The Power of Unentangled Quantum Proofs with Non-negative Amplitudes

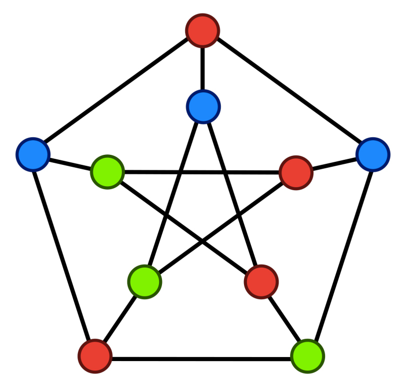
Fernando G. Jeronimo, Pei Wu
Quantum Colloquium @ Simons
April 2023

Quantum Merlin-Arthur (QMA)

poly-size $|\psi\rangle$

$\Pi Q |\psi\rangle |0\rangle$

BQP computation

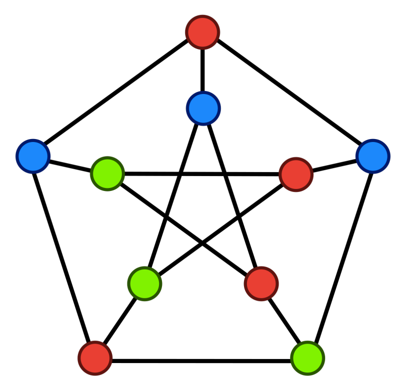


Quantum Merlin-Arthur (QMA)

poly-size $|\psi\rangle$ →

$\Pi Q |\psi\rangle |0\rangle$

BQP computation



(Completeness) $\exists$ a valid coloring:

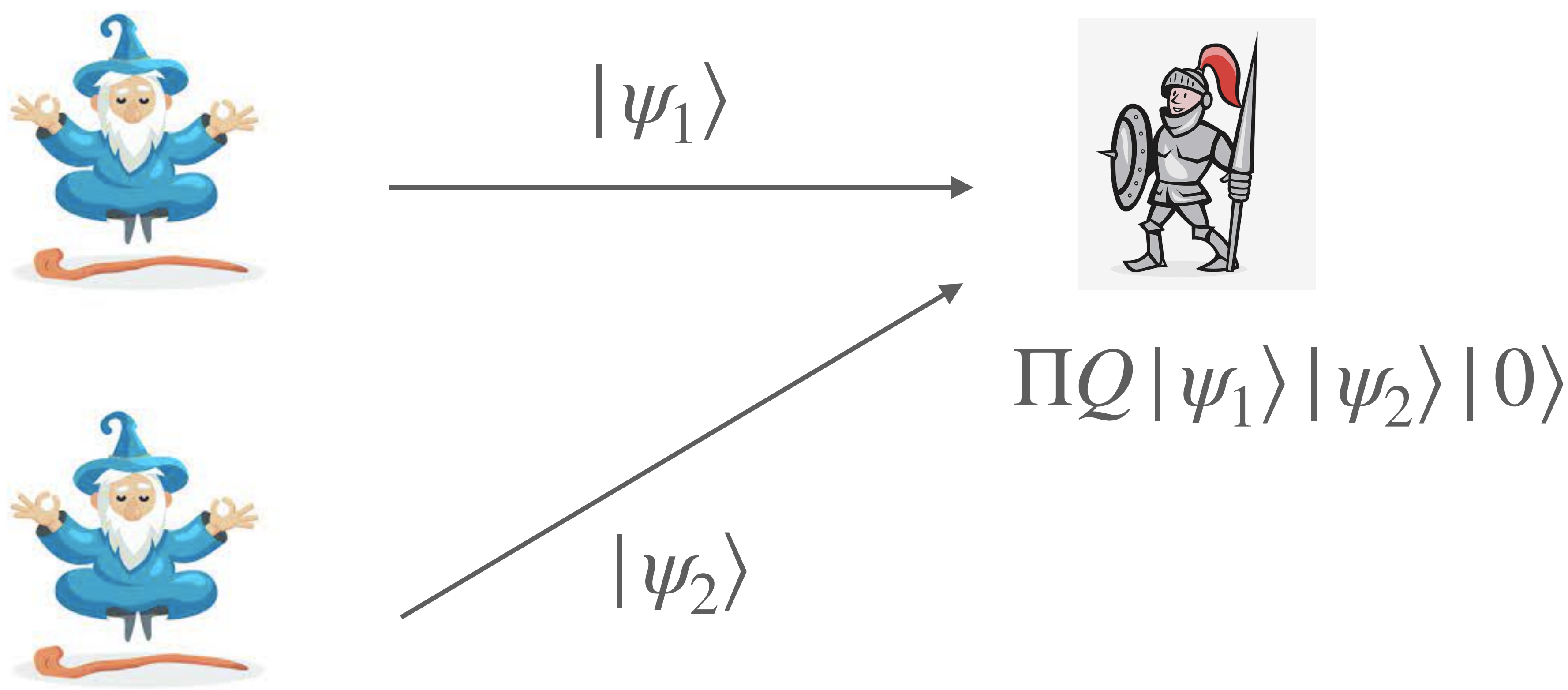
benign Merlin will convince Arthur w.p. $\geq c$

