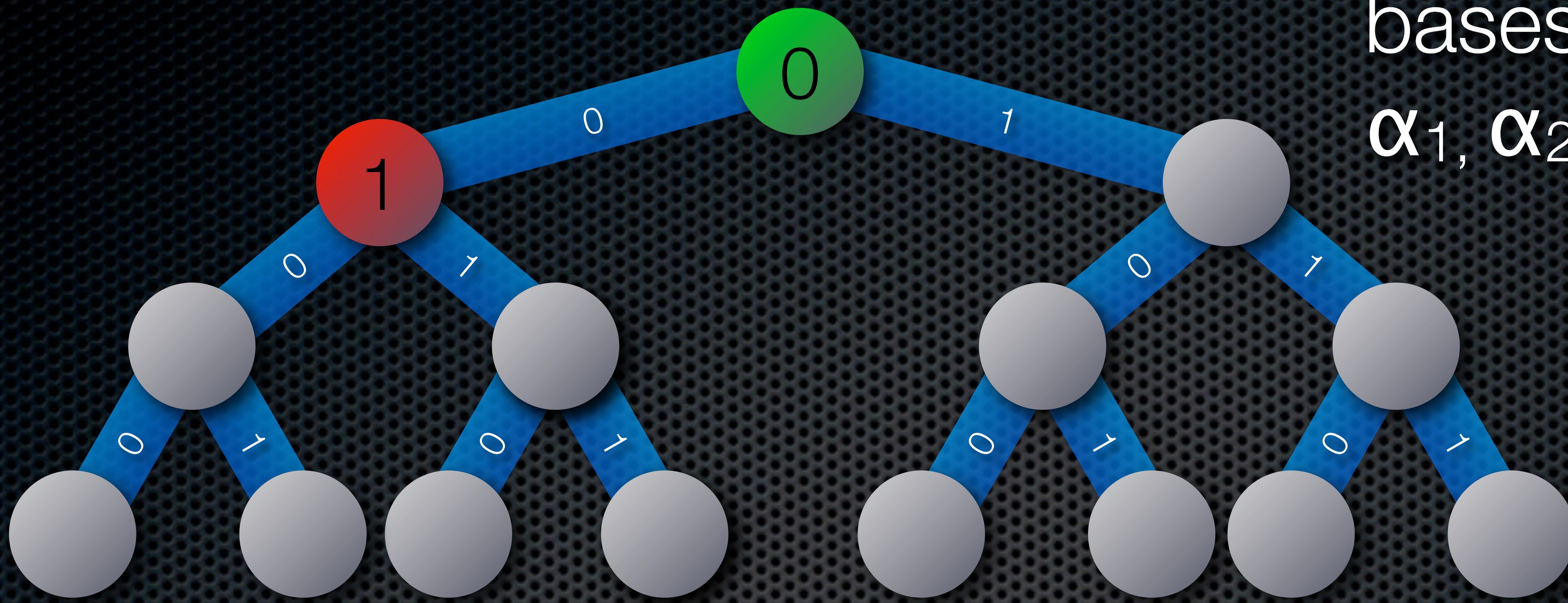
bases:

α_1, α_2

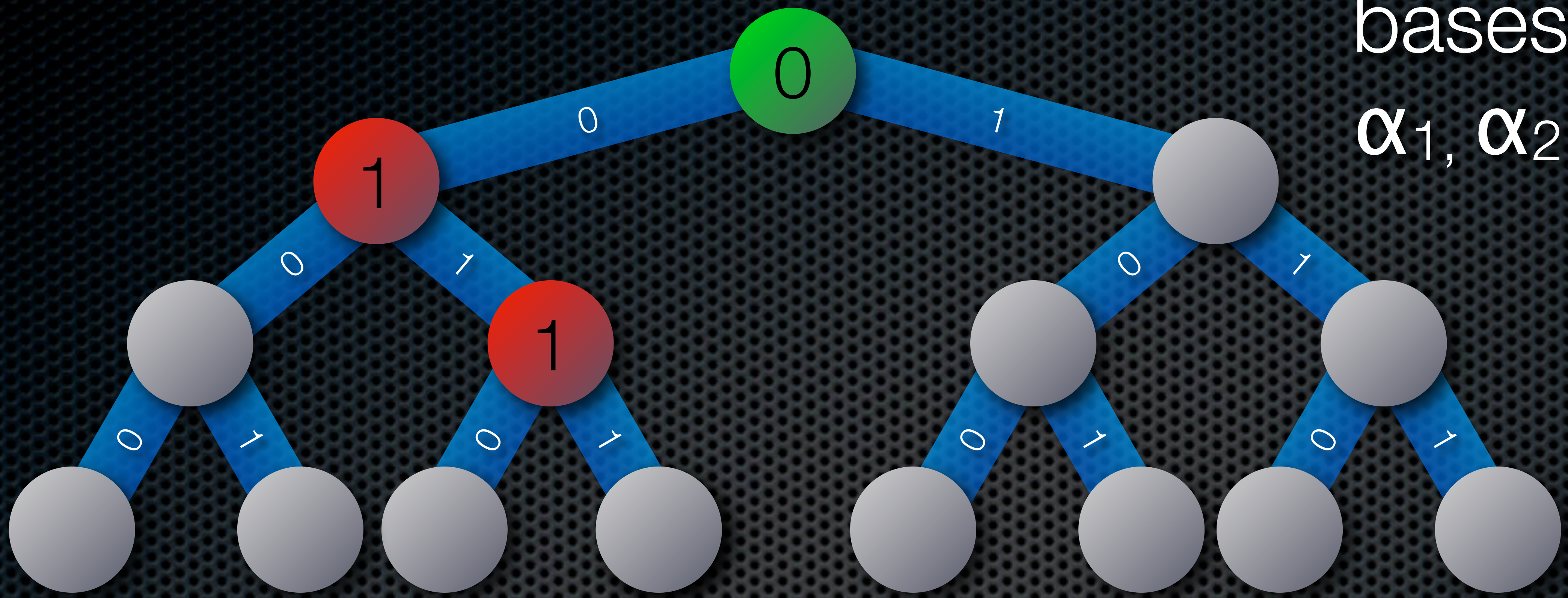
01

bases:

$\alpha_1, \alpha_2, \alpha_3$



01



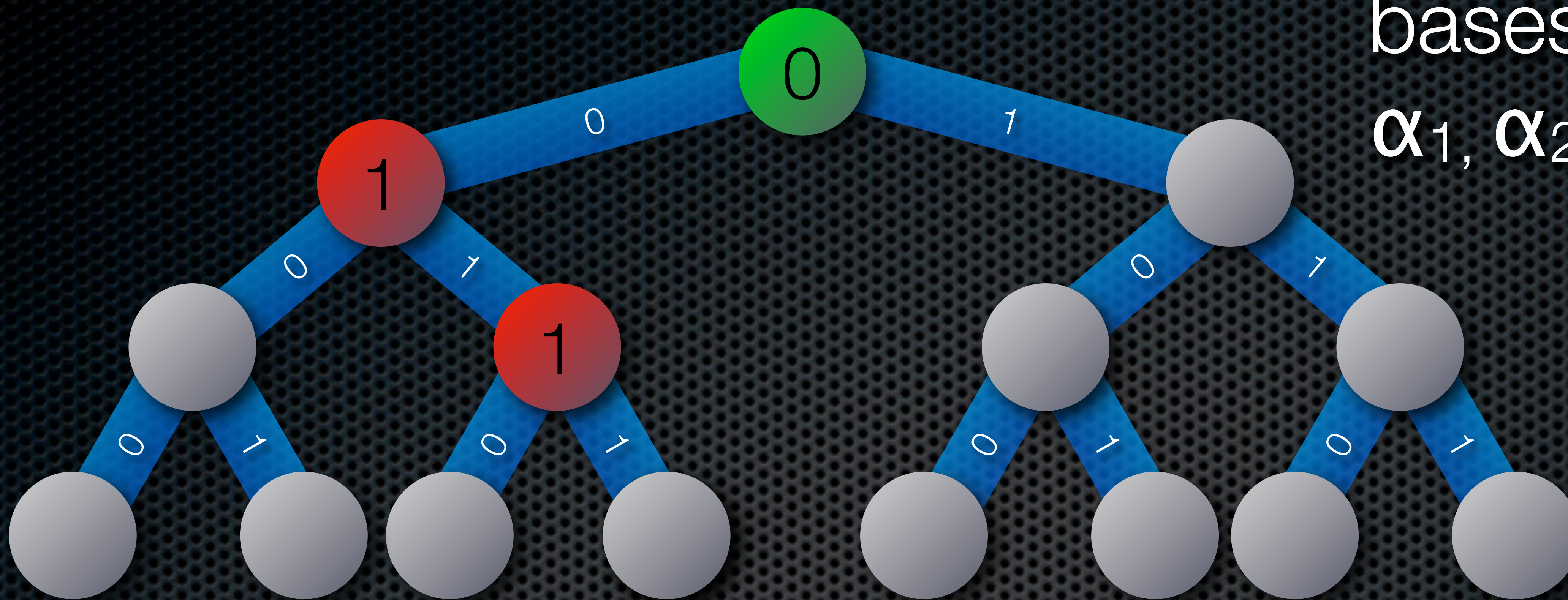
bases:

$\alpha_1, \alpha_2, \alpha_3$

011

bases:

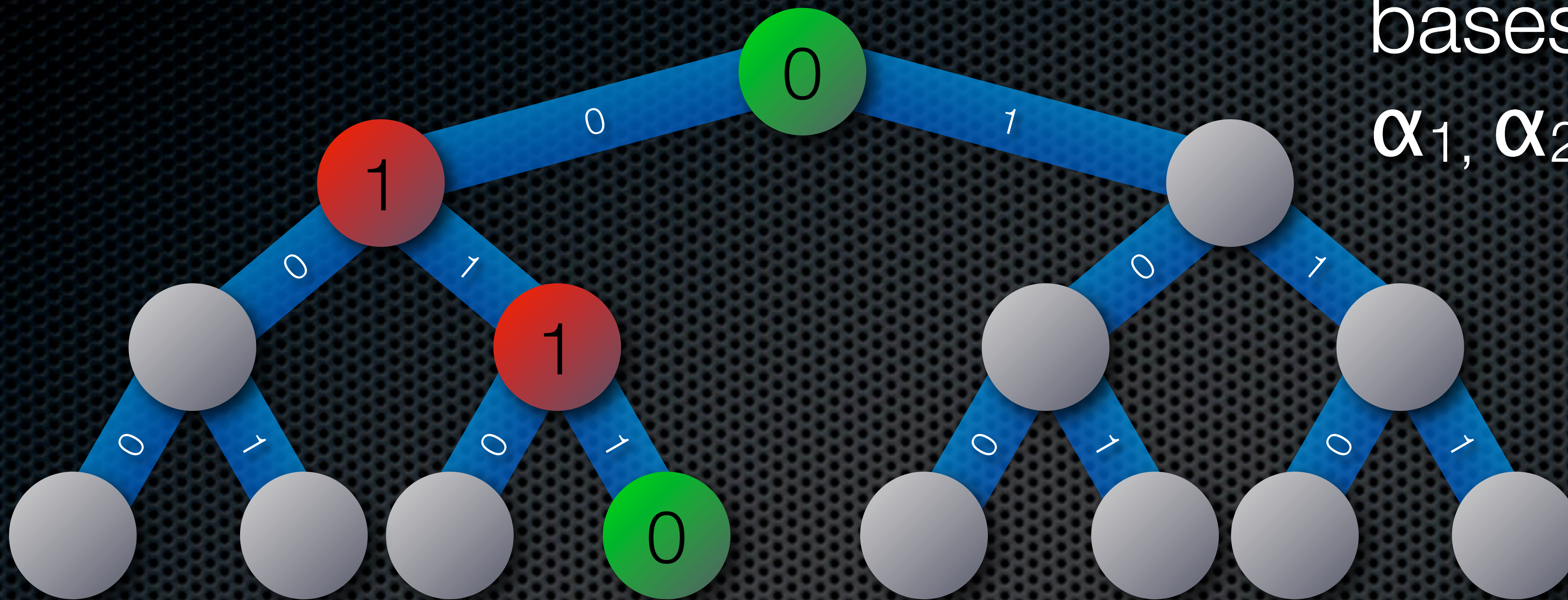
$\alpha_1, \alpha_2, \alpha_3, \alpha_4$



