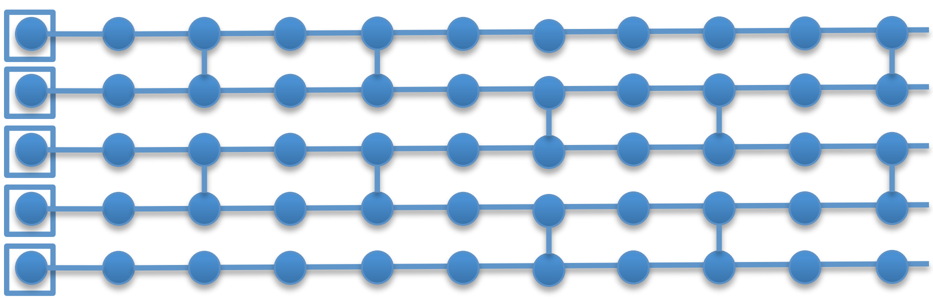
# Efficient pseudorandomness and computational hardness with simple graph states

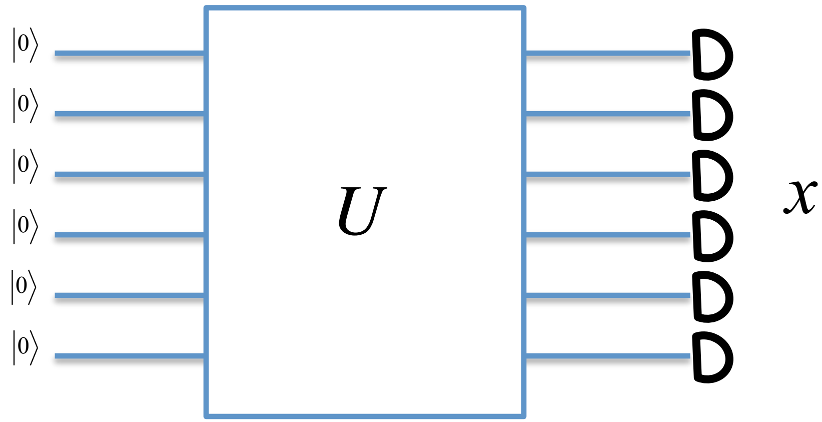
Damian Markham (LIP6), Rawad Mezher (LIP6+Lebanese Uni), Joe Ghalbouni (Lebanese Uni), Joseph Dgheim (Lebanese Uni)



PRA 97, 0233 (2018), in preperation

# Hardness of sampling

e.g. IQP..




Sampling Dx, impossible classically efficiently, if

i) the polynomial hierarchy does not collapse

ii) average case version of hard problem also hard

iii) output not too peaked (anti-concentration)

*Benchmark for quantum technologies*

# Random unitaries and t-designs

Applying $U$ chosen at random (Haar measure)

- Hiding quantum information
- Random encoding of information
- Benchmarking
- Checking entanglement
- Generation of topological order
- Demonstrating quantum supremacy
  - Boson sampling / IQP
- …

# Random unitaries and t-designs

Applying $U$ chosen at random (Haar measure)

- **Hiding quantum information**
- Random encoding of information
- Benchmarking
- Checking entanglement
- Generation of topological order
- Demonstrating quantum supremacy
  - Boson sampling / IQP
- ...

$$U\left|\varphi\right\rangle \sim I$$

Randomly applied U, state
looks like identiy

# Random unitaries and t-designs

Applying $U$ chosen at random (Haar measure)

- Hiding quantum information
- Random encoding of information
- **Benchmarking**
- Checking entanglement
- Generation of topological order
- Demonstrating quantum supremacy
  - Boson sampling / IQP
- …


Comparing input output with
random unitaries can
estimate noise/properties of $\Gamma$

# Random unitaries and t-designs

Applying $U$ chosen at random (Haar measure)

- Hiding quantum information
- Random encoding of information
- Benchmarking
- **Checking entanglement**
- Generation of topological order
- Demonstrating quantum supremacy
  - Boson sampling / IQP
- ...

$$U \otimes U^{+} \left|\phi^{-}\right\rangle \stackrel{?}{=} \left|\phi^{-}\right\rangle$$

Singlet the only state invariant under $U \otimes U^{+}$

# Random unitaries and t-designs

Sounds awesome!

So what's the problem?

- Sampling from the Haar measure (truly random) is difficult!
  - Exp. gates and random bits [Knill '95]

- Practicality of generating random circuits?
  - Must reconfigure circuit based on random variable

# Random unitaries and t-designs

Sounds awesome!

So what's the problem?

- Sampling from the Haar measure (truly random) is difficult!
    - Exp. gates and random bits [Knill '95]

