

Information flow in MBQC and Adiabatic quantum computation

Damian Markham

Joint work with

Bobby Antonio and Janet Anders [arxiv:1309.1443](#)

and

Elham Kashefi [arxiv:1311.3610](#)

CNRS, LTCI– ENST (Telecom ParisTech), Paris



① Background

- MBQC
- gFlow (causal order and corrections)

② Information light cone

- Causal cone from gFlow is also an information light cone!

③ Classical simulatability and universality

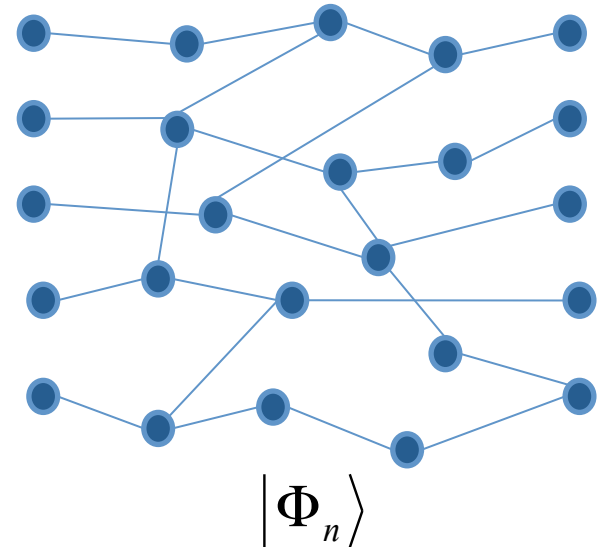
- Size of light cone bounds simulatability
- Points to tradeoff:
 'spread' of information Vs 'use' of spread

④ gFlow for translating MBAC to Adiabatic QC

- gFlow provides translation, hence ideas and intuitions follow

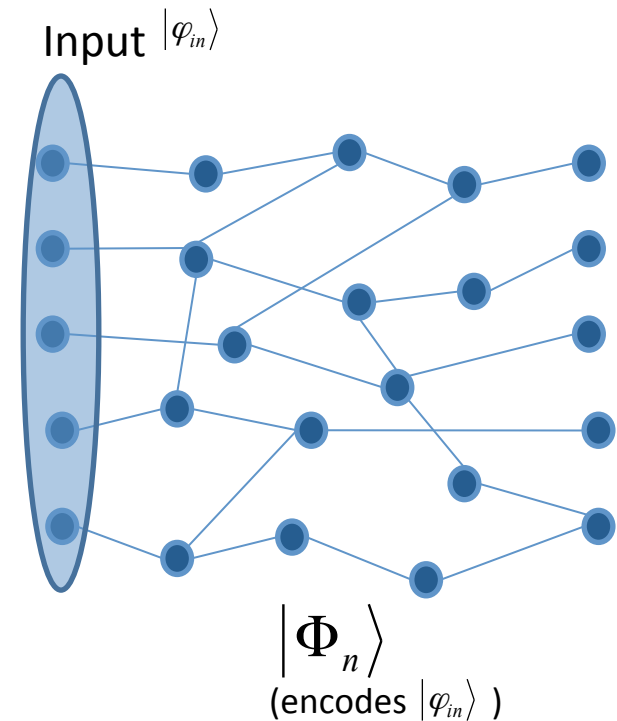
Measurement Based Quantum Computation (MBQC)

- Initial entangled resource state $|\Phi_n\rangle$
- Single qubit measurements
- Local corrections



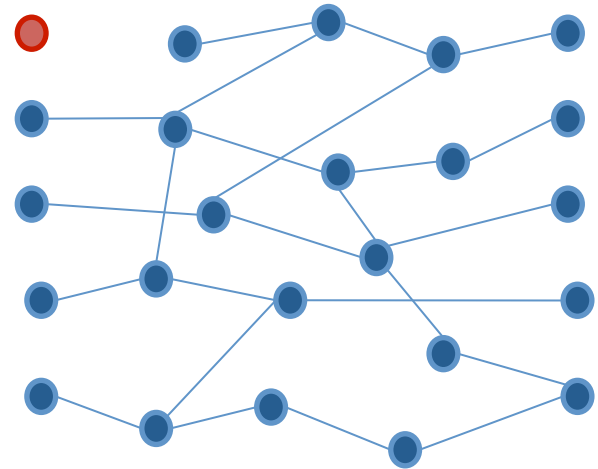
Measurement Based Quantum Computation (MBQC)

- Initial entangled resource state $|\Phi_n\rangle$
- Single qubit measurements
- Local corrections



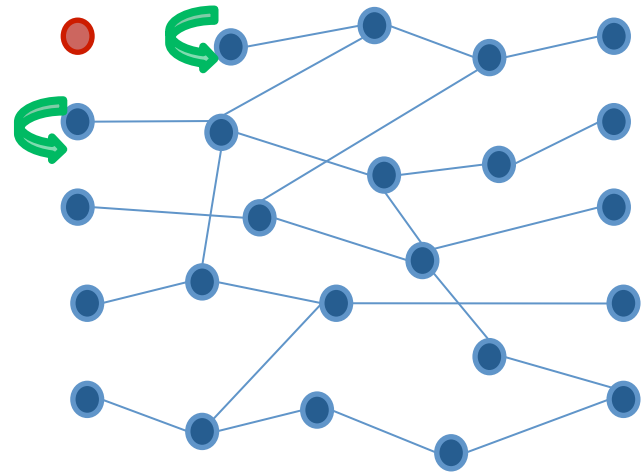
Measurement Based Quantum Computation (MBQC)

- Initial entangled resource state $|\Phi_n\rangle$
- Single qubit measurements
- Local corrections



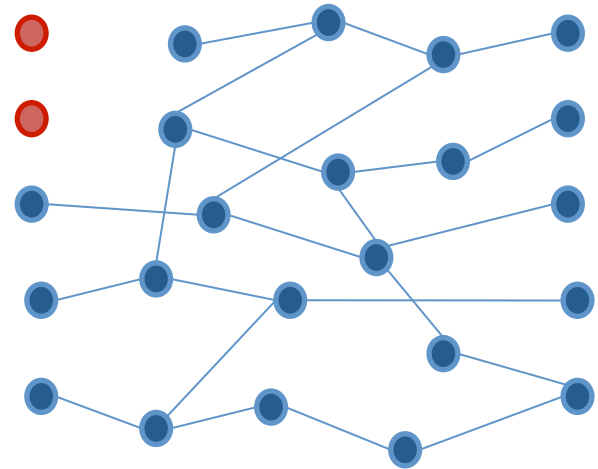
Measurement Based Quantum Computation (MBQC)

- Initial entangled resource state $|\Phi_n\rangle$
- Single qubit measurements
- Local corrections



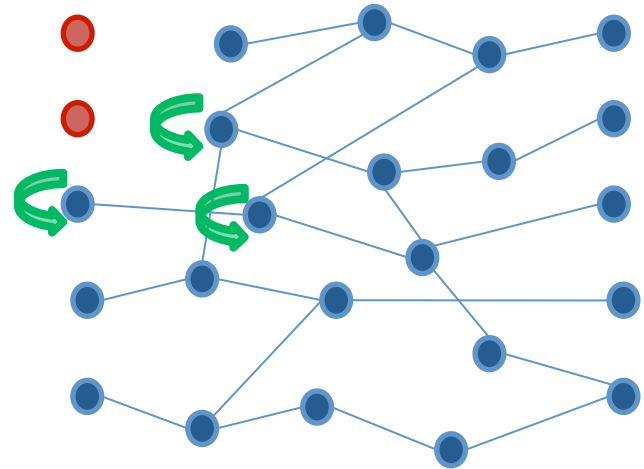
Measurement Based Quantum Computation (MBQC)

- Initial entangled resource state $|\Phi_n\rangle$
- Single qubit measurements
- Local corrections



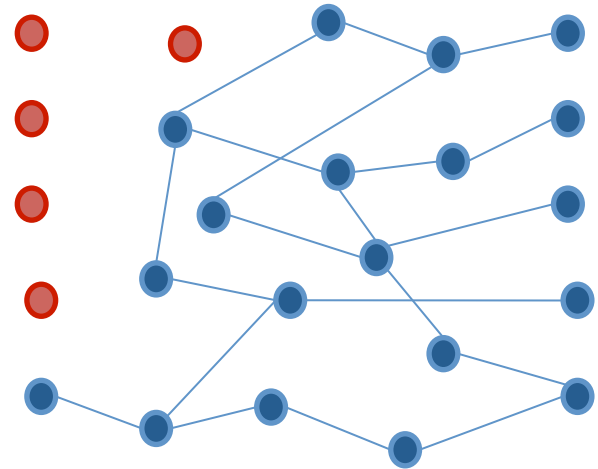
Measurement Based Quantum Computation (MBQC)

- Initial entangled resource state $|\Phi_n\rangle$
- Single qubit measurements
- Local corrections



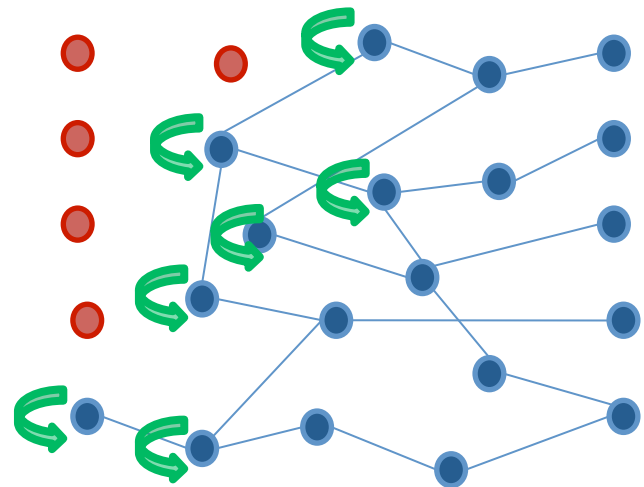
Measurement Based Quantum Computation (MBQC)

- Initial entangled resource state $|\Phi_n\rangle$
- Single qubit measurements
- Local corrections



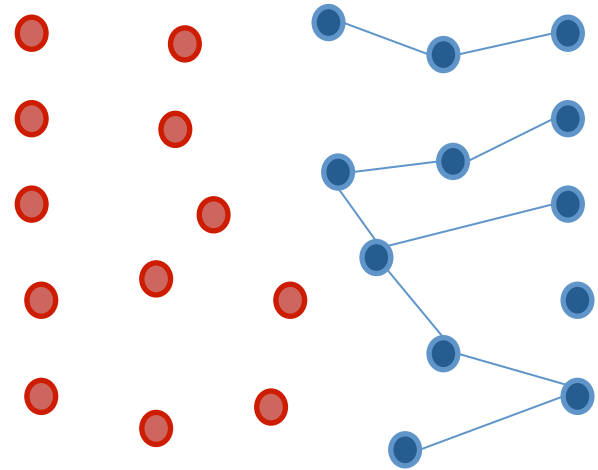
Measurement Based Quantum Computation (MBQC)

- Initial entangled resource state $|\Phi_n\rangle$
- Single qubit measurements
- Local corrections



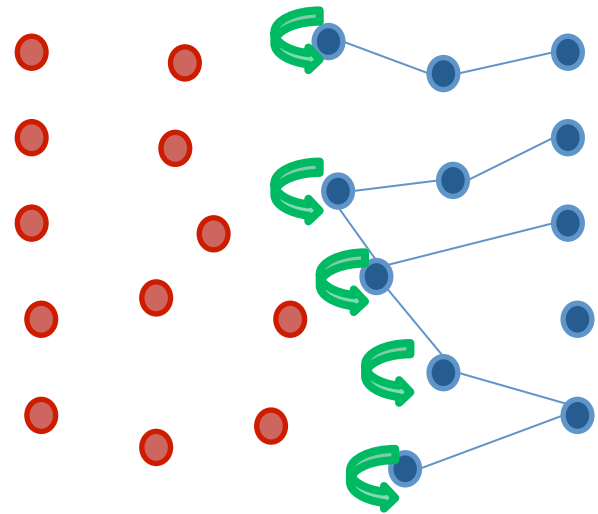
Measurement Based Quantum Computation (MBQC)

- Initial entangled resource state $|\Phi_n\rangle$
- Single qubit measurements
- Local corrections



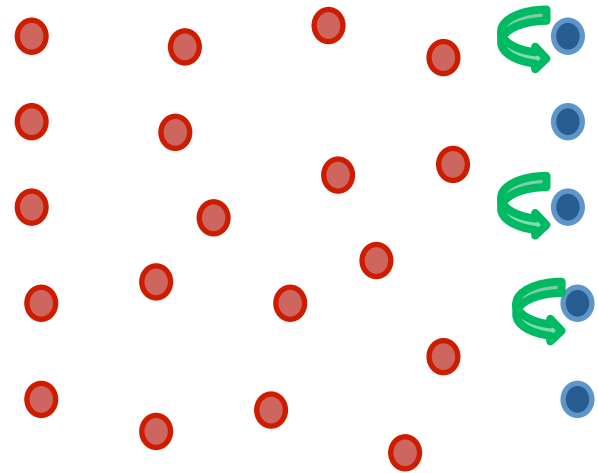
Measurement Based Quantum Computation (MBQC)

- Initial entangled resource state $|\Phi_n\rangle$
- Single qubit measurements
- Local corrections