(Soundness) $\nexists$ valid coloring:

no adversarial Merlin can fool Arthur w.p. $\leq s$

the **gap** is $c - s = \Omega(1)$.

Multiple Merlins



Multiple Merlins

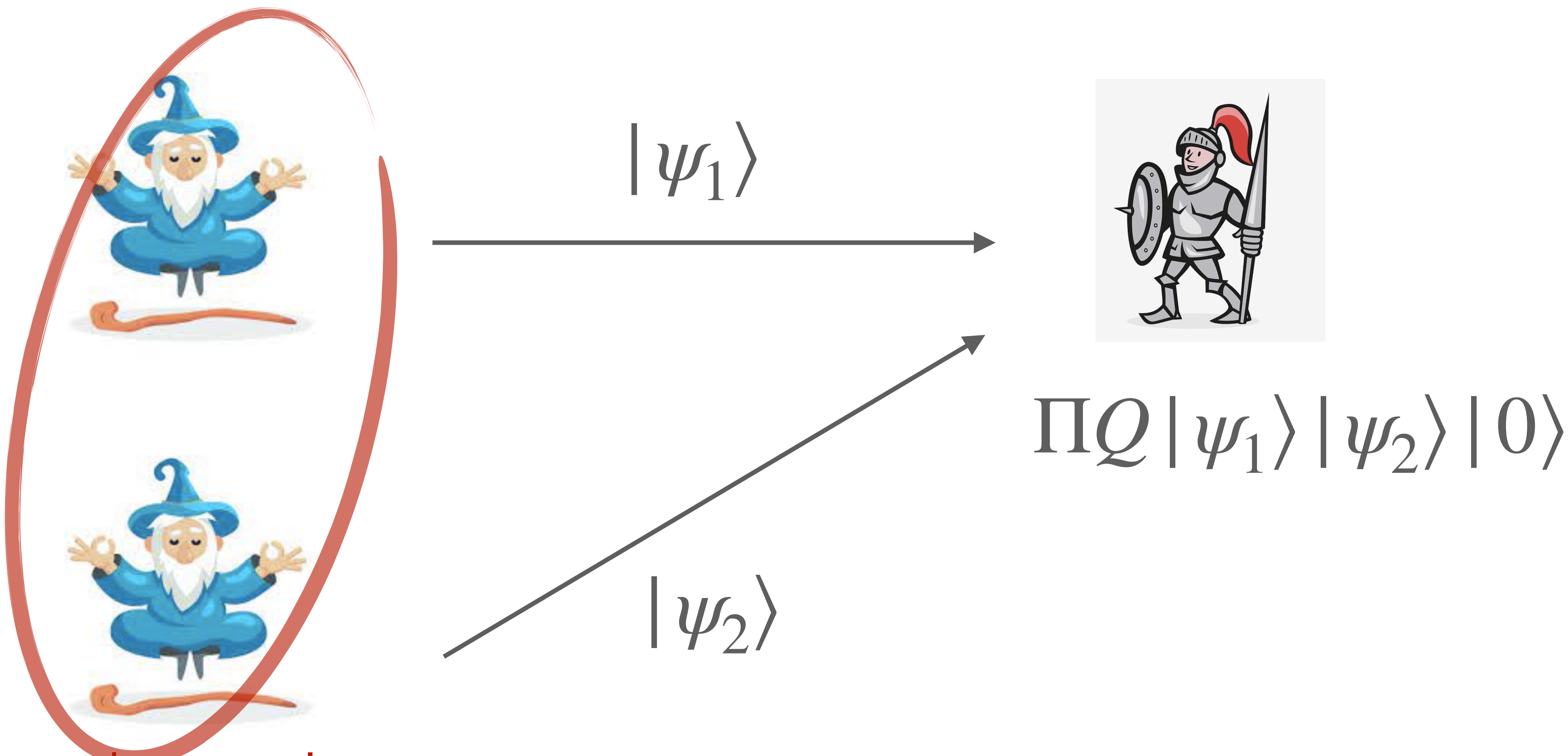
$|\psi_1\rangle$

$|\psi_2\rangle$