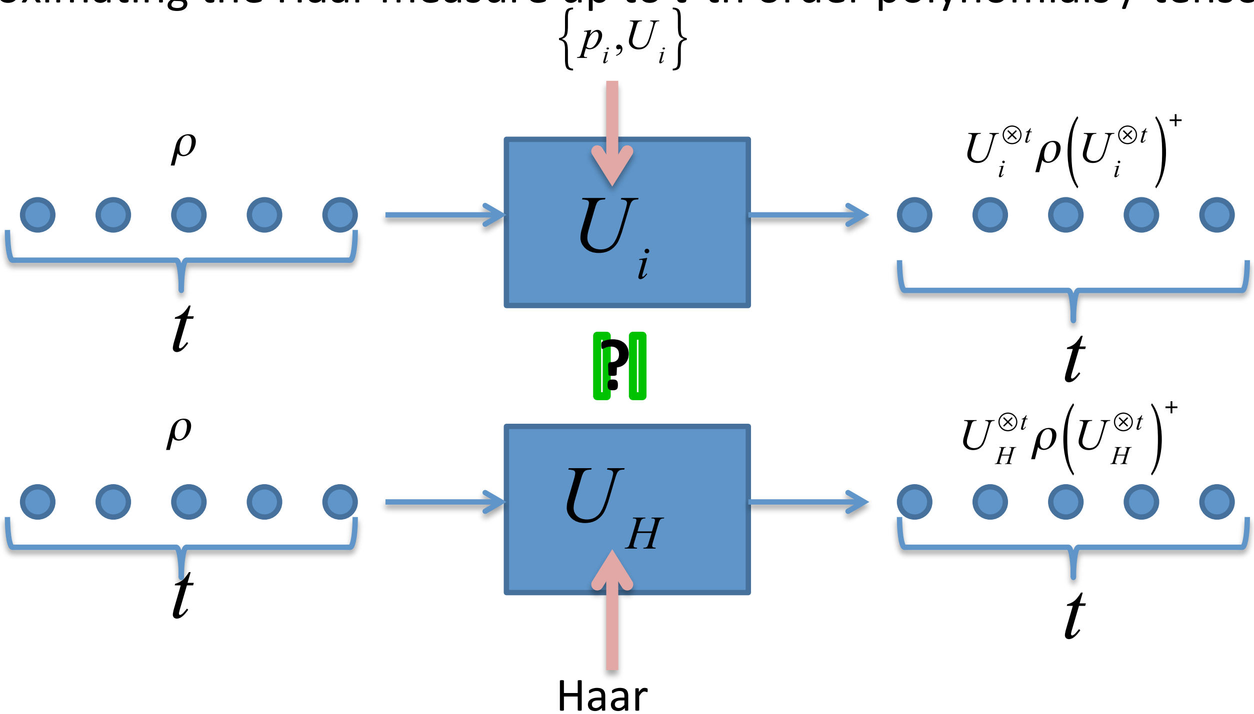
→ approx. with finite distribution
e.g. t-design $\{p_i, U_i\}_{i=1\ldots K}$

- Practicality of generating random circuits?
    - Must reconfigure circuit based on random variable

→ **Our approach**
Use measurement only to generate randomness
(see also [Plato, Plenio, Dahlsten '08])
-> fixed state followed by fixed measurements

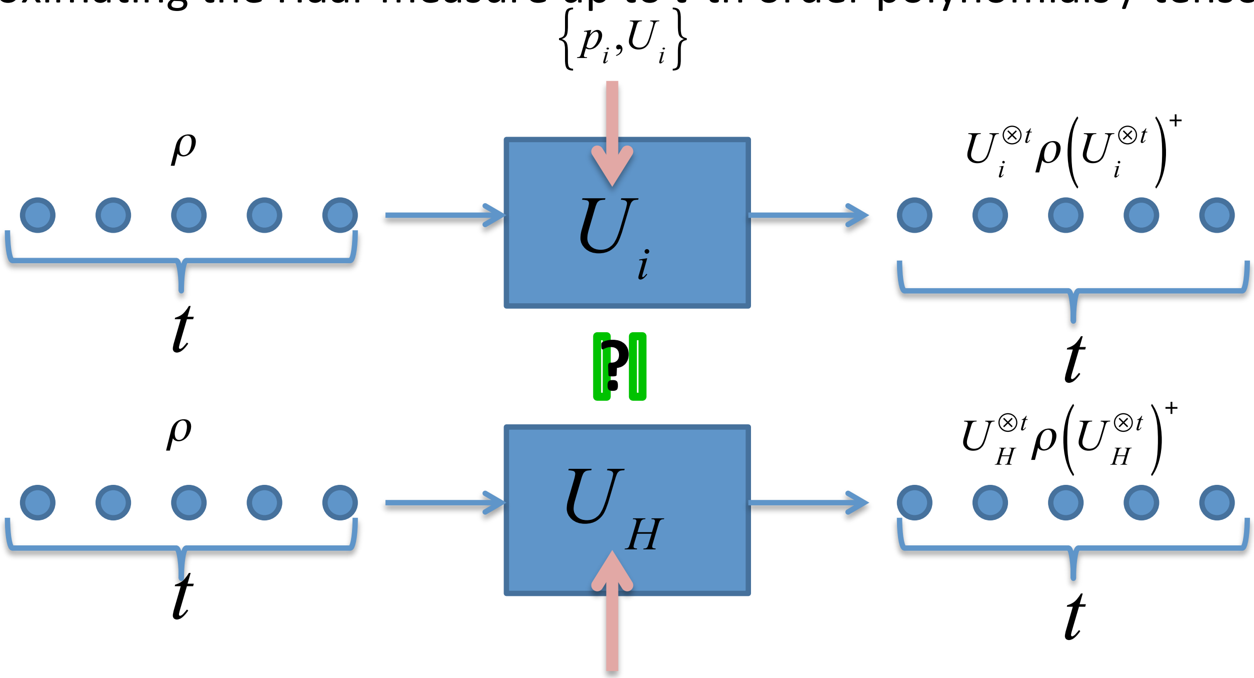
# Unitary t-designs

Approximating the Haar measure up to *t*-th order polynomials / tensor products



# Unitary t-designs

Approximating the Haar measure up to *t*-th order polynomials / tensor products




- Interested in the expectation for t-fold tensor product of the Haar measure

$$\mathrm{E}_H^t(\rho) := \int_{Haar} U^{\otimes t}\rho\left(U^{\otimes t}\right)^+ dU$$

- $\{p_i, U_i\}$ is an $\varepsilon$*-approximate t-design* iff

$$(1-\varepsilon)\mathrm{E}_H^t(\rho) \leq \sum_i p_i U_i^{\otimes t}\rho\left(U_i^{\otimes t}\right)^+ \leq (1+\varepsilon)\mathrm{E}_H^t(\rho) \qquad \forall \quad \rho \in \mathrm{B}(\mathrm{H}^{\otimes t})$$

# Unitary t-designs

Approximating the Haar measure up to *t*-th order polynomials / tensor products

- Interested in the expectation for t-fold tensor product of the Haar measure

$$\mathrm{E}_H^t\left(\rho\right) := \int_{Haar} U^{\otimes t} \rho \left(U^{\otimes t}\right)^{+} dU$$

- $\left\{p_i, U_i\right\}$ is an $\varepsilon$ *-approximate t-design* iff

$$(1-\varepsilon)\mathrm{E}_H^t\left(\rho\right) \leq \sum_i p_i U_i^{\otimes t} \rho \left(U_i^{\otimes t}\right)^{+} \leq (1+\varepsilon)\mathrm{E}_H^t\left(\rho\right) \qquad \forall \quad \rho \in \mathrm{B}(\mathrm{H}^{\otimes t})$$