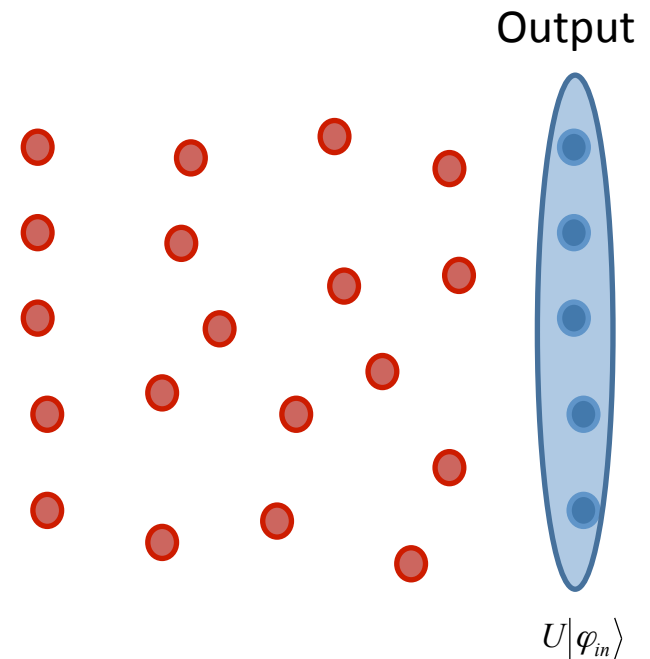
Measurement Based Quantum Computation (MBQC)

- Initial entangled resource state $|\Phi_n\rangle$
- Single qubit measurements
- Local corrections



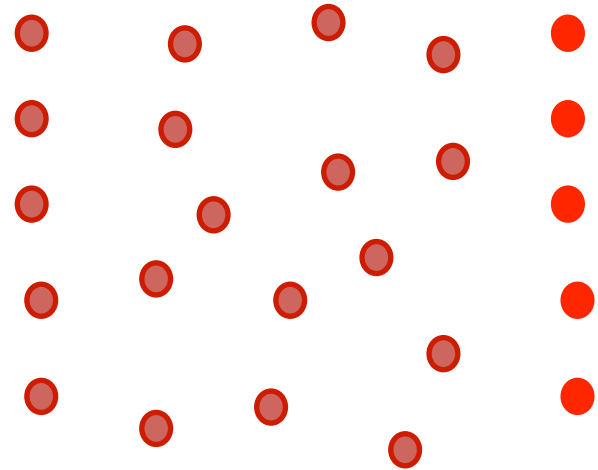
Measurement Based Quantum Computation (MBQC)

- Initial entangled resource state $|\Phi_n\rangle$
- Single qubit measurements
- Local corrections



Measurement Based Quantum Computation (MBQC)

- Initial entangled resource state $|\Phi_n\rangle$
- Single qubit measurements
- Local corrections



Measurement Based Quantum Computation (MBQC)

- What are the correction operations, and why do we need them?

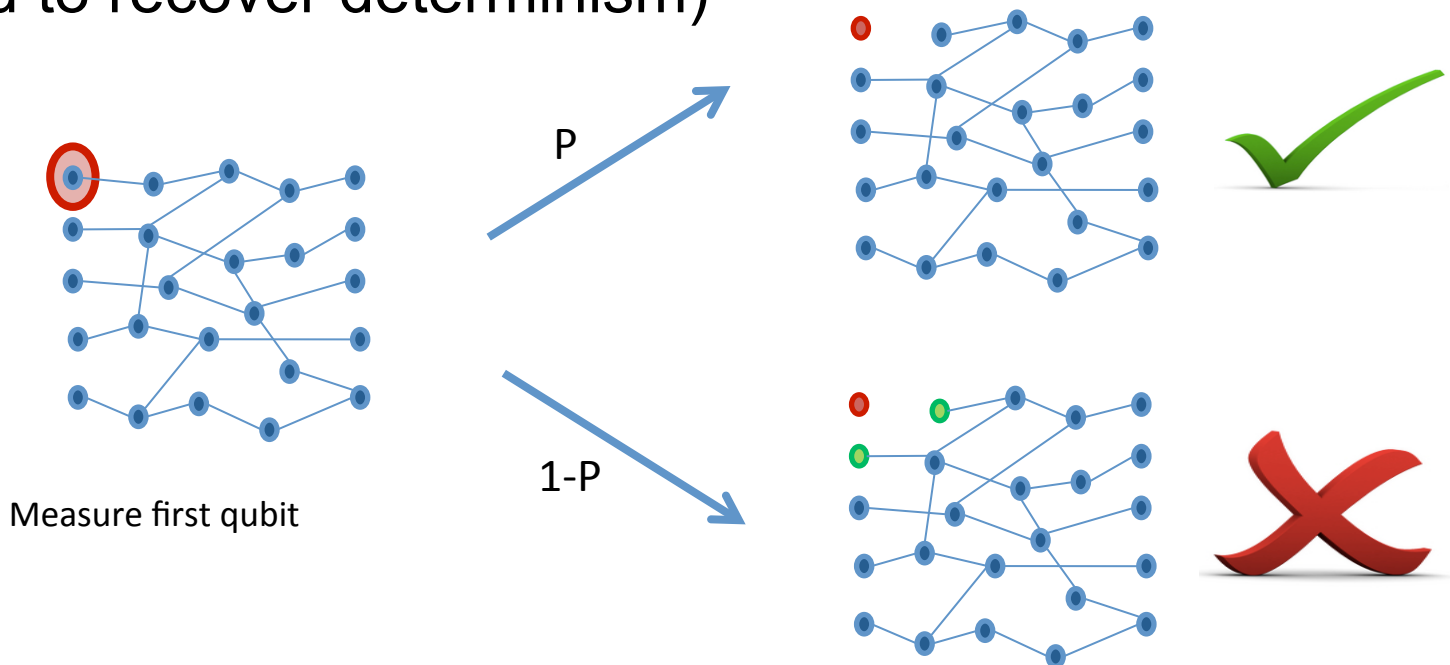
Measurement Based Quantum Computation (MBQC)

- What are the correction operations, and **why do we need them?**
- ➡ Measurement is random
(need to recover determinism)

Measurement Based Quantum Computation (MBQC)

- What are the correction operations, and **why do we need them?**

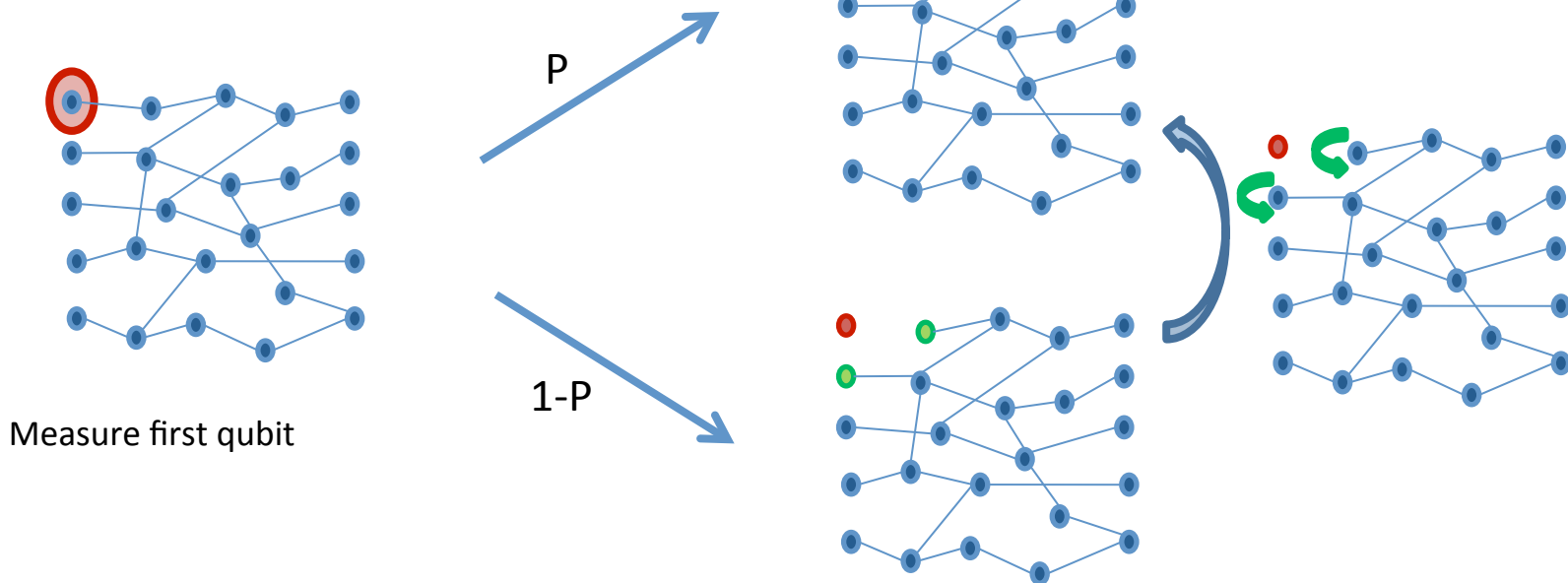
➡ Measurement is random
(need to recover determinism)



Measurement Based Quantum Computation (MBQC)

- What are the correction operations, and **why do we need them?**

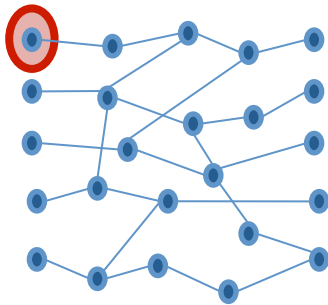
➡ Measurement is random
(need to recover determinism)



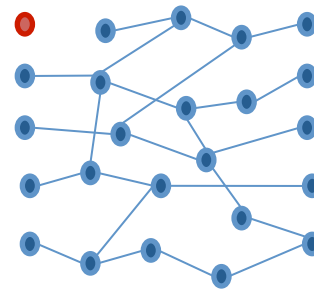
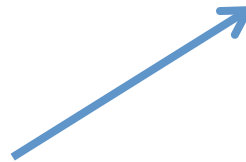
Measurement Based Quantum Computation (MBQC)

- What are the correction operations, and **why do we need them?**

➡ Measurement is random
(need to recover determinism)



Measure first qubit



Measurement Based Quantum Computation (MBQC)

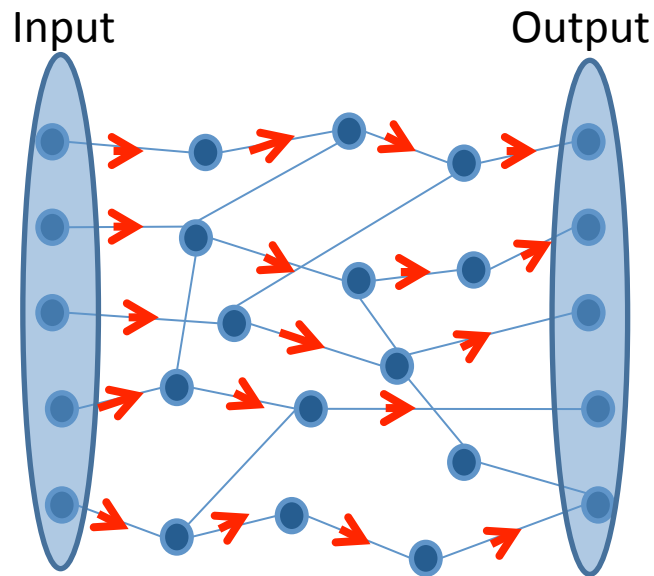
- **What are the correction operations, and why do we need them?**

gFlow tells us when it can be done, and which operations to make

- ➡ Imposes a CAUSAL ORDER (measurement sequence)
- ➡ Describes information spread
- ➡ Consequences for simulatability / universality
- ➡ Translation to other models of computation (AQC)

gFlow

- Condition for a graph state to allow deterministic computation (tells you if corrections exist and what they are)



gFlow:

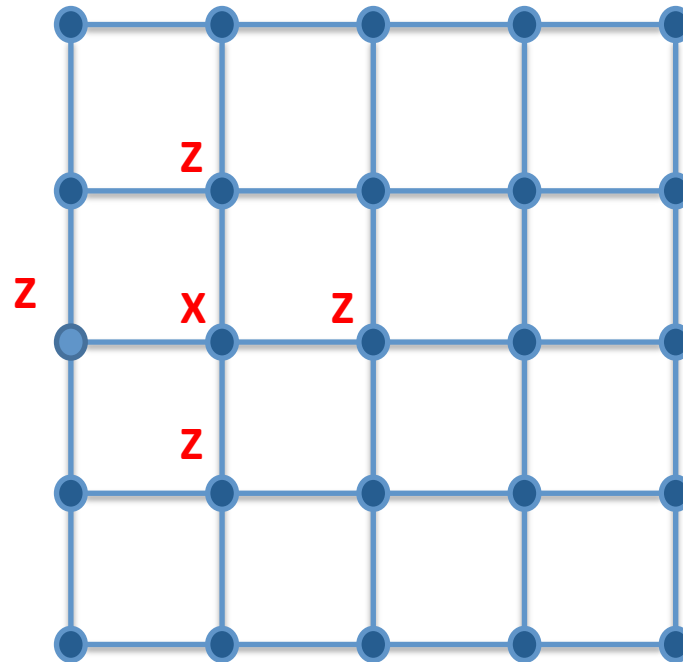
- 'correcting sets': who corrects for what measurements
- time order (so corrections can be consistent)