$\Pi Q|\psi_1\rangle|\psi_2\rangle|0\rangle$

share no entanglement!

Multiple Merlins



share no entanglement!

(Completeness) ∃ a valid coloring:

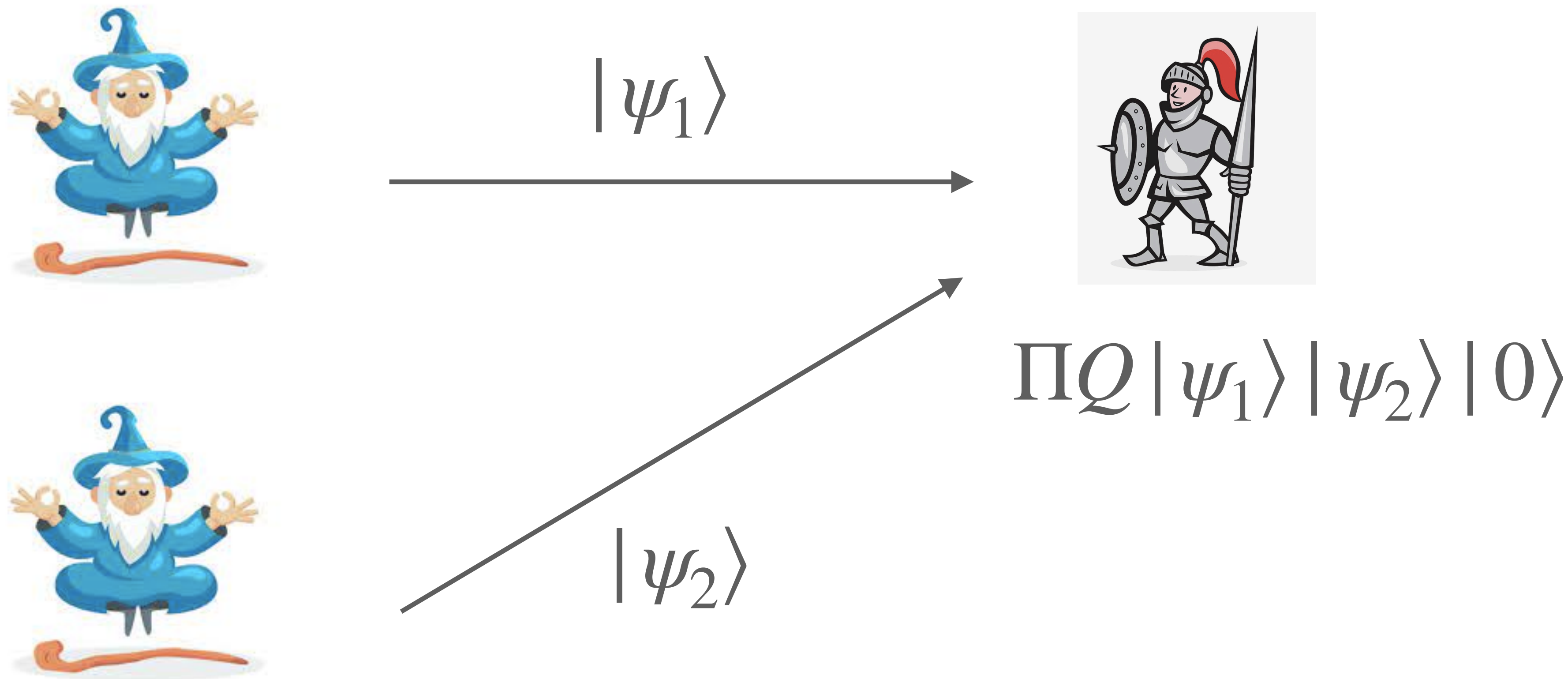
benign Merlins will convince Arthur w.p. $\geq c$