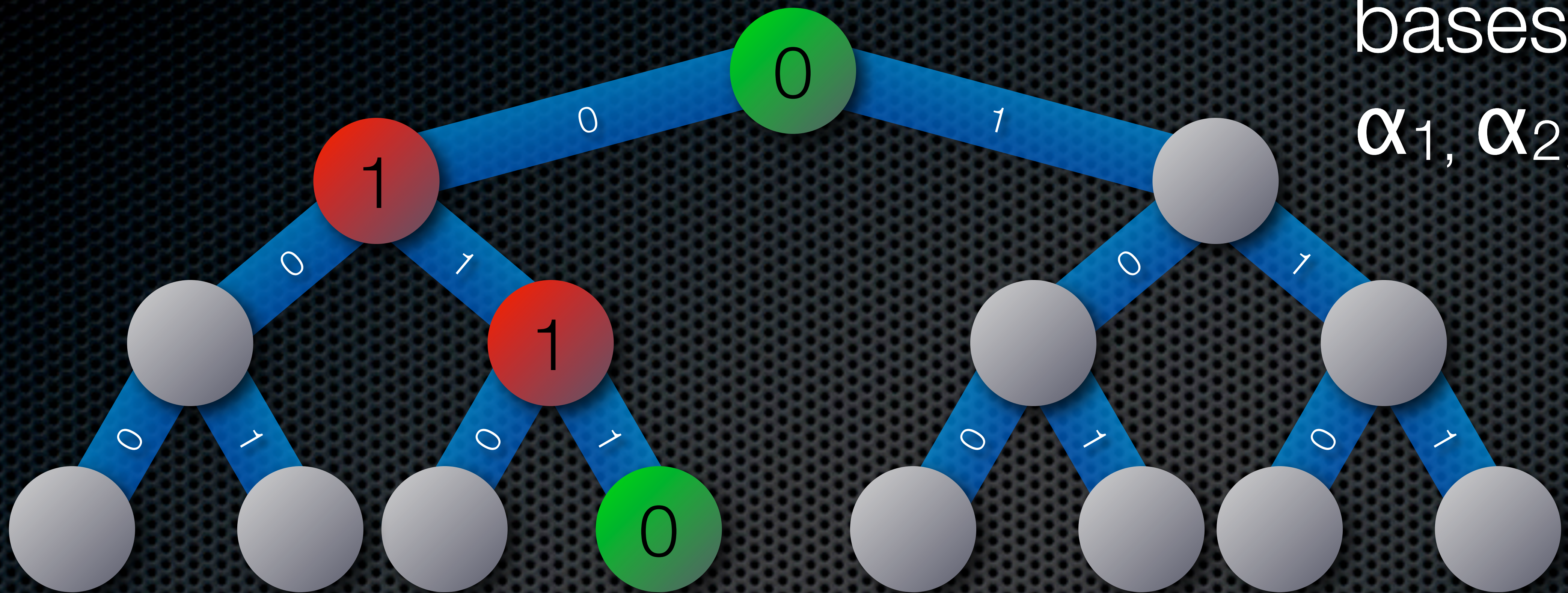
011

bases:

$\alpha_1, \alpha_2, \alpha_3, \alpha_4$



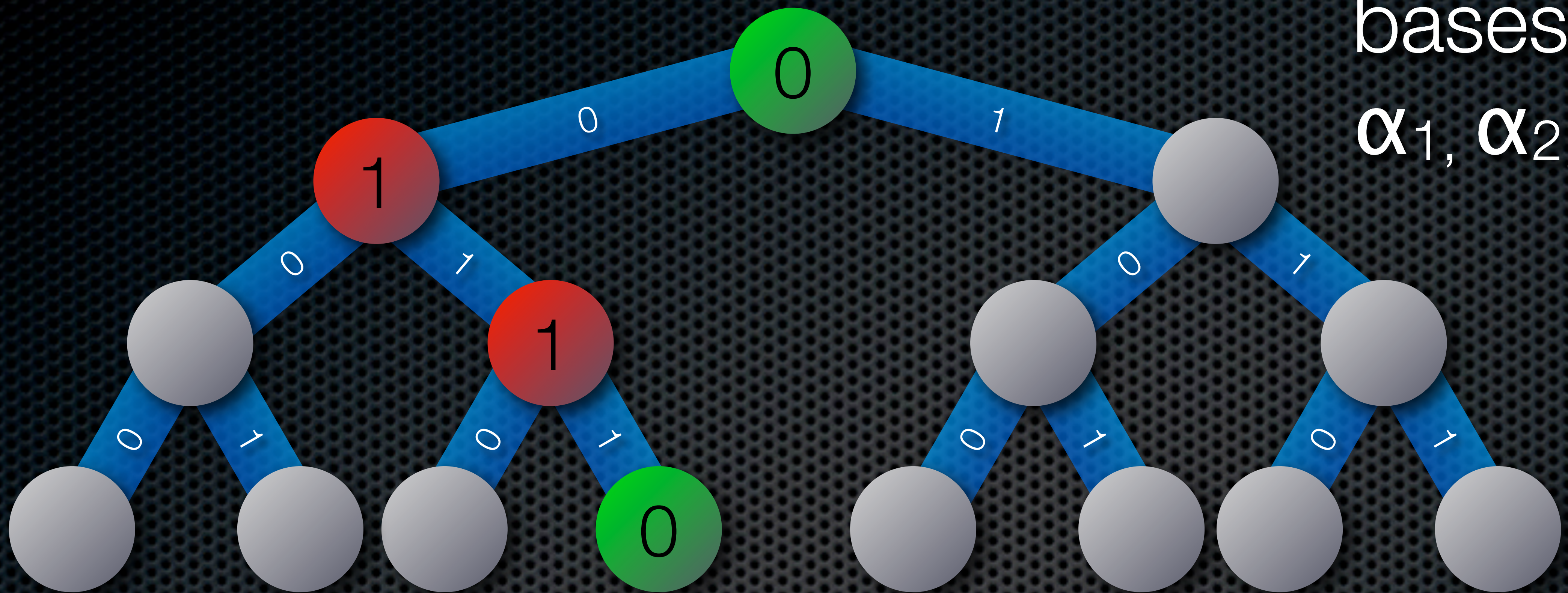
0110



bases:

$\alpha_1, \alpha_2, \alpha_3, \alpha_4$

The “good” outcomes G cause the classical control computer to output a valid factorization. We want this to succeed with constant probability, say p>.5



bases:

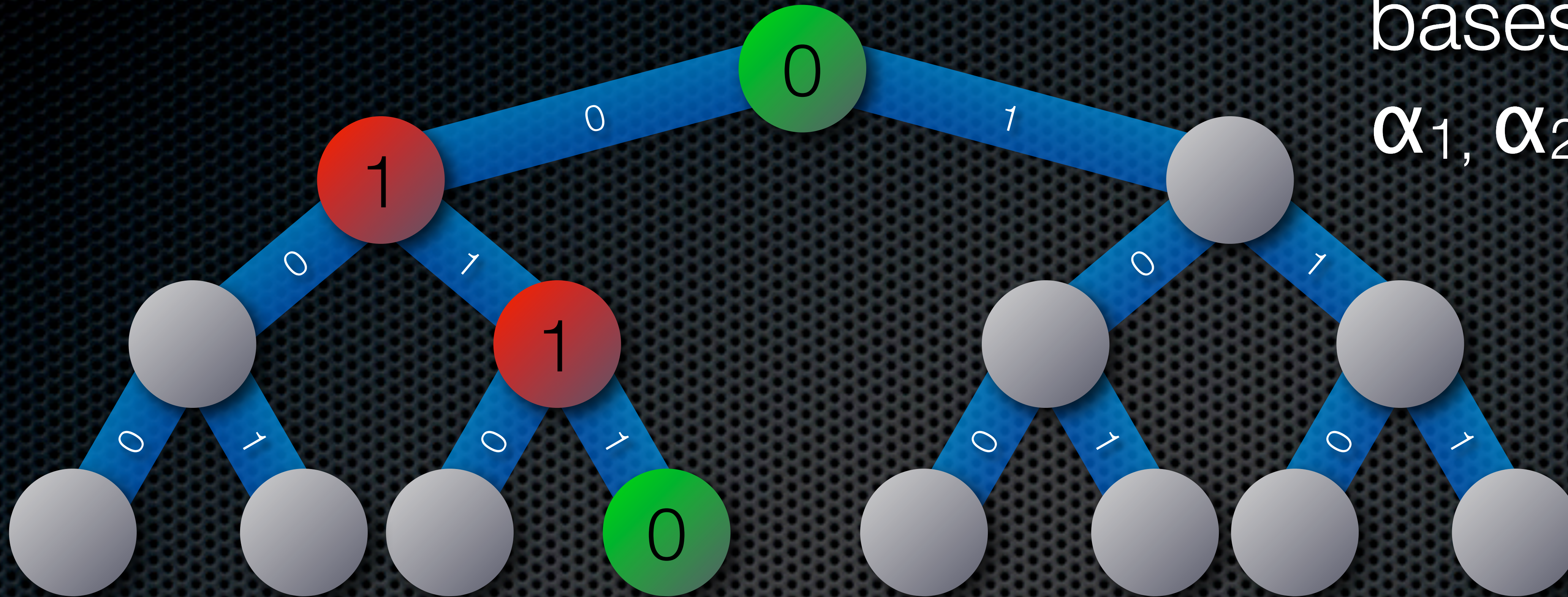
$\alpha_1, \alpha_2, \alpha_3, \alpha_4$