- $t=1$ Pauli operators — operator basis
  $t=2$ Clifford group — benchmarking — [Dankert et al '09]
  $t=3$ Clifford group — [Koeng et al /Zhu / Web 15]
  $t=4$ — thermalisation — [Muller et al '15]

# Unitary t-designs

Approximating the Haar measure up to *t*-th order polynomials / tensor products

- Interested in the expectation for t-fold tensor product of the Haar measure

$$\mathrm{E}_H^t\left(\rho\right) := \int_{Haar} U^{\otimes t}\rho\left(U^{\otimes t}\right)^{+} dU$$

- $\left\{p_i, U_i\right\}$ is an $\varepsilon$ *-approximate t-design* iff

$$(1-\varepsilon)\mathrm{E}_H^t\left(\rho\right) \leq \sum_i p_i U_i^{\otimes t}\rho\left(U_i^{\otimes t}\right)^{+} \leq (1+\varepsilon)\mathrm{E}_H^t\left(\rho\right) \qquad \forall \quad \rho \in \mathrm{B}(\mathrm{H}^{\otimes t})$$

- $t=1$ Pauli operators — operator basis
  $t=2$ Clifford group — benchmarking — [Dankert et al '09]
  $t=3$ Clifford group — [Koeng et al /Zhu / Web 15]
  $t=4$ — thermalisation — [Muller et al '15]

- *Efficient* construction $\varepsilon$-approximate t-designs using random circuits — [Brandao, Horodecki, Harrow '12] (HBB)

# Measurement based ensembles

- Idea: sample $\{p_i, U_i\}_{i=1\ldots K}$ using measurement (*a la teleportation)*

  -> Measurement based q-computation without corrections does this!

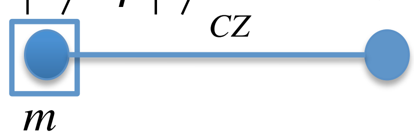
# Measurement based ensembles

- Idea: sample $\{p_i, U_i\}_{i=1\ldots K}$ using measurement (*a la teleportation)*

-> Measurement based q-computation without corrections does this!

<u>E,g.</u>

$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ $|+\rangle = 1/\sqrt{2}\left(|0\rangle + |1\rangle\right)$



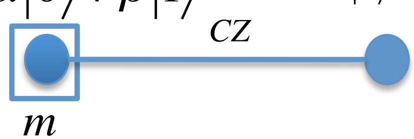
# Measurement based ensembles

- Idea: sample $\{p_i, U_i\}_{i=1\ldots K}$ using measurement (*a la teleportation)*

  -> Measurement based q-computation without corrections does this!

<u>E,g.</u>

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$$




$$CZ|\varphi\rangle|+\rangle = CZ(\alpha|0\rangle + \beta|1\rangle)|+\rangle$$

$$= |+^{\theta}\rangle HZ(\theta)|\varphi\rangle + |-^{\theta}\rangle HZ^{m}Z(\theta)|\varphi\rangle$$

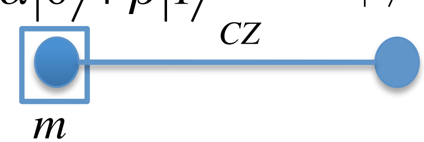
# Measurement based ensembles

- Idea: sample $\{p_i, U_i\}_{i=1\ldots K}$ using measurement (*a la teleportation)*

  -> Measurement based q-computation without corrections does this!

<u>E,g.</u>

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |+\rangle = 1/\sqrt{2}\left(|0\rangle + |1\rangle\right)$$




$$\begin{aligned} CZ|\varphi\rangle|+\rangle &= CZ\left(\alpha|0\rangle + \beta|1\rangle\right)|+\rangle \\ &= |+^{\theta}\rangle \boxed{HZ(\theta)|\varphi\rangle} + |-^{\theta}\rangle \boxed{HZ^m Z(\theta)|\varphi\rangle} \end{aligned}$$

-> measure in $|\pm^{\theta}\rangle = 1/\sqrt{2}\left(|0\rangle \pm e^{i\theta}|1\rangle\right)$ basis

$$\left\{p_m = 1/2, \quad U_m(\theta) = HZ^m Z(\theta)\right\}_{m=0,1}$$

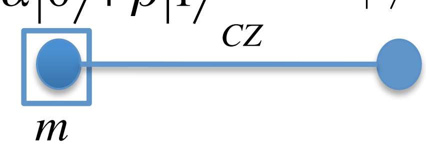
# Measurement based ensembles

- Idea: sample $\{p_i, U_i\}_{i=1\ldots K}$ using measurement (*a la teleportation)*

-> Measurement based q-computation without corrections does this!

<u>E,g.</u>

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |+\rangle = 1/\sqrt{2}\left(|0\rangle + |1\rangle\right)$$




$$CZ|\varphi\rangle|+\rangle = CZ\left(\alpha|0\rangle + \beta|1\rangle\right)|+\rangle$$