gFlow as acronychal corrections

- Tools: Graph states and stabilisers

$$K_i := X_i \otimes \prod_{(i,j) \in Ed} Z_j$$

$$K_i |G\rangle = |G\rangle$$



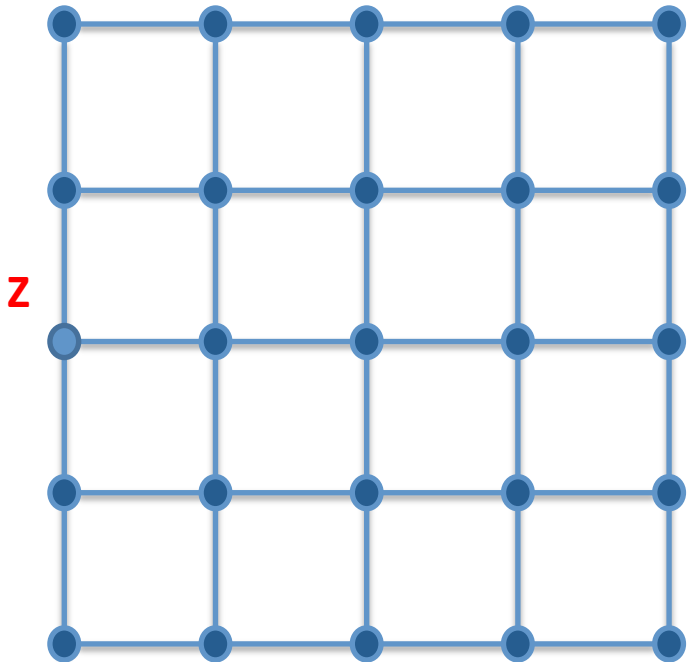
gFlow as acronychal corrections

- Tools: Graph states and stabilisers

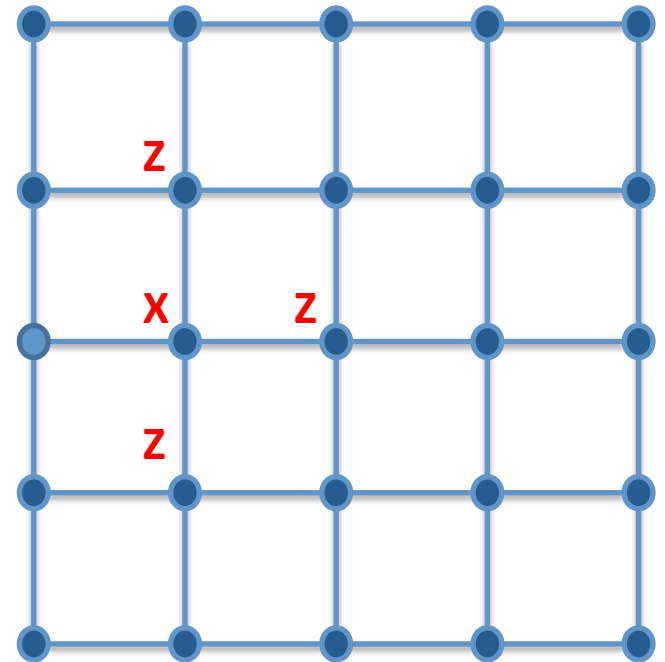
$$K_i := X_i \otimes \prod_{(i,j) \in Ed} Z_j$$

$$K_i |G\rangle = |G\rangle$$

$$Z_j |G\rangle = X_{i \in N(j)} \otimes \prod_{\substack{k \in N(i) \\ k \neq j}} Z_k |G\rangle$$



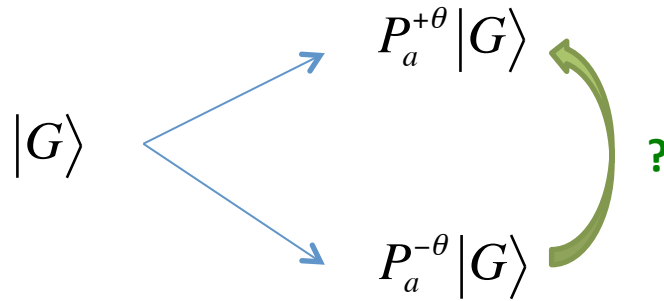
=



gFlow as acronychal corrections

- Measure qubit a

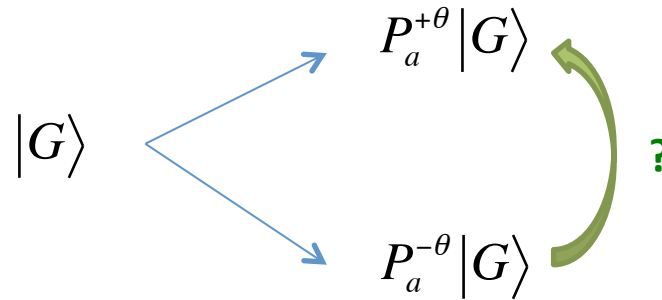
$$M_a^\theta = P_a^{+\theta} - P_a^{-\theta} \quad P_a^{\pm\theta} := |\pm\theta\rangle\langle\pm\theta| \quad |\pm\theta\rangle = \frac{|0\rangle \pm e^{-i\theta}|1\rangle}{\sqrt{2}}$$



gFlow as acronychal corrections

- Measure qubit a

$$M_a^\theta = P_a^{+\theta} - P_a^{-\theta} \quad P_a^{\pm\theta} := |\pm\theta\rangle\langle\pm\theta| \quad |\pm\theta\rangle = \frac{|0\rangle \pm e^{-i\theta}|1\rangle}{\sqrt{2}}$$

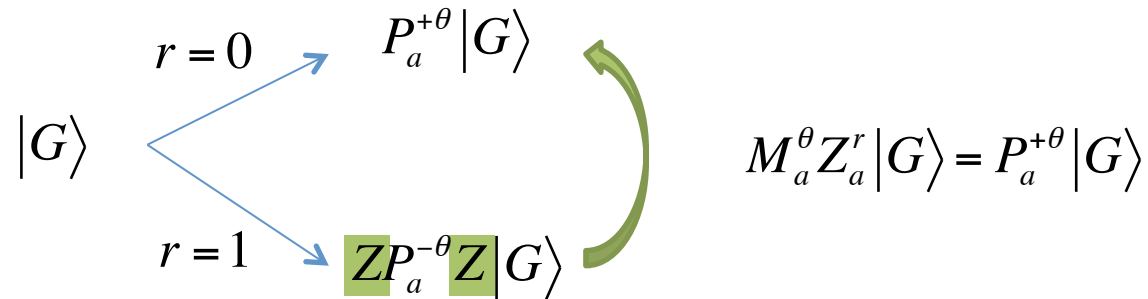


- use $ZP_a^{-\theta}Z = P_a^{+\theta}$

gFlow as acronychal corrections

- Measure qubit a

$$M_a^\theta = P_a^{+\theta} - P_a^{-\theta} \quad P_a^{\pm\theta} := |\pm\theta\rangle\langle\pm\theta| \quad |\pm\theta\rangle = \frac{|0\rangle \pm e^{-i\theta}|1\rangle}{\sqrt{2}}$$

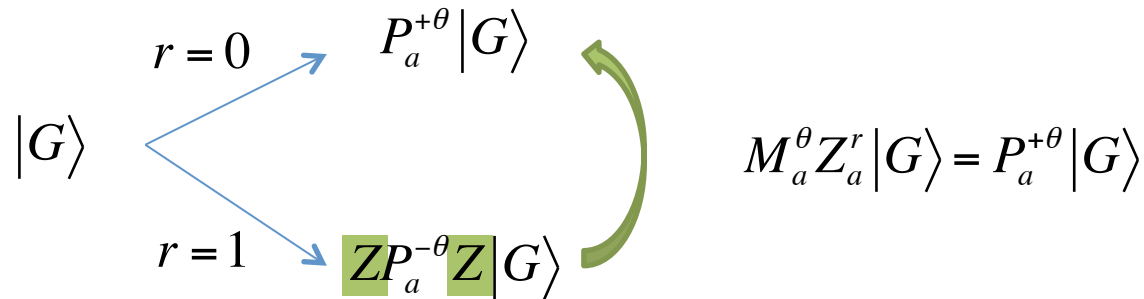


- use $ZP_a^{-\theta}Z = P_a^{+\theta}$

gFlow as acronychal corrections

- Measure qubit a

$$M_a^\theta = P_a^{+\theta} - P_a^{-\theta} \quad P_a^{\pm\theta} := |\pm\theta\rangle\langle\pm\theta| \quad |\pm\theta\rangle = \frac{|0\rangle \pm e^{-i\theta}|1\rangle}{\sqrt{2}}$$

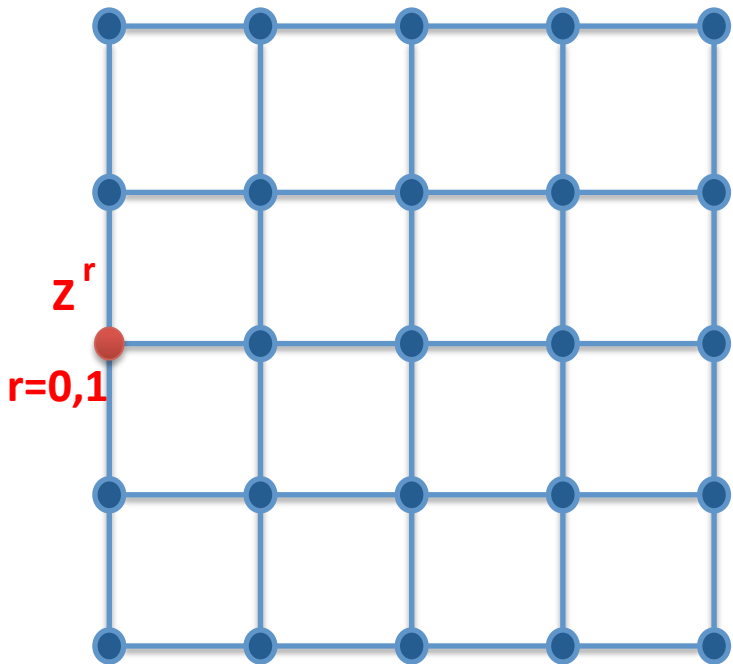


- Problem: have to know r before we do the measurement!
(acronychal)
- Solution: Use the graph stabilisers to simulate...
Correct on different systems - commutes with measurement!

$$M_a Z_a^{r_a} |G\rangle = X_i^{r_a} \bigotimes_{\substack{j \in N(i) \\ j \neq a}} Z_j^{r_a} M_a |G\rangle$$

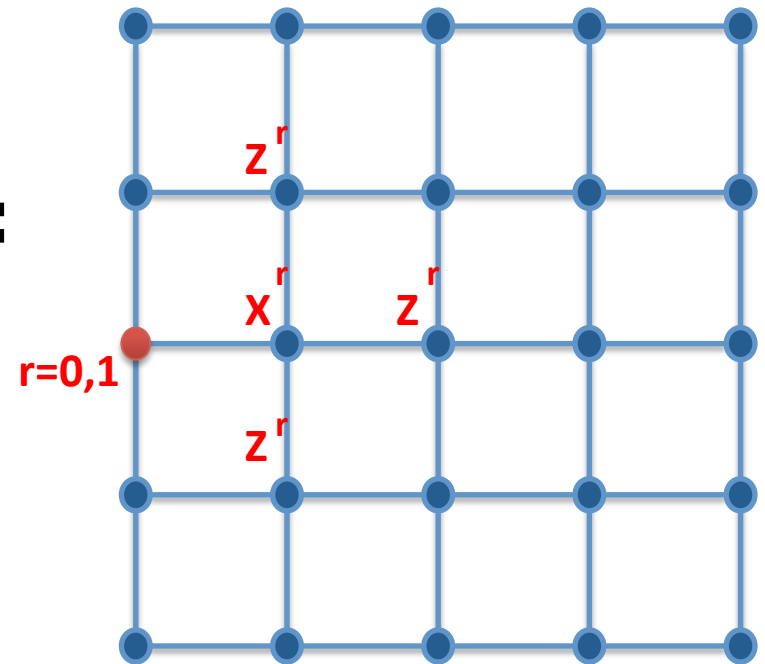
gFlow as acronychal corrections

$$M_a Z_a^{r_a} |G\rangle = X_i^{r_a} \bigotimes_{\substack{j \in N(i) \\ j \neq a}} Z_j^{r_a} M_a |G\rangle$$



- correction
- then measure (impossible)

=

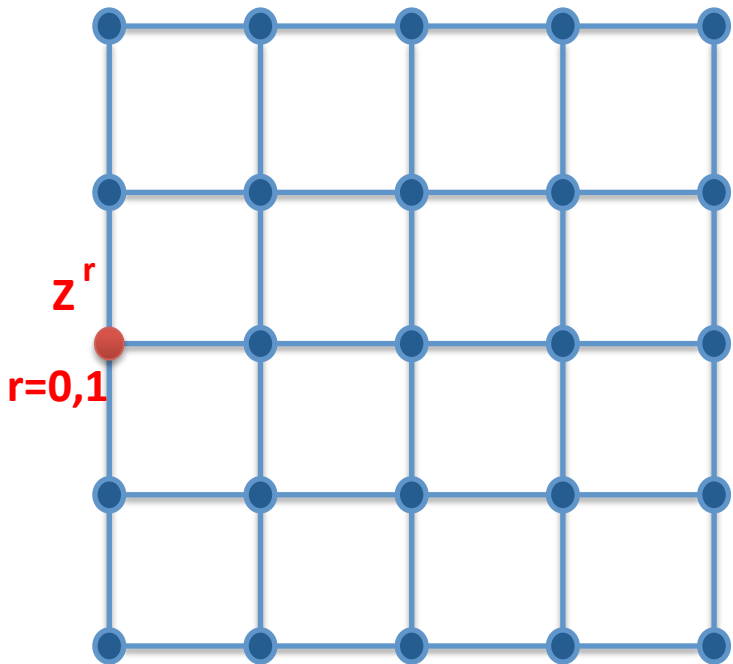


- measure
- then correct (great!)

- Can measure first, then correct
 - how to choose correction set?
 - consistent time order?