The "good" outcomes G cause the classical control computer to output a valid factorization. We want this to succeed with constant probability, say p>.5

Suppose

$E_g > n-\delta$,

$\delta = O(\log n)$



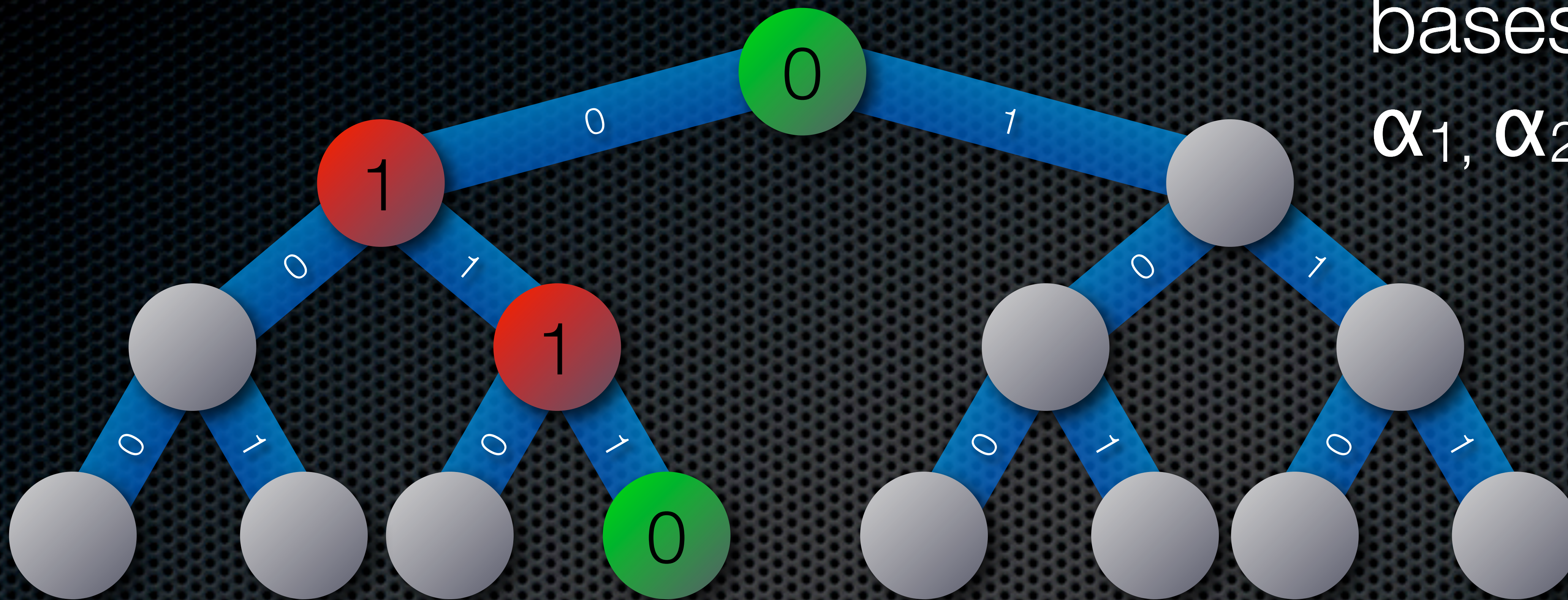
bases:
$\alpha_1, \alpha_2, \alpha_3, \alpha_4$

The "good" outcomes G cause the classical control computer to output a valid factorization. We want this to succeed with constant probability, say p>.5

Suppose $E_g > n-\delta$, $\delta = O(\log n)$

$$|\langle\alpha|\Psi\rangle|^2 \leq 2^{-E_g} \leq 2^{-n+\delta}$$

$$\Rightarrow \frac{|G|}{2^n} > 2^{-\delta-1} = \text{poly}(1/n).$$



bases:

$\alpha_1, \alpha_2, \alpha_3, \alpha_4$

The "good" outcomes G cause the classical control computer to output a valid factorization. We want this to succeed with constant probability, say p>.5

Suppose $E_g > n-\delta$, $\delta = O(\log n)$

$$|\langle\alpha|\Psi\rangle|^2 \le 2^{-E_g} \le 2^{-n+\delta}$$

$$\Rightarrow \frac{|G|}{2^n} > 2^{-\delta-1} = \text{poly}(1/n).$$

To simulate classically, just ignore the measurement results and use a classical coin!

Large geometric measure → Useless for MBQC

Large geometric measure → Useless for MBQC

This is vacuous unless such states exist.

Large geometric measure → Useless for MBQC

This is vacuous unless such states exist.

In fact, they are abundant.

Theorem 2 (GFE): The fraction of n qubit states with

$E_g < n - O(\log n)$

is less than $\exp(-n^2)$.

Large geometric measure → Useless for MBQC

This is vacuous unless such states exist.

In fact, they are abundant.

Theorem 2 (GFE): The fraction of n qubit states with $E_g < n - O(\log n)$ is less than $\exp(-n^2)$.

The proof involves standard measure concentration arguments (via ϵ-nets) and known results about random states

Random states
are extravagant.