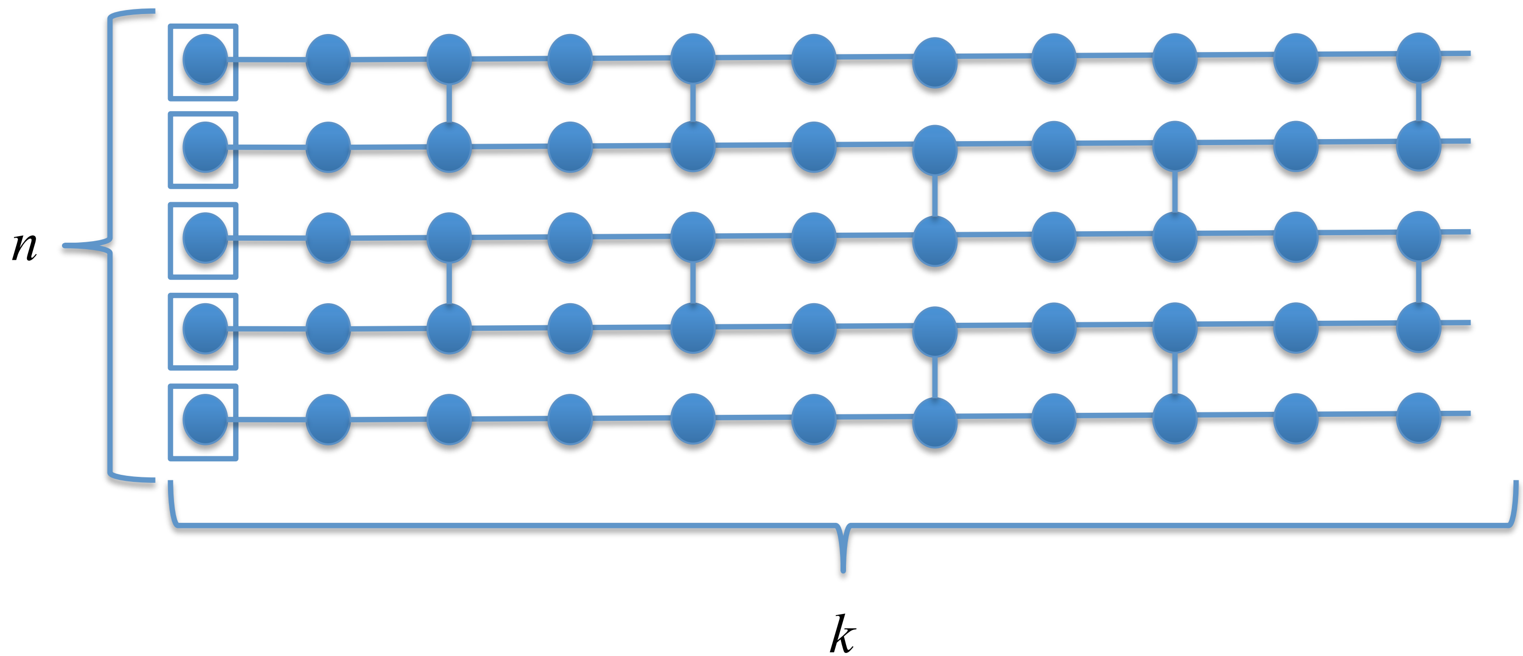
$$= \left|+^{\theta}\right\rangle HZ(\theta)|\varphi\rangle + \left|-^{\theta}\right\rangle HZ^{m}Z(\theta)|\varphi\rangle$$

-> measure in $\left|\pm^{\theta}\right\rangle = 1/\sqrt{2}\left(|0\rangle \pm e^{i\theta}|1\rangle\right)$ basis

$$\left\{p_m = 1/2, \quad U_m(\theta) = HZ^{m}Z(\theta)\right\}_{m=0,1}$$

- Use to build BHH efficient approximate t-designs
- Instances of hard problems

# Graph state for t-design and hard sampling



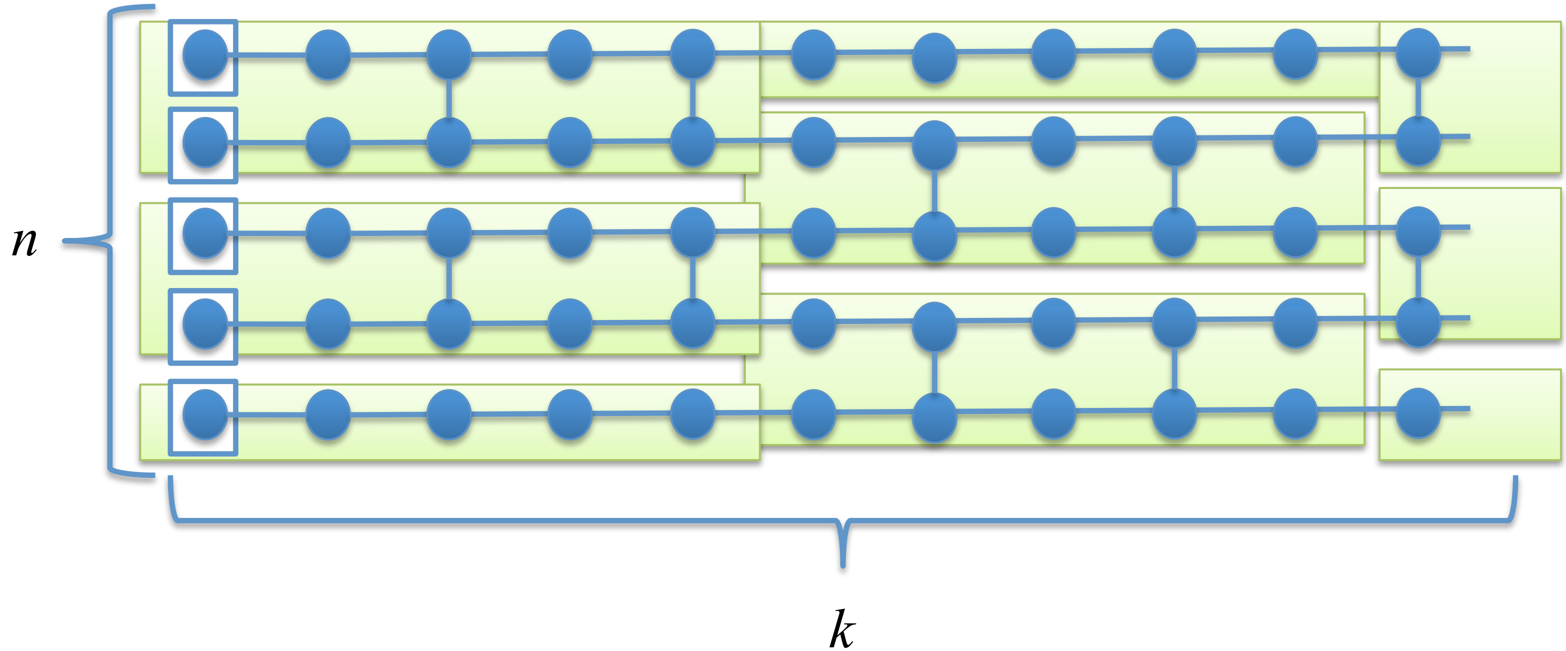

- $\varepsilon$-approximate t-design $k = \mathrm{poly}\left(n, t, \log\left(\frac{1}{\varepsilon}\right)\right)$