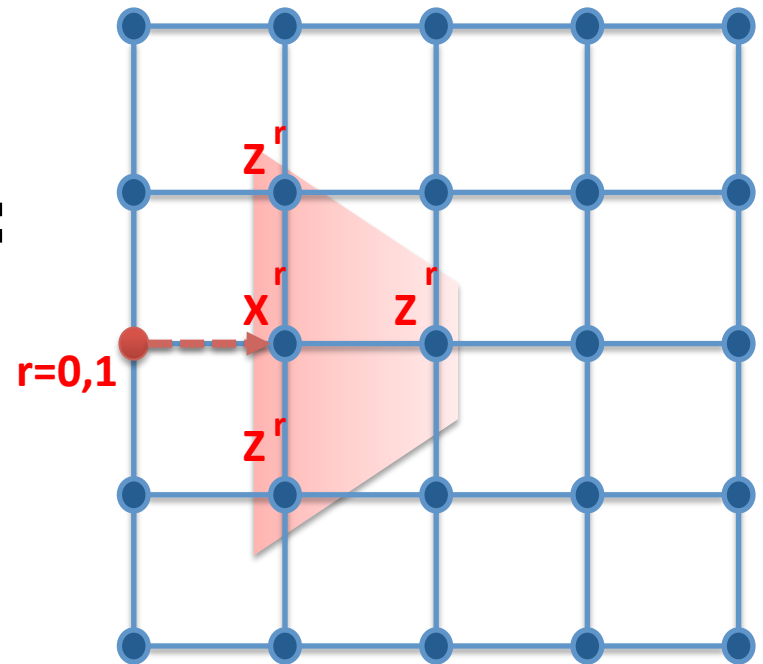
gFlow as acronychal corrections

$$M_a Z_a^{r_a} |G\rangle = X_i^{r_a} \bigotimes_{\substack{j \in N(i) \\ j \neq a}} Z_j^{r_a} M_a |G\rangle$$



- correction
- then measure (impossible)

=



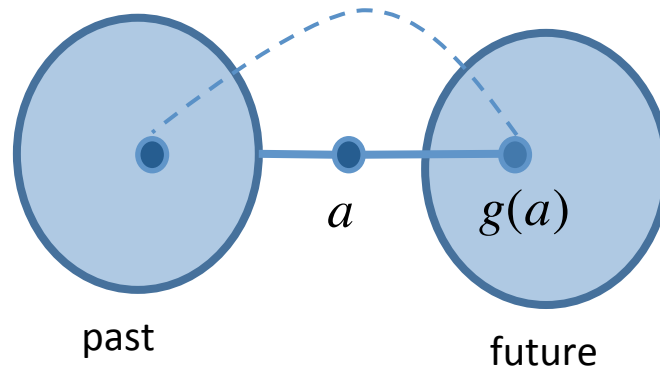
- measure
- then correct (great!)

- Can measure first, then correct
 - how to choose correction set?
 - consistent time order?

} gFlow

gFlow

- Find a good set of neighbours to to corrections in a *consistent* way



1) $g(a)$ is in 'future' of a

2) It corrects!

3) It does not interfere with previous corrections

(time order)

(neighbour / odd edges)

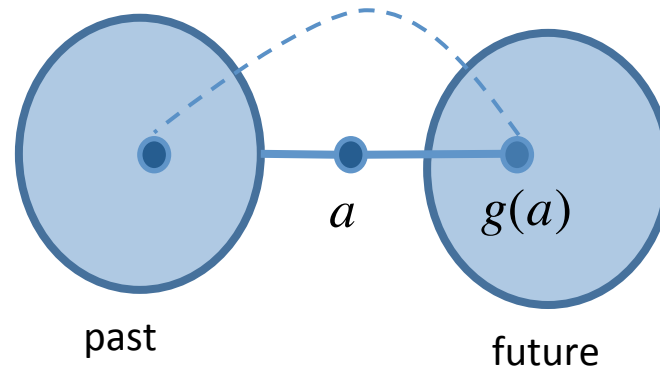
(not neighbour / even to
past)

- $\prod_{i \in g(a)} K_i$ gives you a Z_a , and nothing on past
 - Achronycal correction $\left(Z_a \prod_{i \in g(a)} K_i \right)^{r_a}$

- Anticorrolation with X_a (Logical operator update)
(translation to AQC)

gFlow

- Find a good set of neighbours to to corrections in a *consistent* way



- 1) $g(a)$ is in 'future' of a
- 2) It corrects!
- 3) It does not interfere with previous corrections

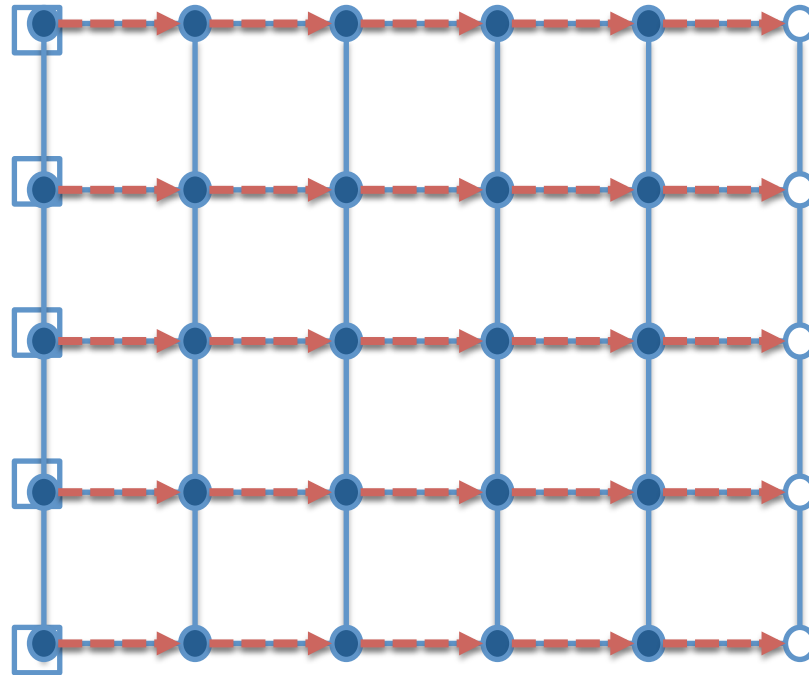
(time order)
(neighbour / odd edges)
(not neighbour / even to
past)

$$\left(Z_a \prod_{i \in g(a)} K_i \right)^{r_a}$$

- Optimisation of time/depth
- Optimisation of number of qubits
- Information light cone
- Simulatability / universality
- Translation to AQC