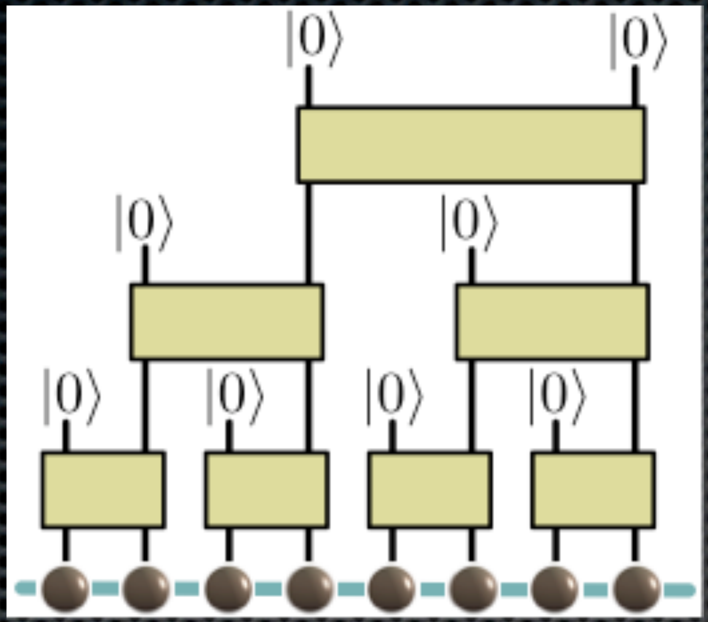
Random states are extravagant.

Random states are extravagant.

Can provably useless states be created efficiently?

Random states are extravagant.

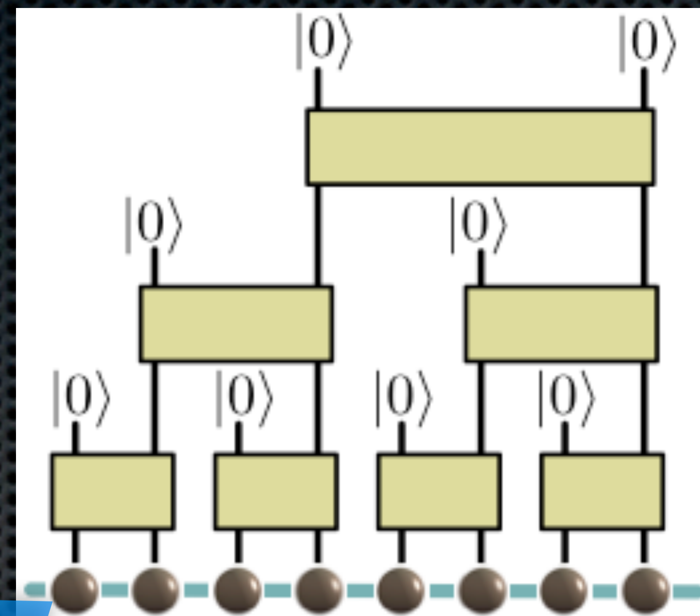
Can provably useless states be created efficiently?



We can get to $E_g > n - o(n)$ using a TTN construction.

Random states are extravagant.

Can provably useless states be created efficiently?

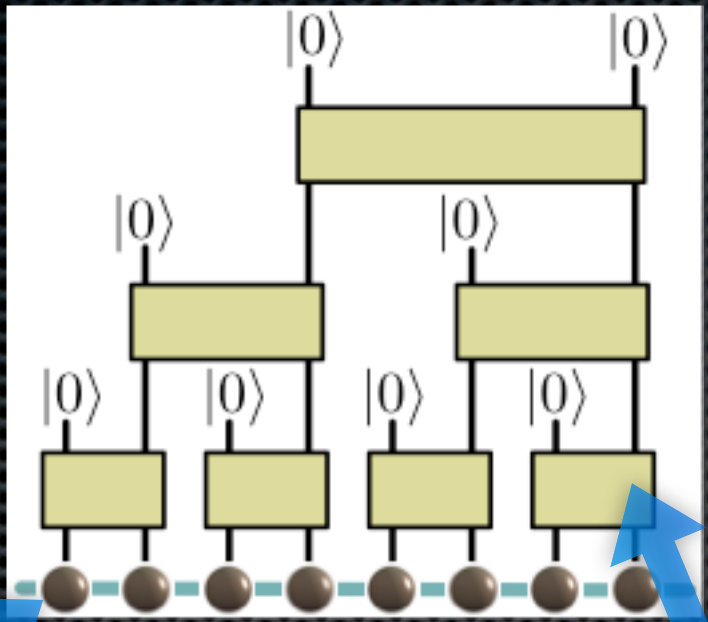


d-level systems

We can get to $E_g > n - o(n)$ using a TTN construction.

Random states are extravagant.

Can provably useless states be created efficiently?



We can get to $E_g > n-o(n)$ using a TTN construction.

d-level systems

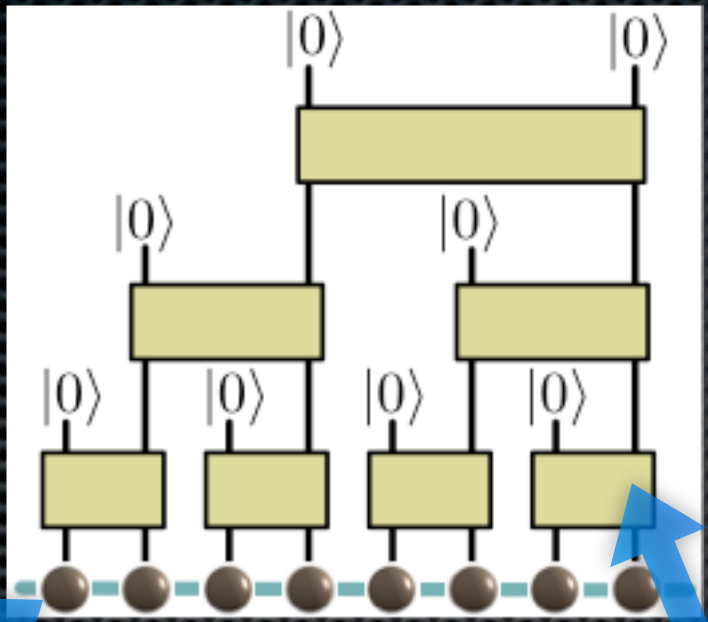
Isometry V = V(U)

$$V : \mathbb{C}^d \to \mathbb{C}^d \otimes \mathbb{C}^d$$

$$V|\beta\rangle = U|0\rangle \otimes |\beta\rangle$$

Random states are extravagant.