- Hard sampling output $x$ of all $m = nk$ qubits

*$D(x)$ cannot be sampled efficiently in time $poly(m)$ up to error $1/22$ in $l_1$ norm*

[R. Mezher, J. Ghalbouni, J. Dgheim, DM PRA 97, 0233 (2018), + in preperation]

# Graph state for t-design and hard sampling



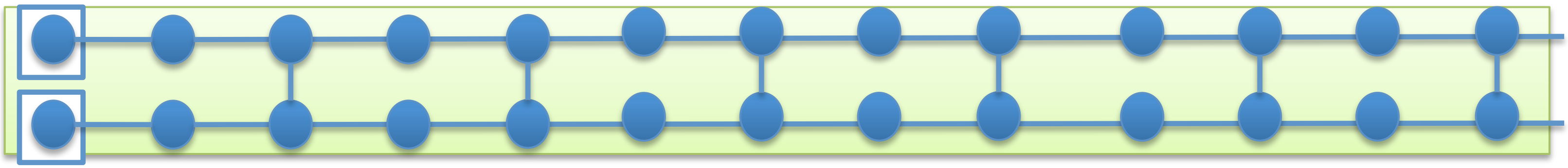

- $\varepsilon$-approximate t-design $k = \mathrm{poly}\left(n, t, \log\left(\frac{1}{\varepsilon}\right)\right)$

- Hard sampling output $x$ of all $m = nk$ qubits

$D(x)$ *cannot be sampled efficiently in time* $poly(m)$ *up to error* $1/22$ *in* $l_1$ *norm*

[R. Mezher, J. Ghalbouni, J. Dgheim, DM PRA 97, 0233 (2018), + in preperation]

# Graph gadget

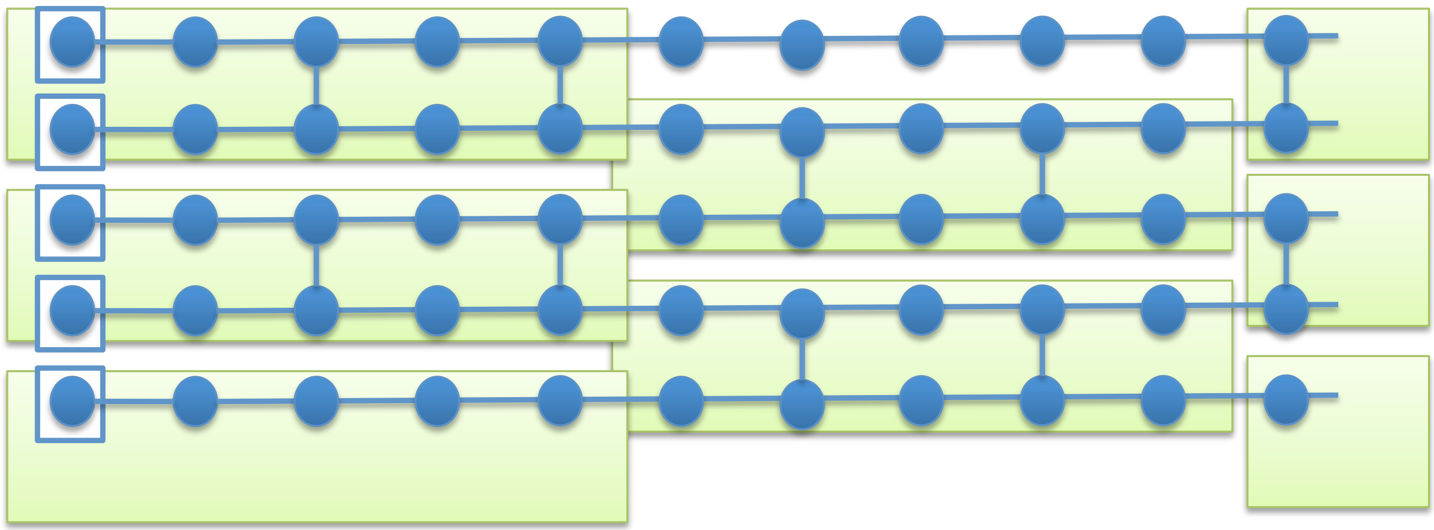


For fixed measurement angles

- Uniformly samples from $\{U_i\}$
- $\{U_i\}$ is universal on $SU(4)$
- $\{U_i\}$ contains elements and their inverses

[R. Mezher, J. Ghalbouni, J. Dgheim, DM PRA 97, 0233 (2018), + in preperation]