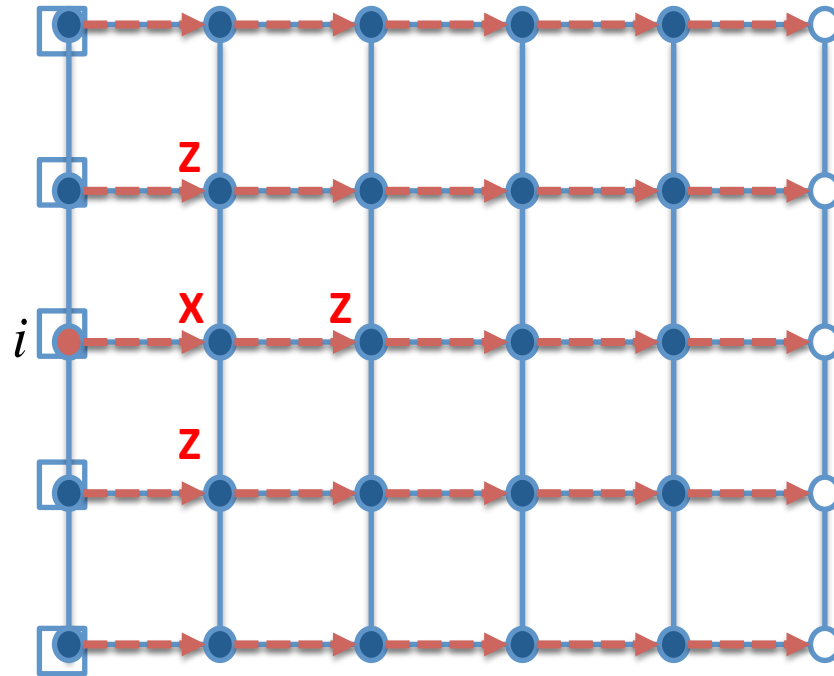
Light Cones

- E.g. Cluster state



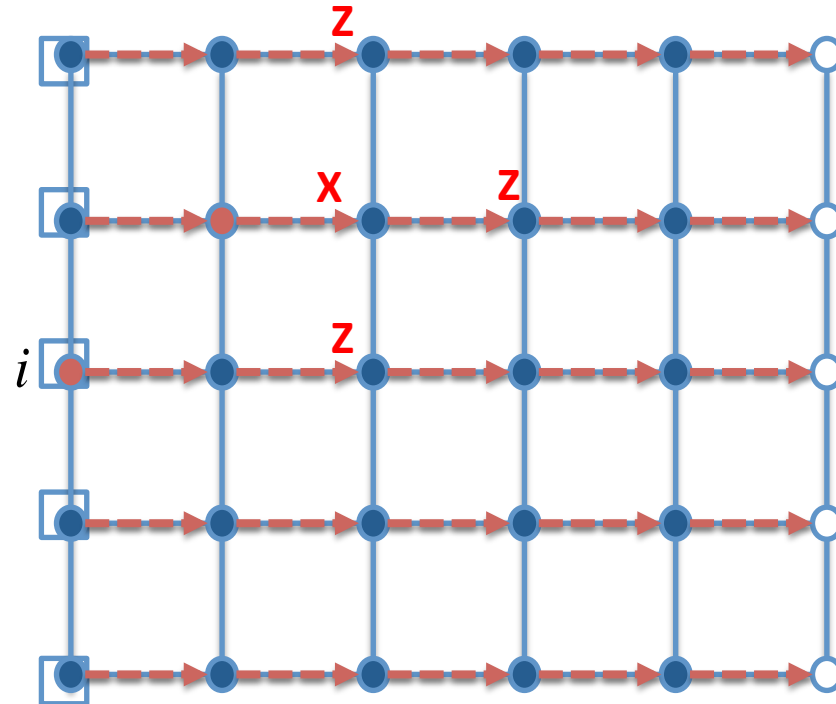
Light Cones

- E.g. Cluster state



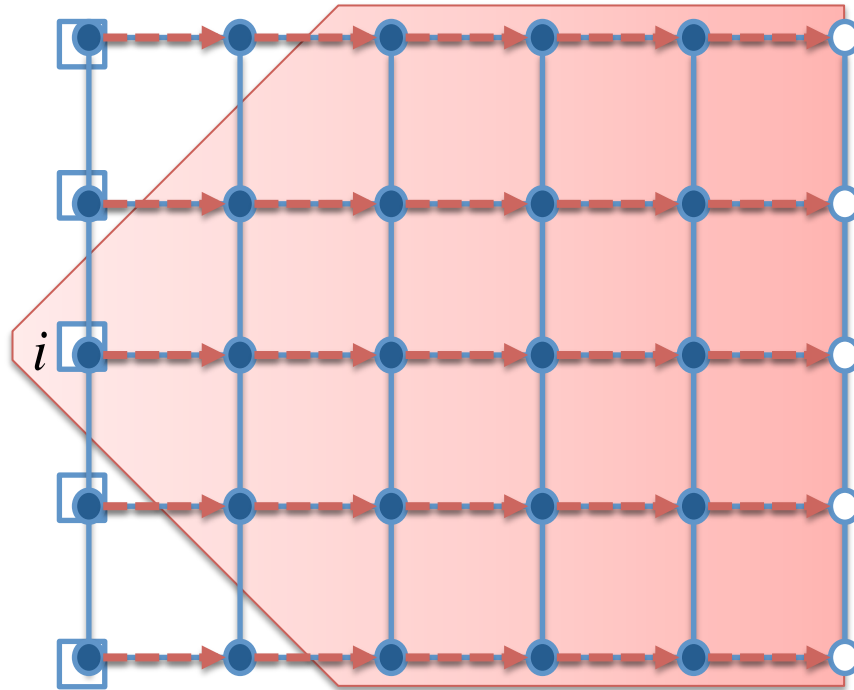
Light Cones

- E.g. Cluster state



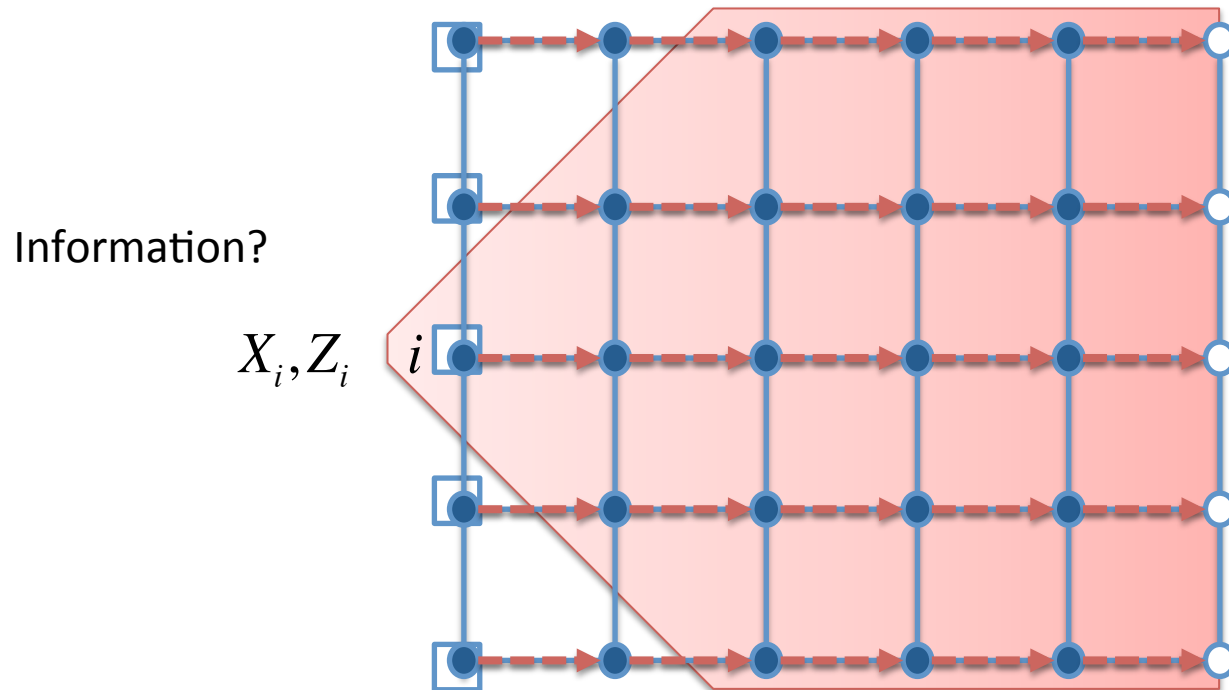
Light Cones

- E.g. Cluster state: causal light cone



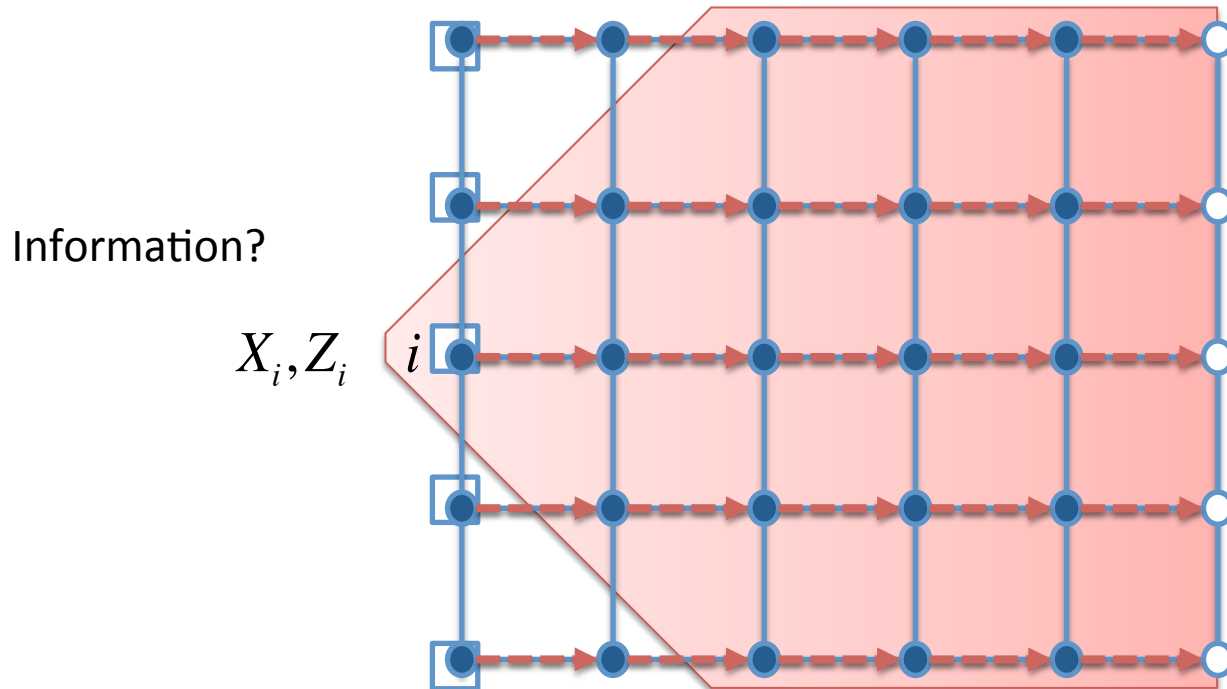
Light Cones

- E.g. Cluster state: causal light cone



Light Cones

- E.g. Cluster state: causal light cone



- Logical operators X_i, Z_i spread across the same cone!
-> information light cone

Information spread and simulation

- Logical Heisenberg picture

$$\rho = \frac{1}{2}(I + \eta_x X + \eta_y Y + \eta_z Z) \quad \Rightarrow \quad \tilde{\rho} = \frac{1}{2}(I + \eta_x \tilde{X} + \eta_y \tilde{Y} + \eta_z \tilde{Z})$$

- Trace complete set of logical operators

$$L_{X_i} \quad \Rightarrow \quad \tilde{L}_{X_i}$$

$$\langle \varphi | L_{X_i} | \varphi \rangle = \langle \tilde{\varphi} | \tilde{L}_{X_i} | \tilde{\varphi} \rangle$$

E.g. Unitary

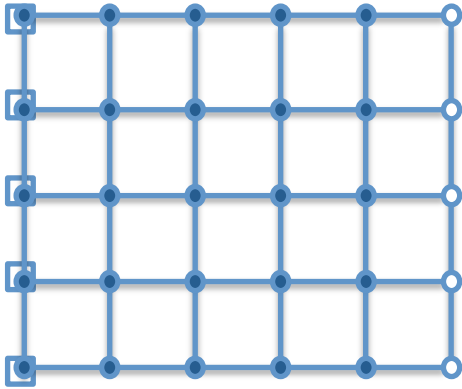
$$L_{X_i} \quad \Rightarrow \quad \tilde{L}_\alpha = U L_{X_i} U^\dagger$$

$$\langle \varphi | L_{X_i} | \varphi \rangle = \langle \varphi | U^\dagger \tilde{L}_\alpha U | \varphi \rangle$$

- All information can be read from $\tilde{L}_{X_i}$
 -> location of info ~ extent of $\tilde{L}_{X_i}$

Information spread and simulation

- Graph state MBQC



$$K_i := X_i \otimes \prod_{(i,j) \in Ed} Z_j$$

$$K_i |G(\varphi)\rangle = |G(\varphi)\rangle \quad \forall i \notin I$$

Space of dim. $2^{|I|}$

- Stabilisers are logical identities

$$L_\alpha \approx L_\alpha K_i$$

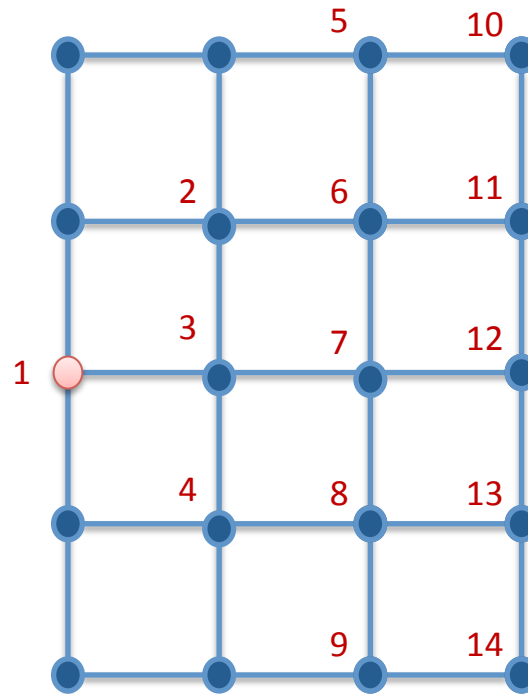
$$\langle G(\varphi) | L_\alpha | G(\varphi) \rangle = \langle G(\varphi) | L_\alpha K_i | G(\varphi) \rangle$$

- Measurements?

- If $[L_\alpha, M] = 0 \rightarrow L_\alpha$ do not change!
- Use stabilisers (logical identities)... choice? $\rightarrow$ gFlow

Information spread and simulation

- E.g. Cluster state

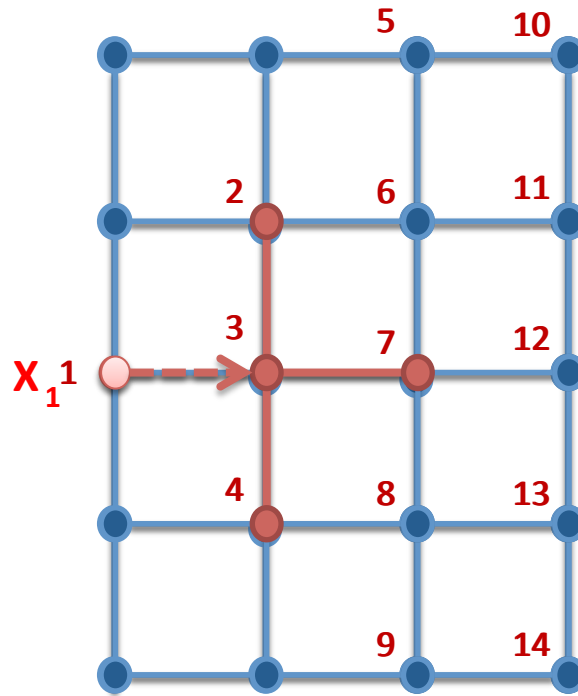


$$L_{X_1} = X_1 \otimes Z_3$$

$$L_{Z_1} = Z_1$$

Information spread and simulation

- E.g. Cluster state

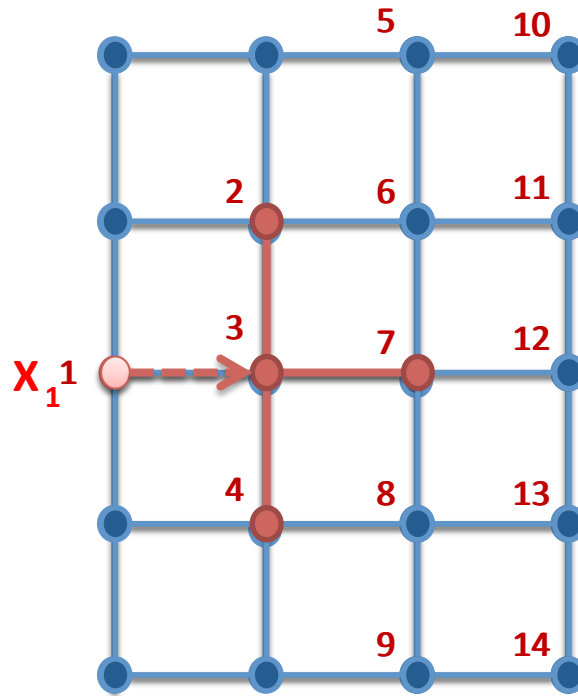


$$L_{X_1} = X_1 \otimes Z_3$$

$$L_{Z_1} = Z_1 K_3$$

Information spread and simulation

- E.g. Cluster state

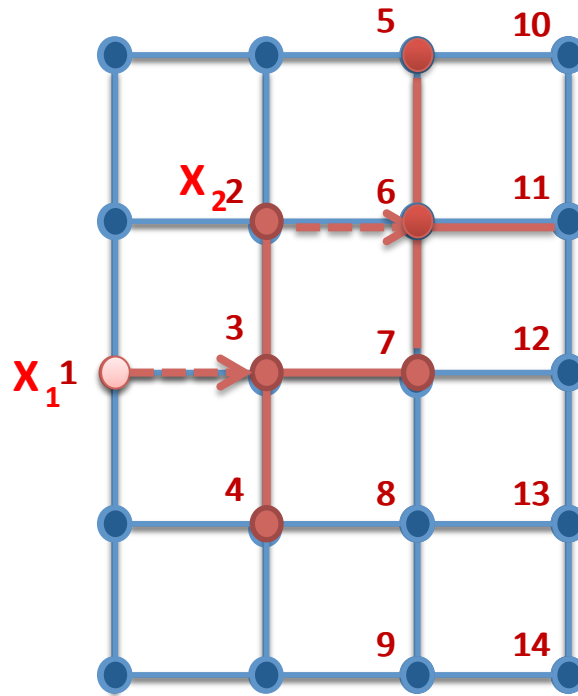


$$L_{X_1} = X_1 \otimes Z_3$$

$$L_{Z_1} = I_1 \otimes Z_2 \otimes X_3 \otimes Z_4 \otimes Z_7$$

Information spread and simulation

- E.g. Cluster state

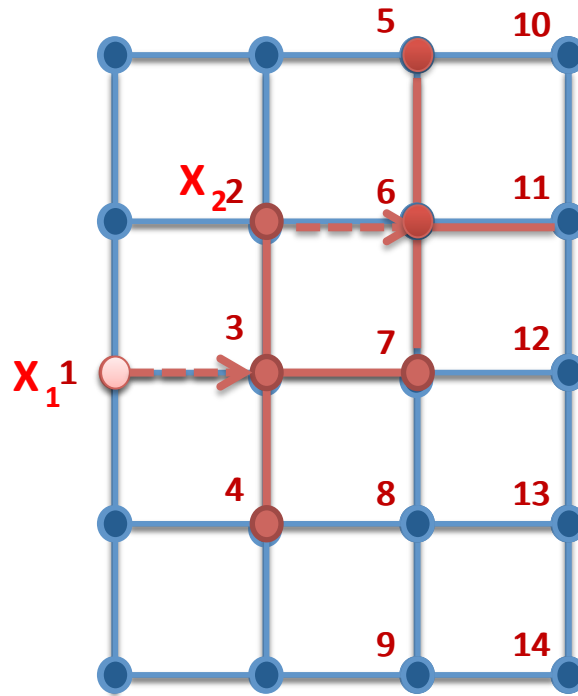


$$L_{X_1} = X_1 \otimes Z_3$$

$$L_{Z_1} = I_1 \otimes Z_2 \otimes X_3 \otimes Z_4 \otimes Z_7 K_6$$

Information spread and simulation

- E.g. Cluster state



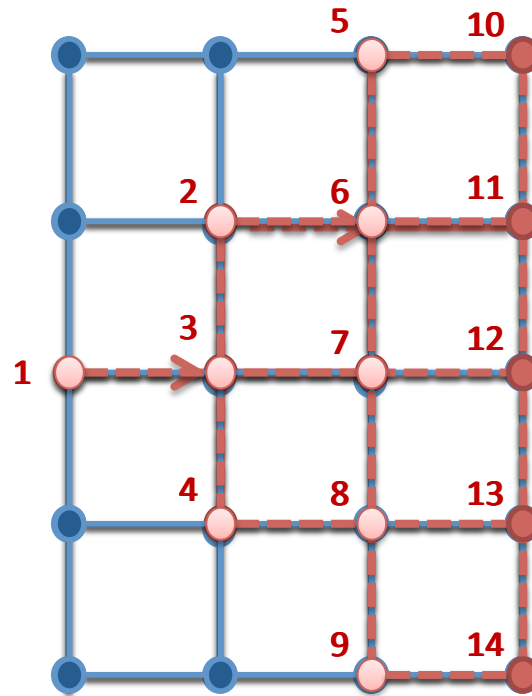
$$L_{X_1} = X_1 \otimes Z_3$$

$$L_{Z_1} = I_1 \otimes I_2 \otimes X_3 \otimes Z_4 \otimes Z_5 \otimes X_6 \otimes I_7 \otimes Z_{11}$$