Can provably useless states be created efficiently?



We can get to $E_g > n-o(n)$ using a TTN construction.

d-level systems

Isometry V = V(U)

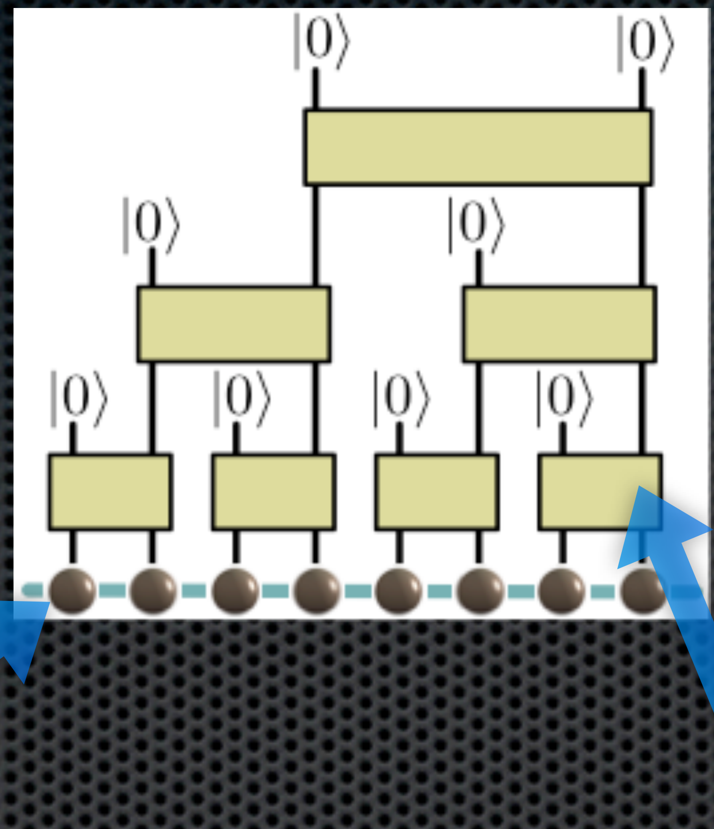
$$V : \mathbb{C}^d \to \mathbb{C}^d \otimes \mathbb{C}^d$$

$$V|\beta\rangle = U|0\rangle \otimes |\beta\rangle$$

Concatenate to get the state of 2^k qudits at level k.

Random states are extravagant.

Can provably useless states be created efficiently?



We can get to $E_g > n - o(n)$ using a TTN construction.

d-level systems

Isometry V = V(U)

$$V : \mathbb{C}^d \to \mathbb{C}^d \otimes \mathbb{C}^d$$

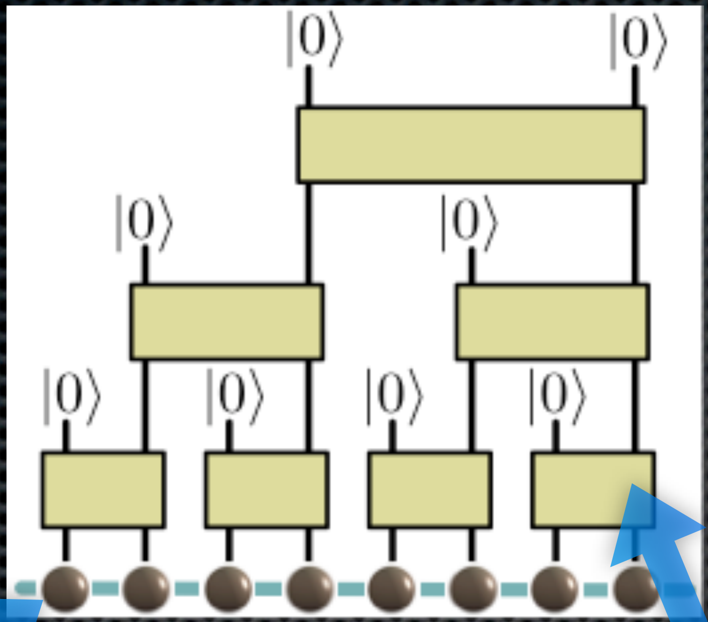
$$V|\beta\rangle = U|0\rangle \otimes |\beta\rangle$$

Concatenate to get the state of 2^k qudits at level k.

Now choose each U randomly, and let d grow slowly, $(\log n)^{1/2}$.

Random states are extravagant.

Can provably useless states be created efficiently?



We can get to $E_g > n-o(n)$ using a TTN construction.

d-level systems

Isometry V = V(U)

$$V : \mathbb{C}^d \to \mathbb{C}^d \otimes \mathbb{C}^d$$

$$V|\beta\rangle = U|0\rangle \otimes |\beta\rangle$$

Concatenate to get the state of 2^k qudits at level k.