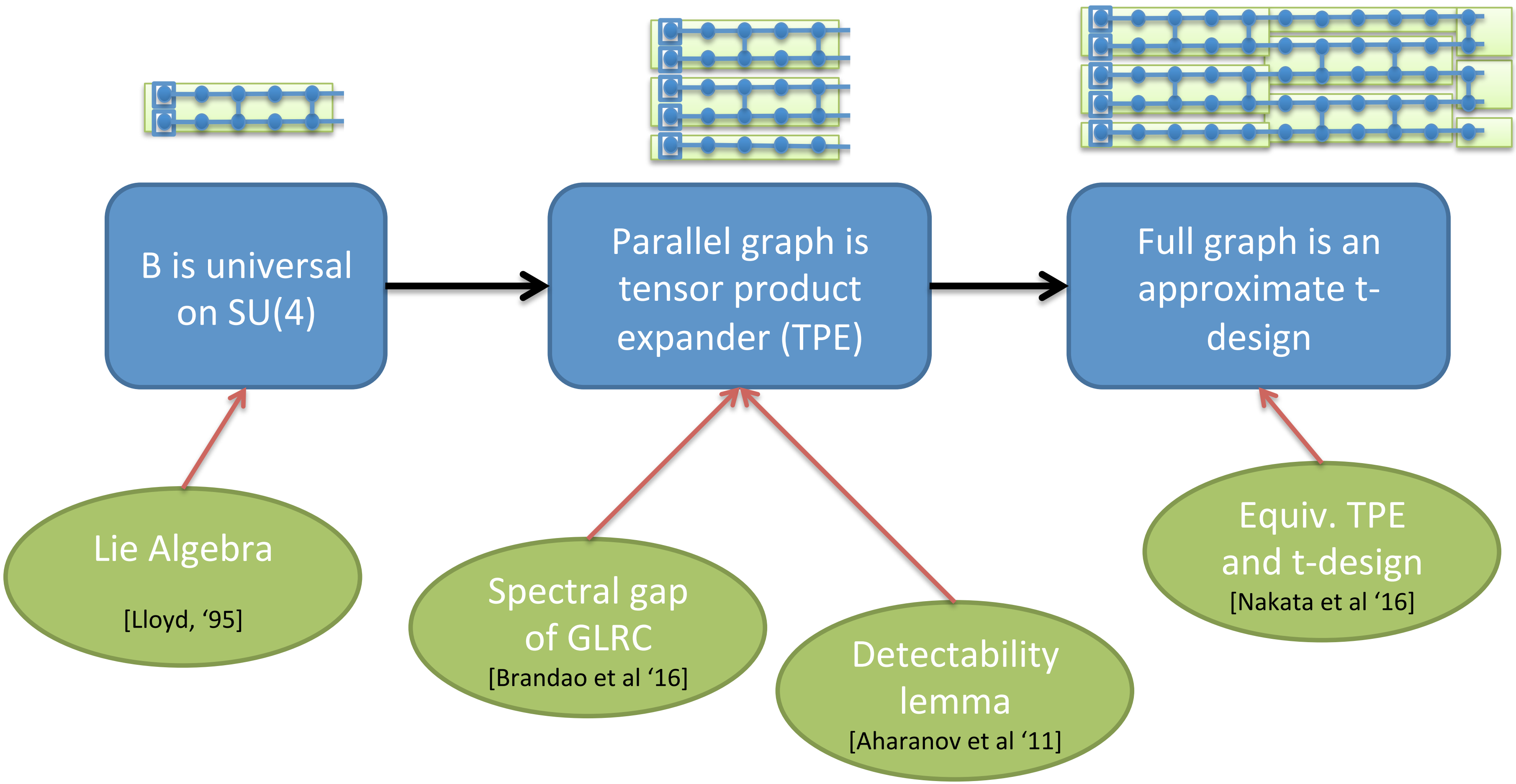
# t-designs on regular lattices, proof sketch…



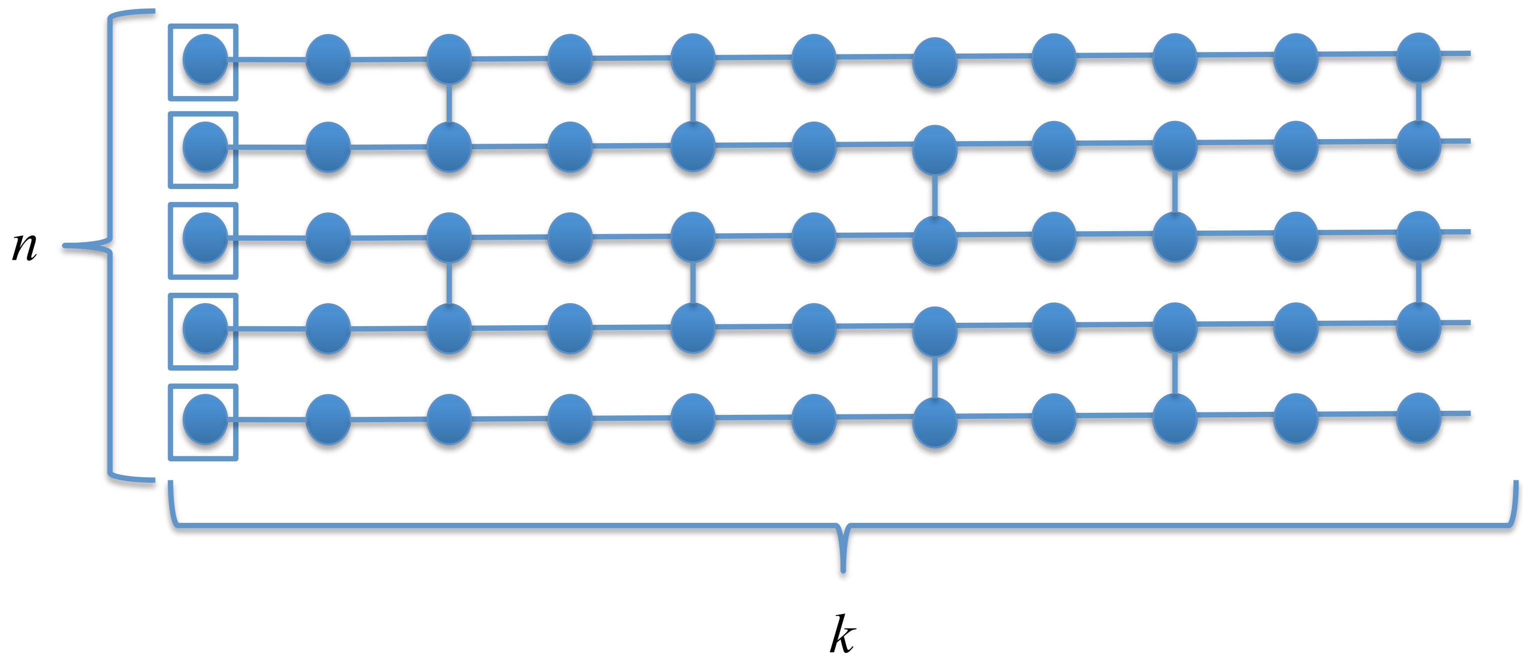
Then proof follows similar to [Bradao, Harrow, Horodecki ’12]

- restatement as Hamiltonian gap problem
- detectability lemma [Aharanov, Arad, Vazirani, Landau, ‘11]