$$L_{Z_1} = X_{10} \otimes Z_{11} \otimes X_{12} \otimes Z_{13} \otimes X_{14}$$

Information spread and simulation

- E.g. Cluster state



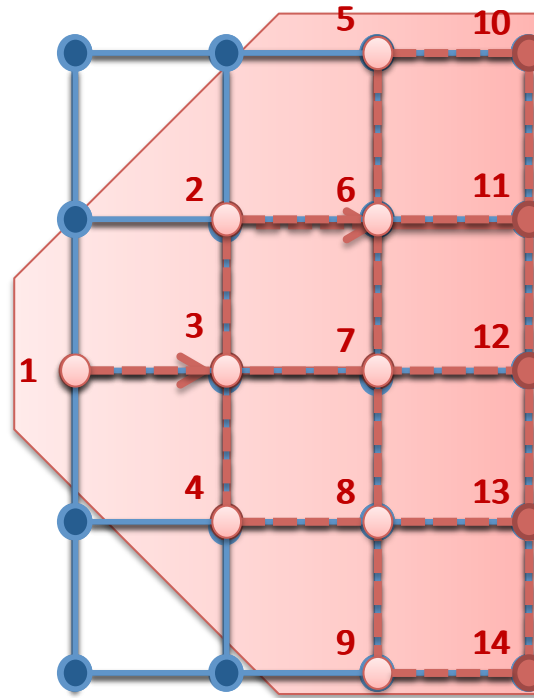
- General case: round by round

- if $\{X_i, L_\alpha\} = 0$

$$L_\alpha \longrightarrow L_\alpha \prod_{j \in g(i)} K_j$$

Information spread and simulation

- E.g. Cluster state



- General case: round by round

- if $\{X_i, L_\alpha\} = 0$

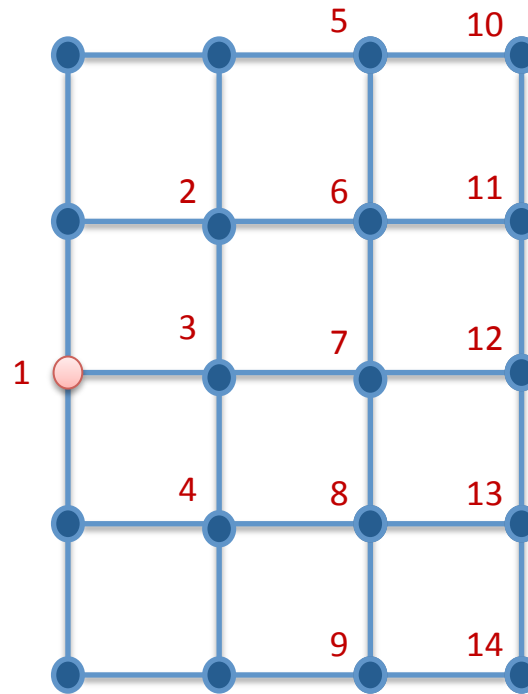
$$L_\alpha \longrightarrow L_\alpha \prod_{j \in g(i)} K_j$$

- Information forward cone: spread across F_C

Information spread and simulation

- E.g. Cluster state: general angles

- $M_a^\theta = P_a^{+\theta} - P_a^{-\theta}$ rotate by $Z(\theta)$ and measure X



$$K_i^{\theta_i} := \cos(\theta_i) X_i \otimes \prod_{(i,j) \in Ed} Z_j + i \sin(\theta_i) Z_i X_i \otimes \prod_{(i,j) \in Ed} Z_j$$

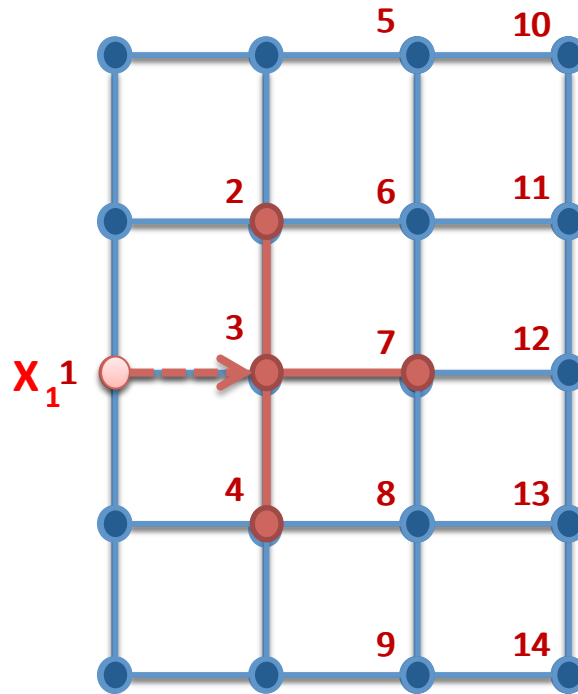
$$L_{X_1} = \cos(\theta_1) X_1 \otimes Z_3 + i \sin(\theta_1) Z_1 X_1 \otimes Z_3$$

$$L_{Z_1} = Z_1$$

Information spread and simulation

- E.g. Cluster state: general angles

- $M_a^\theta = P_a^{+\theta} - P_a^{-\theta}$ rotate by $Z(\theta)$ and measure X



$$K_i^{\theta_i} := \cos(\theta_i) X_i \otimes \prod_{(i,j) \in Ed} Z_j + i \sin(\theta_i) Z_i X_i \otimes \prod_{(i,j) \in Ed} Z_j$$

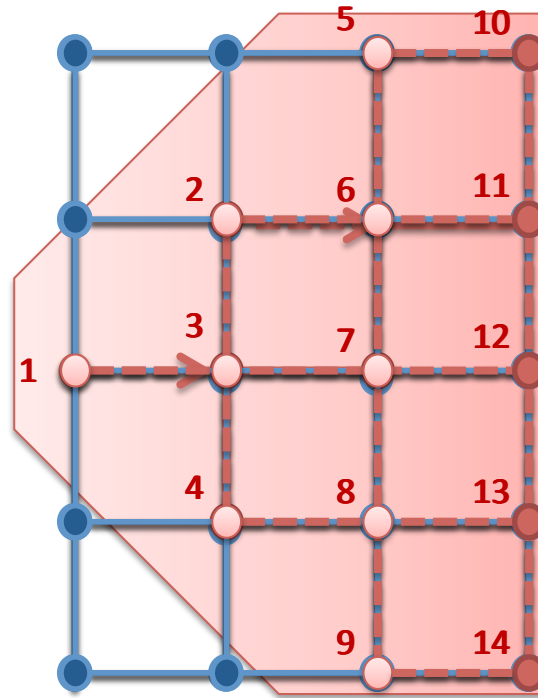
$$L_{X_1} = \cos(\theta_1) X_1 \otimes Z_3 + i \sin(\theta_1) Z_1 X_1 \otimes Z_3$$

$$L_{Z_1} = Z_1$$

- Every time we use a stabiliser, double terms (or more)

Information spread and simulation

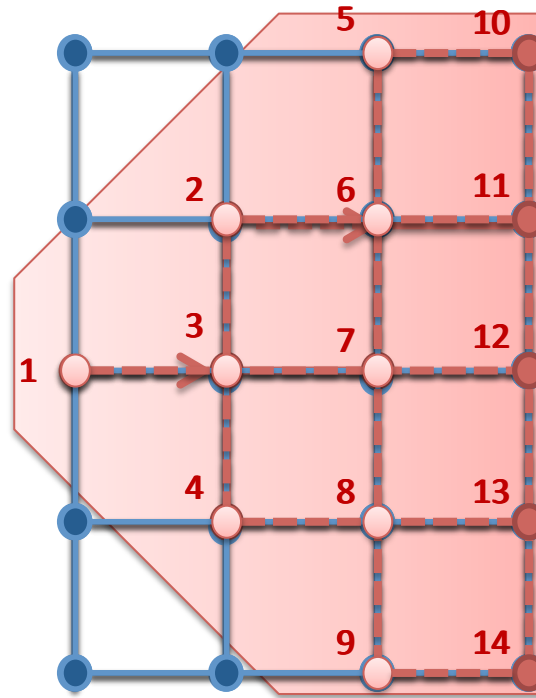
- E.g. Cluster state



- Information forward cone: spread across F_C
- Cost of simulation $O(\exp(F_C))$

Information spread and simulation

- E.g. Cluster state



- Information forward cone: spread across F_C
- Cost of simulation $O(\exp(F_C))$ **worst case angles!**
- efficient for Pauli (Clifford) $\theta = 0, \pi$

Universality?

- Balance:

Spread
(via ent)

Vs

Use of spread
(# ways of using ent)

Universality?

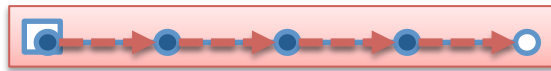
- Balance:

Spread
(via ent)

Vs

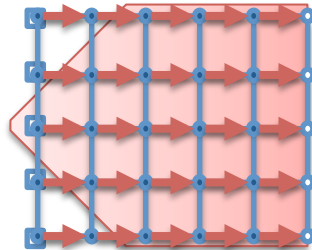
Use of spread
(# ways of using ent)

- e.g.
1D)



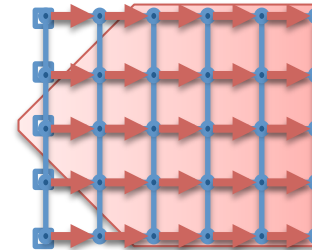
Limited spread

2D)



Spread balanced with use (arbitrary θ)

2D) Pauli



Spread, but not 'used' ($\theta = 0, \pi$)

Universality?

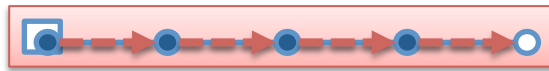
- Balance:

Spread
(via ent)

Vs

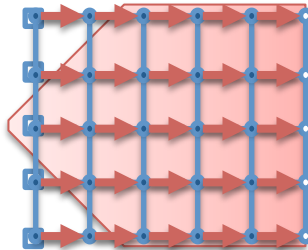
Use of spread
(# ways of using ent)

- e.g.
1D)

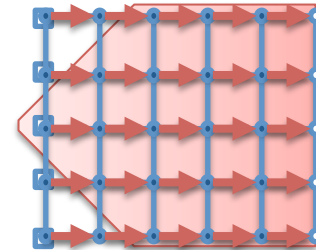


Limited spread

2D)



2D) Pauli



Spread balanced with use (arbitrary θ)

Spread, but not 'used' ($\theta = 0, \pi$)

- Analogy to 2nd Law / phase transition?

Energy

Vs

Entropy?

MBQC and gFlow

- Structure for feed forward: corrections and time order
- Natural spread of information
 - Simulation $O(\exp(F_C))$
 - Information light cone F_C
- True difficulty in simulation / universality balance

Spread vs Use

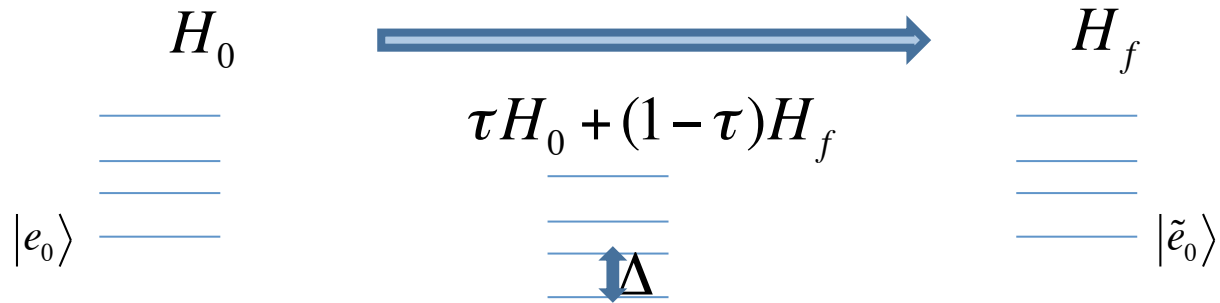
MBQC and gFlow

- Structure for feed forward: corrections and time order
- Natural spread of information
 - Simulation $O(\exp(F_C))$
 - Information light cone F_C
- True difficulty in simulation / universality balance

Spread vs Use

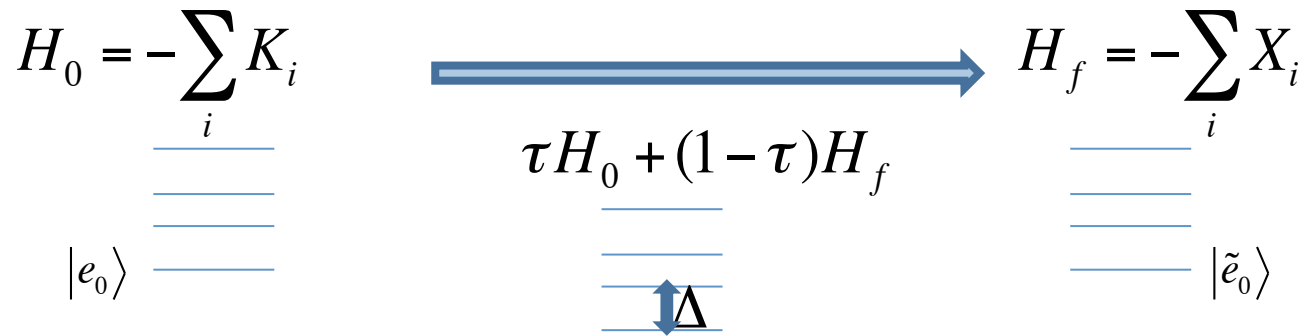
Not simple! (clifford + $\pi/8$)
-> maybe gFlow helps (same language)

AQC and gFlow?