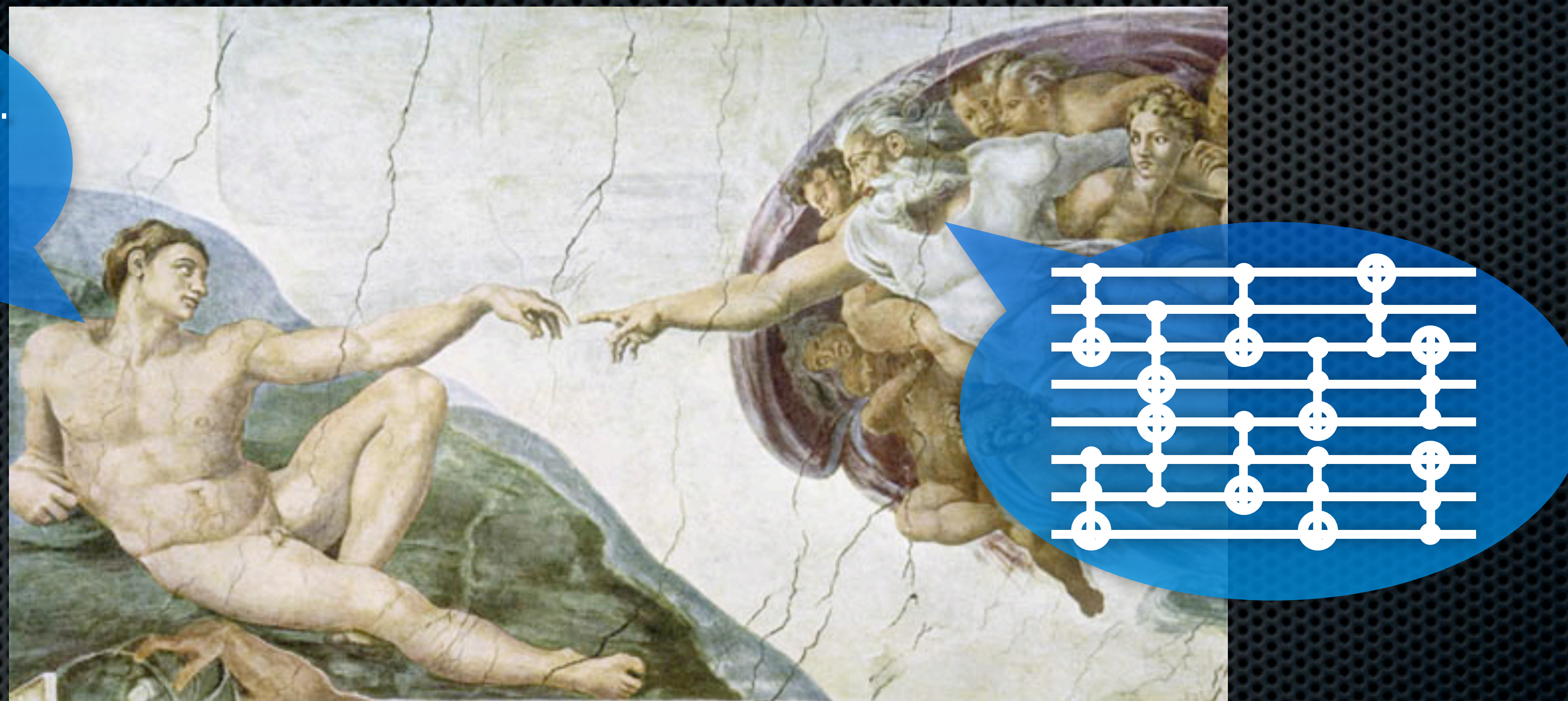
Now choose each U randomly, and let d grow slowly, $(\log n)^{1/2}$.

$E_g > n - o(n)$

Decision problems

I have a generic Ψ.
Can I compute
anything with it?

$$|\Psi\rangle$$



- For almost every state Ψ, there is no poly-bounded classical control circuit which allows a significant advantage over classical randomness.
  Only problems in BPP can be solved. (BMW '08)

$$\Pr_{\Psi}\left\{\exists C \ \left|C(\Psi) - C(2^{-n}\mathbb{1})\right| > \epsilon\right\} \leq \left(8^8 w\right)^{3v} e^{-c\epsilon^2 2^n}$$

Randomness vs entanglement?

Random states such that $E_g \leq \log K + O(1)$ also offer no advantage!

- Choose nK states at random from $\mathbb{C}^2$ to construct the following (where K is superpolynomial in n):

$$R := \sum_{j=1}^{K} |\psi_j^{(1)}\rangle\langle\psi_j^{(1)}| \otimes \cdots \otimes |\psi_j^{(n)}\rangle\langle\psi_j^{(n)}|$$

- Randomly pick a state from the support of R then:

$$|\Psi\rangle = \frac{1}{\sqrt{\langle\Psi_0|R|\Psi_0\rangle}} \sqrt{R}|\Psi_0\rangle$$

$$\Pr_\Psi \left\{\exists C \; \left|C(\Psi) - C(2^{-n}\mathbb{1})\right| > \epsilon\right\} \leq \left(2^n + \left(8^8 w\right)^{3v}\right) e^{-c'\epsilon^2 K^{1/3}}$$

Questions

- Can we derandomize these constructions?
- Can Hastings' techniques give improved bounds?
- Are efficiently created states subject to this effect?
- What happens with a polynomial number of copies?
- What implications does this have for the circuit model?