# t-designs on regular lattices, proof sketch…



# Hardness of sampling



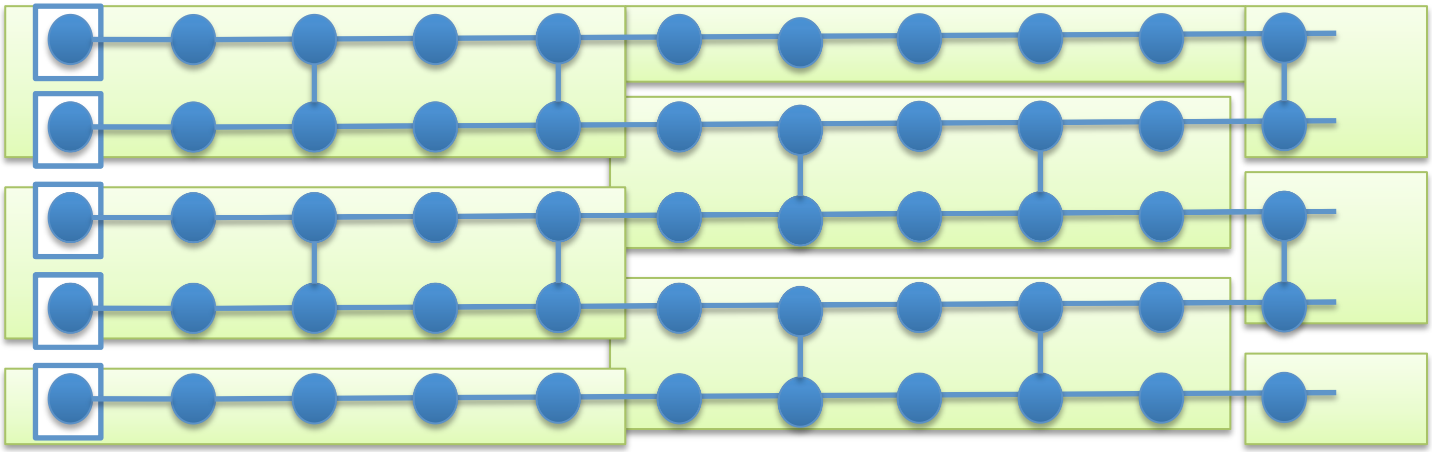

See
[Hangleiter, Bermejo-Vega, M. Schwarz, J. Eisert '18]
[Bermejo-Vega, Hangleiter, Schwarz, Raussendorf, Eisert '18]

- Assuming

  Conjecture 1: Polyomial hierarchy does not collapse to the third level
  Conjecture 2: Associated worst case ♯P hard prob, is average case hard

A classical computer cannot sample from the output distribution up to $l_1$ -norm error $\frac{1}{22}$ in time $O\left(\mathrm{poly}(nk)\right)$

# Hardness of sampling, proof sketch...

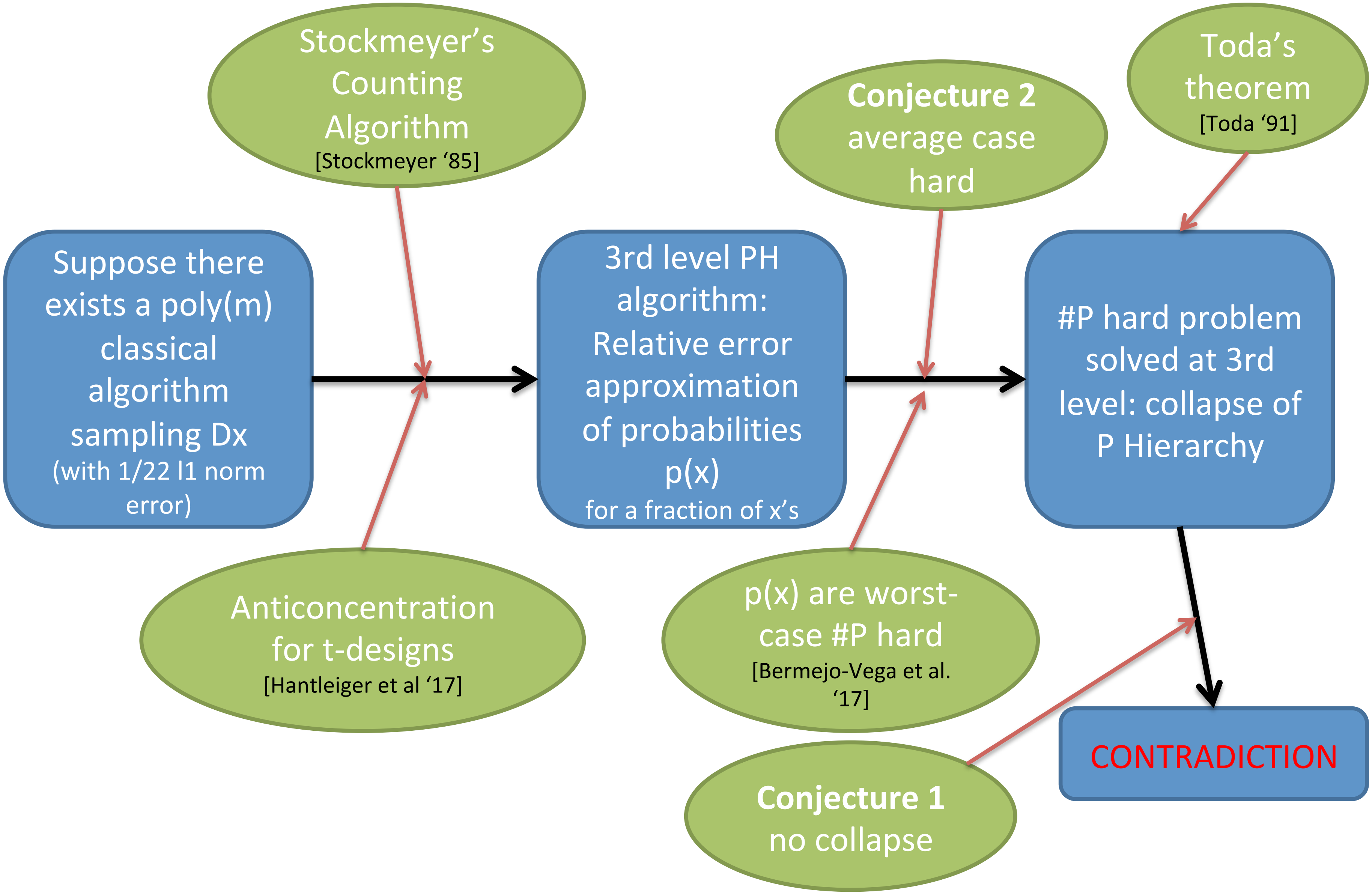


- Contains universal gate set -> ♯P hard in worst case
  [Van den Nest '08], [Aaronson, Chen '16]