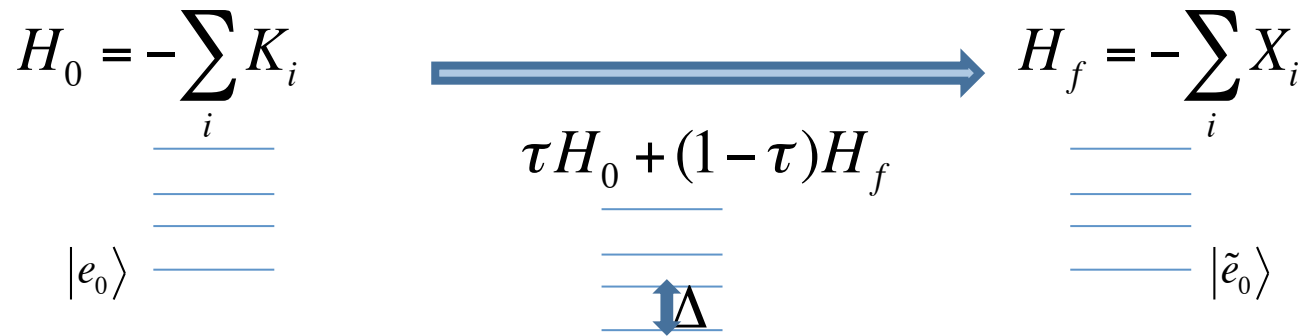
- Adiabatic theorem: slow enough, stay in ground state

AQC and gFlow?



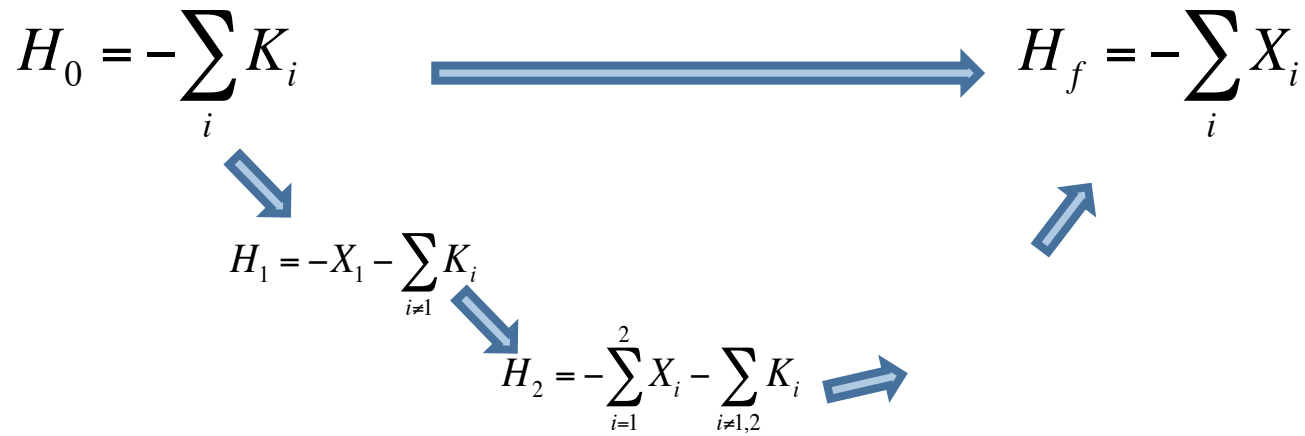
- Adiabatic theorem: slow enough, stay in ground state
- Bacon Flammia, cluster state $\rightarrow$ AQC

AQC and gFlow?



- Adiabatic theorem: slow enough, stay in ground state
- Bacon Flammia, cluster state $\rightarrow$ AQC
- Use gFlow to generalise AGSQC

AGSQC and gFlow



- gFlow gives natural H_i

- Easy to solve

- Tradeoff?

Classical computation $\longleftrightarrow$ degree of H_0

- Spread of information bounds t

gFlow AGSQC 1:

step by step

$$H_0 = -\sum_i K_i \Rightarrow H_1 = -X_1 - \sum_{i \neq 1} K_i \Rightarrow H_2 = -\sum_{i=1}^2 X_i - \sum_{i \neq 1,2} K_i \Rightarrow \dots \Rightarrow H_f = -\sum_i X_i$$

- gFlow implies gives natural H_i

$$\forall i, \exists \alpha(i) \in g(i) \text{ s.t.}$$

$$\{X_i, K_{\alpha(i)}\} = 0 \quad [X_i, K_{j>i}] = 0$$

$$\begin{aligned} H(\tau) &= \tau \left(-\sum_i K_i \right) + (1-\tau) \left(-X_1 - \sum_{\substack{j \neq \alpha(i) \\ j \geq i}} K_j \right) \\ &= \tau K_{\alpha(1)} + (1-\tau) \left(-X_1 - \sum_{\substack{j \neq \alpha(i) \\ j \approx i}} K_j \right) + \sum_{j>i} K_j \end{aligned}$$

gFlow AGSQC 1:

step by step

$$H_0 = -\sum_i K_i \Rightarrow H_1 = -X_1 - \sum_{i \neq 1} K_i \Rightarrow H_2 = -\sum_{i=1}^2 X_i - \sum_{i \neq 1,2} K_i \Rightarrow \dots \Rightarrow H_f = -\sum_i X_i$$

- gFlow implies gives natural H_i

$$\forall i, \exists \alpha(i) \in g(i) \text{ s.t.}$$

$$\{X_i, K_{\alpha(i)}\} = 0 \quad [X_i, K_{j>i}] = 0$$

$$H(\tau) = \tau \left(-\sum_i K_i \right) + (1-\tau) \left(-X_1 - \sum_{\substack{j \neq \alpha(i) \\ j \geq i}} K_j \right)$$

$$= \left(K_{\alpha(1)} + (1-\tau) \left(-X_1 - \sum_{\substack{j \neq \alpha(i) \\ j \approx i}} K_j \right) \right) + \sum_{\substack{j \neq \alpha(i) \\ j > i}} K_j$$

- time

$$t = O(\text{poly}(n))$$

gFlow AGSQC 2:

Round by round

$$\tilde{H}_0 = -\sum_i T_i \Rightarrow \tilde{H}_1 = -\sum_{i \in R_1} X_i - \sum_{i \notin R_1} T_i \Rightarrow \tilde{H}_2 = -\sum_{i \in R_1 R_2} X_i - \sum_{i \notin R_1 R_2} T_i \Rightarrow \dots \Rightarrow H_f = -\sum_i X_i$$

- Play with degree using gFlow

$$\tilde{H}_0 = -\sum_i T_i \quad T_i = \prod_{j \in g(i)} K_j$$

-> same ground state space, same spectrum

$$\{X_i, T_i\} = 0 \quad [X_i, T_{j \geq i}] = 0$$

- Round by round, as gFlow

-> not quite $t = \text{depth}(MBQC)$ as is [work in progress!]

- Trade-off

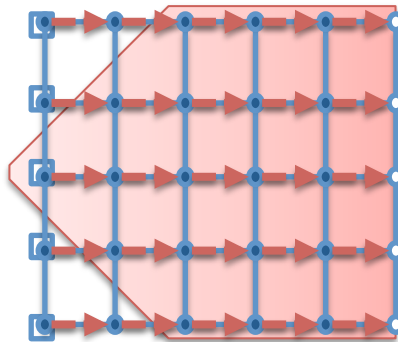
-> speed against degree

gFlow AGSQC 2:

Direct

$$H_0 = -\sum_i K_i \quad \longrightarrow \quad H_f = -\sum_i X_i$$

- Speed t depends on spread (finite speed of spread)



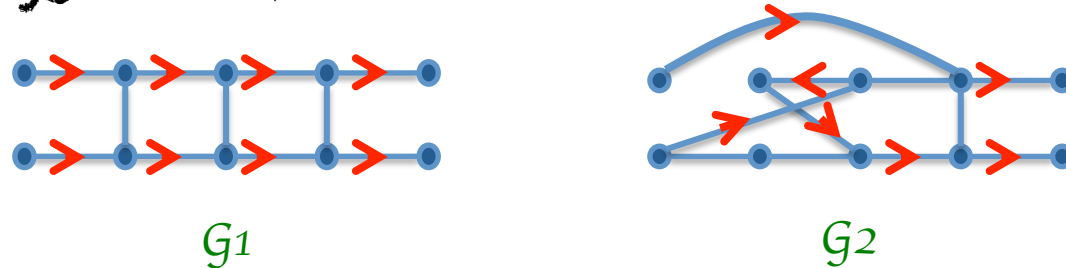
- Trade-off: countered by high degree

$$\tilde{H}_0 = -\sum_i T_i \quad \longrightarrow \quad H_f = -\sum_i X_i$$

Conclusions

- gFlow shows information spread

Information light cone = causal light cone
Playground for causal order?



- Spread bounds simulation

Cost $O(\exp(F_C))$

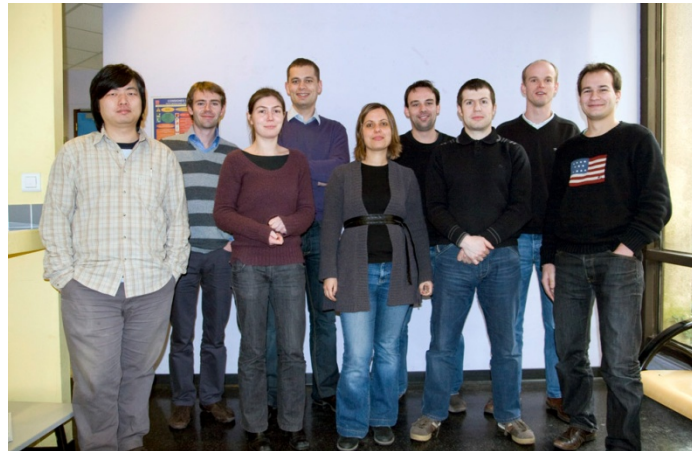
- 'Good' resource

Balance: Spread Vs 'Use'

- General translation to AGSQC

Translation of trade-offs?
Notions of spread

Thank you!



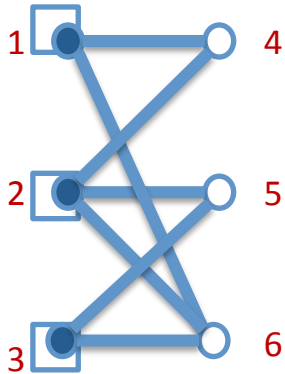
<http://iq.enst.fr/>

LOOKING FOR POST DOCS



Examples

- Sometimes need more than one in correcting set



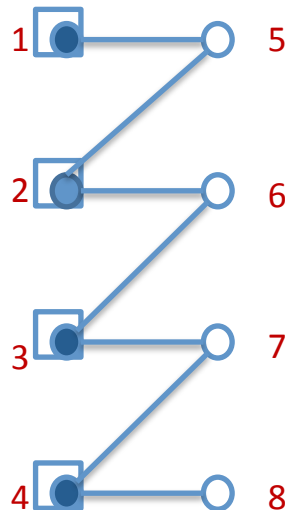
$$g(1) = 4$$

$$g(2) = 5$$

$$g(3) = 4, 6$$

$$1 < 2 < 3$$

- Not unique (allows for tradeoff) A. Broadbent, E. Kashefi TCS '07, D. Browne, E. Kashefi and S. Perdrrix TQC '10



$$g(i) = i + 4$$

$$1 < 2 < 3 < 4$$

$$\# rounds = n$$

$$g(i) = 5, \dots, i + 4$$

$$g(1) = 5$$

$$g(2) = 5, 6$$

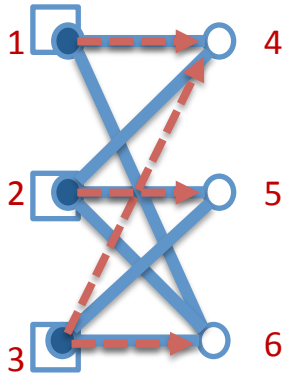
...

$$1 \approx 2 \approx 3 \approx 4$$

$$\# rounds = 1$$

Examples

- Sometimes need more than one in correcting set



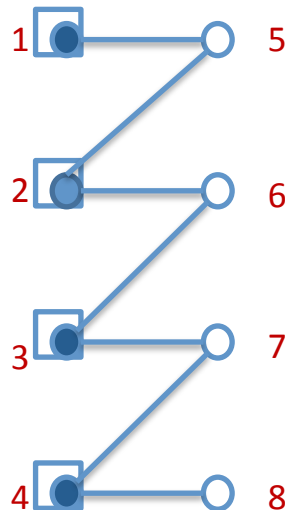
$$g(1) = 4$$

$$g(2) = 5$$

$$g(3) = 4, 6$$

$$1 < 2 < 3$$

- Not unique (allows for tradeoff) A. Broadbent, E. Kashefi TCS '07, D. Browne, E. Kashefi and S. Perdrix TQC '10



$$g(i) = i + 4$$

$$1 < 2 < 3 < 4$$

$$\# rounds = n$$

$$g(i) = 5, \dots, i + 4$$

$$g(1) = 5$$

$$g(2) = 5, 6$$

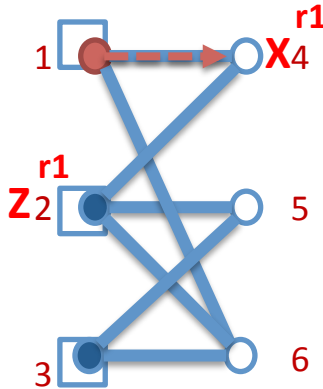
...