- 2-designs anticoncentrate
  [Hangleiter, Bermejo-Vega, M. Schwarz, J. Eisert '18]

- Standard proofs for sampling hardness via Stockmeyer
  (e.g. [Bermejo-Vega, Hangleiter, Schwarz, Raussendorf, Eisert '18])

# Hardness of sampling, proof sketch…



# Connection to Jones Polynomials

- Standard map

Circuits $\longleftrightarrow$ Jones Polynomials

[Kitaev '05] [Wocjan, Yard '06] [Aharonov, Arad '06]

- Approximating our circuits approximates associated Jones Polynomials

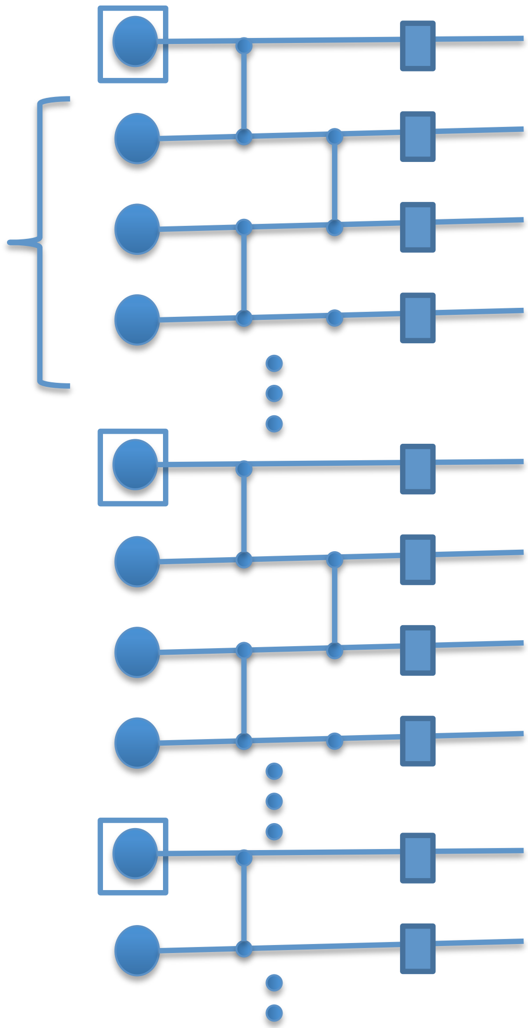
(see also [Fujii, Morimae '13])

*Approximating, up to relative error,*
*the Jones polynomial over the plat closure of*
*braids formed of a length* $l \geq O(n^{3.97})$ *of compositions*
*of generators of the braid group of* $4n$
*strands (and their inverses) is #P -hard.*

- Alternative form of conjecture

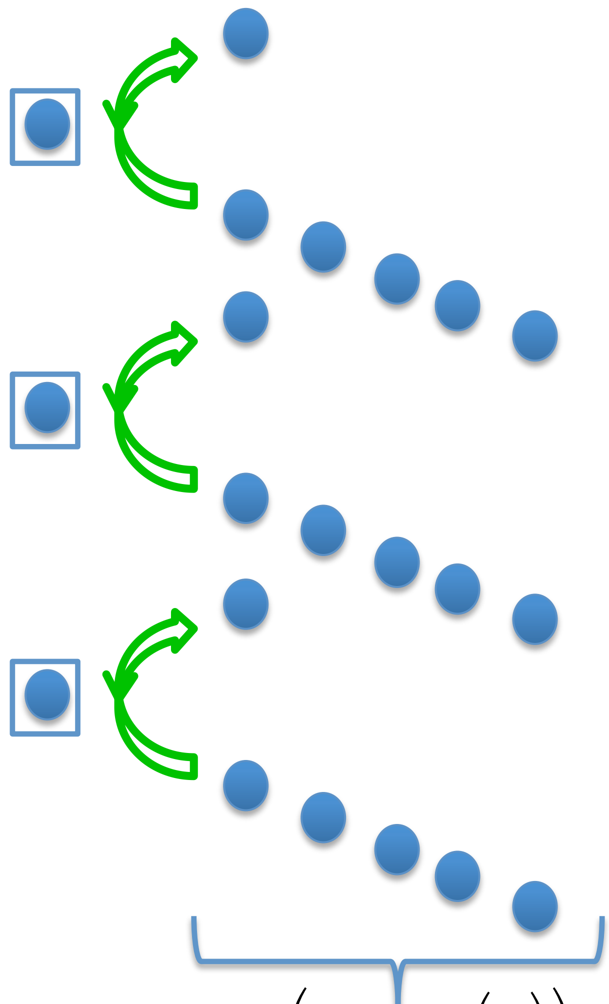
# Circuit picture

$$\mathrm{poly}\left(n, t, \log\left(\frac{1}{\varepsilon}\right)\right)$$



- Constant depth t-designs and quantum speedup

# Scattering…



$$\text{poly}\left(n, t, \log\left(\frac{1}{\varepsilon}\right)\right)$$

- 4-designs efficiently thermalise [Muller et al '15]

# Conclusions and perspectives

- Fixed measurement hardness and approximate t-design
- Constant depth circuits
- Simplest examples well implementable now
- Many techniques for verified versions (verified sampling, t-design generation)

<u>Applications</u>
- Demonstration of certified quantum computational advantage
- Scattering / thermalisation / scrambling
- Benchmarking [R. Alexander, P. Turner, S. Bartlett PRA 2016]
- Cryptography?

…

# Thank you!

PRA 97, 0233 (2018), in preperation