$$1 \approx 2 \approx 3 \approx 4$$

$$\# rounds = 1$$

Examples

- Sometimes need more than one in correcting set



$$g(1) = 4$$

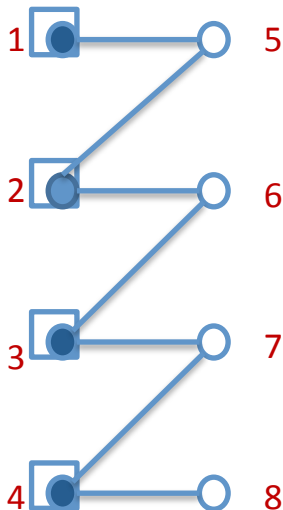
$$K_4 = Z_1 \otimes Z_2 \otimes X_4$$

$$g(2) = 5$$

$$g(3) = 4, 6$$

$$1 < 2 < 3$$

- Not unique (allows for tradeoff) A. Broadbent, E. Kashefi TCS '07, D. Browne, E. Kashefi and S. Perdrix TQC '10



$$g(i) = i + 4$$

$$g(i) = 5, \dots, i + 4$$

$$g(1) = 5$$

$$g(2) = 5, 6$$

...

$$1 < 2 < 3 < 4$$

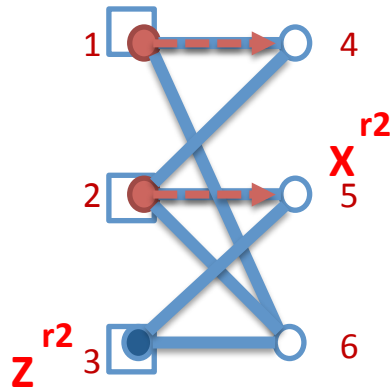
$$1 \approx 2 \approx 3 \approx 4$$

$$\# rounds = n$$

$$\# rounds = 1$$

Examples

- Sometimes need more than one in correcting set



$$g(1) = 4$$

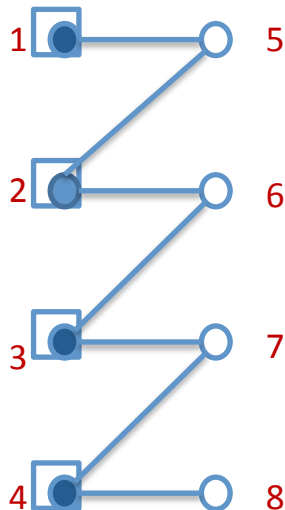
$$g(2) = 5$$

$$g(3) = 4, 6$$

$$1 < 2 < 3$$

$$K_5 = Z_2 \otimes Z_3 \otimes X_5$$

- Not unique (allows for tradeoff) A. Broadbent, E. Kashefi TCS '07, D. Browne, E. Kashefi and S. Perdrix TQC '10



$$g(i) = i + 4$$

$$1 < 2 < 3 < 4$$

$$\# rounds = n$$

$$g(i) = 5, \dots, i + 4$$

$$g(1) = 5$$

$$g(2) = 5, 6$$

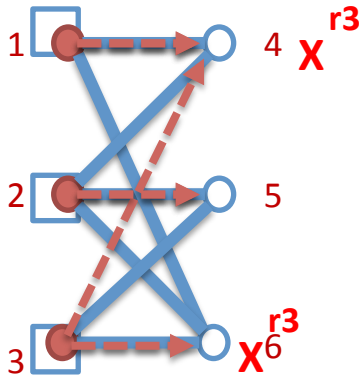
...

$$1 \approx 2 \approx 3 \approx 4$$

$$\# rounds = 1$$

Examples

- Sometimes need more than one in correcting set



$$g(1) = 4$$

$$g(2) = 5$$

$$g(3) = 4, 6$$

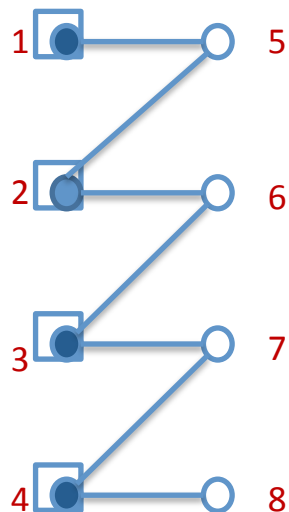
$$1 < 2 < 3$$

$$K_4 K_6 = X_4 \otimes X_6$$

Other Z s cancel

- Not unique (allows for tradeoff)

A. Broadbent, E. Kashefi TCS '07, D. Browne, E. Kashefi and S. Perdrix TQC '10



$$g(i) = i + 4$$

$$1 < 2 < 3 < 4$$

$$\# rounds = n$$

$$g(i) = 5, \dots, i + 4$$

$$g(1) = 5$$

$$g(2) = 5, 6$$

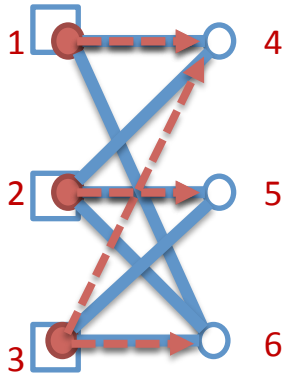
...

$$1 \approx 2 \approx 3 \approx 4$$

$$\# rounds = 1$$

Examples

- Sometimes need more than one in correcting set



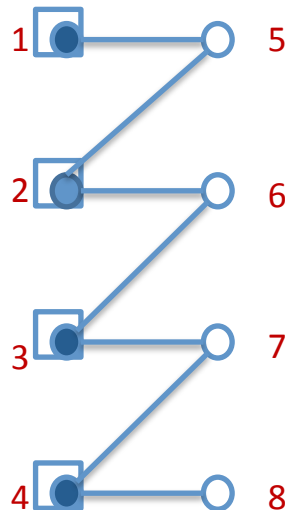
$$g(1) = 4$$

$$g(2) = 5$$

$$g(3) = 4, 6$$

$$1 < 2 < 3$$

- Not unique (allows for tradeoff) A. Broadbent, E. Kashefi TCS '07, D. Browne, E. Kashefi and S. Perdrix TQC '10



$$g(i) = i + 4$$

$$1 < 2 < 3 < 4$$

$$\# rounds = n$$

$$g(i) = 5, \dots, i + 4$$

$$g(1) = 5$$

$$g(2) = 5, 6$$

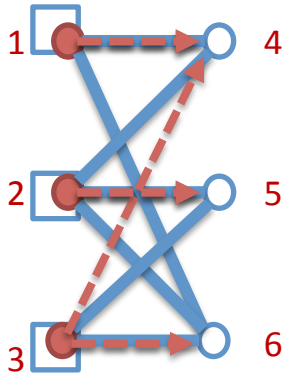
...

$$1 \approx 2 \approx 3 \approx 4$$

$$\# rounds = 1$$

Examples

- Sometimes need more than one in correcting set



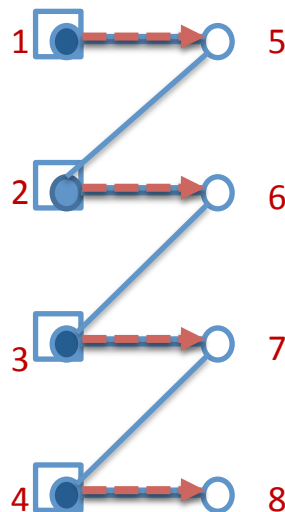
$$g(1) = 4$$

$$g(2) = 5$$

$$g(3) = 4, 6$$

$$1 < 2 < 3$$

- Not unique (allows for tradeoff) A. Broadbent, E. Kashefi TCS '07, D. Browne, E. Kashefi and S. Perdrix TQC '10



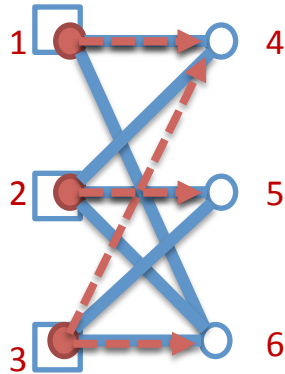
$$g(i) = i + 4$$

$$1 < 2 < 3 < 4$$

$$\# rounds = n$$

Examples

- Sometimes need more than one in correcting set



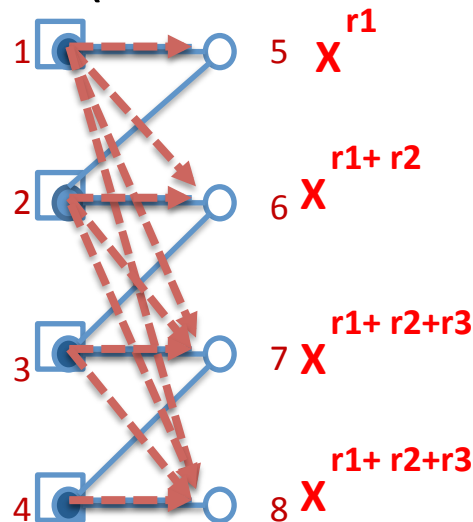
$$g(1) = 4$$

$$g(2) = 5$$

$$g(3) = 4, 6$$

$$1 < 2 < 3$$

- Not unique (allows for tradeoff) A. Broadbent, E. Kashefi TCS '07, D. Browne, E. Kashefi and S. Perdrrix TQC '10



$$g(i) = i + 4$$

$$g(i) = i + 4, \dots, 8$$

$$g(1) = 5, 6, 7, 8$$

$$g(2) = 6, 7, 8$$

...

$$1 \approx 2 \approx 3 \approx 4$$

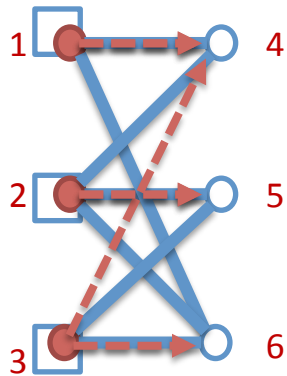
$$\# rounds = 1$$

$$1 < 2 < 3 < 4$$

$$\# rounds = n$$

Examples

- Sometimes need more than one in correcting set



$$g(1) = 4$$

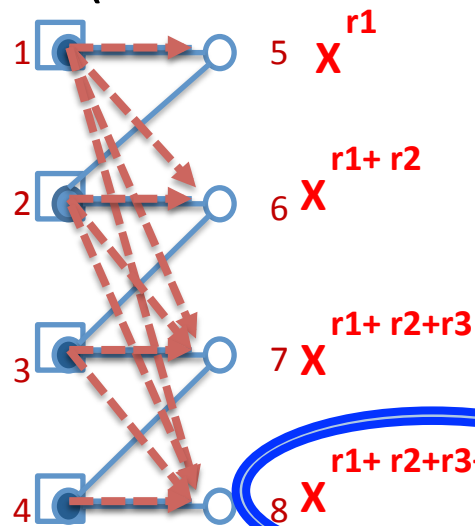
$$g(2) = 5$$

$$g(3) = 4, 6$$

$$1 < 2 < 3$$

- Not unique (allows for tradeoff)

A. Broadbent, E. Kashefi TCS '07, D. Browne, E. Kashefi and S. Perdrix TQC '10



$$g(i) = i + 4$$

$$1 < 2 < 3 < 4$$

$$\# rounds = n$$

$$g(i) = i + 4, \dots, 8$$

$$g(1) = 5, 6, 7, 8$$

$$g(2) = 6, 7, 8$$

...

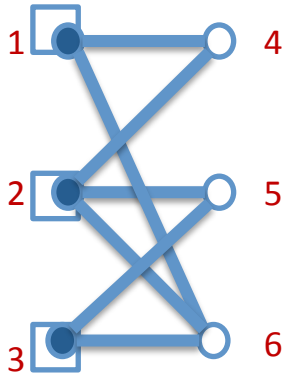
$$1 \approx 2 \approx 3 \approx 4$$

$$\# rounds = 1$$

Classical comp $\log(n)$

Examples

- Sometimes need more than one in correcting set



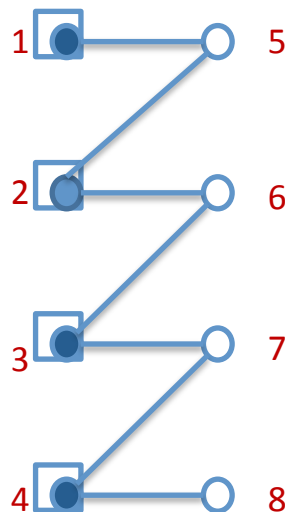
$$g(1) = 4$$

$$g(2) = 5$$

$$g(3) = 4, 6$$

$$1 < 2 < 3$$

- Not unique (allows for tradeoff) A. Broadbent, E. Kashefi TCS '07, D. Browne, E. Kashefi and S. Perdrix TQC '10



$$g(i) = i + 4$$

$$g(i) = i + 4, \dots, 8$$

$$g(1) = 5, 6, 7, 8$$

$$g(2) = 6, 7, 8$$

...

$$1 < 2 < 3 < 4$$

$$1 \approx 2 \approx 3 \approx 4$$

$$\# \text{ rounds} = n$$

$$\# \text{ rounds} = 1$$

$$\text{Classical comp } \text{const.} \quad \text{Classical comp } \log(n)$$