(Soundness) ∄ valid coloring:

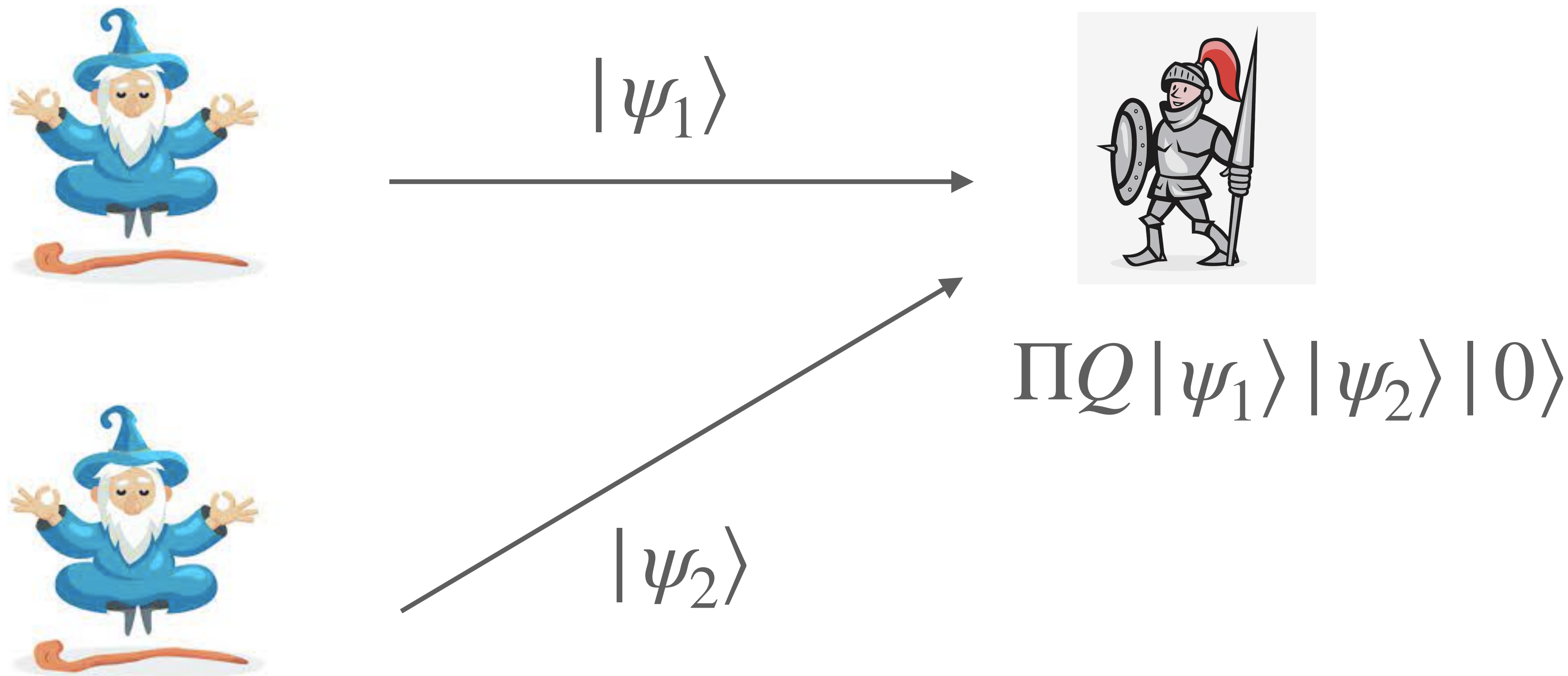
no adversarial Merlins can fool Arthur w.p. $\leq s$

the **gap** is $c - s = \Omega(1)$.

Multiple Merlins

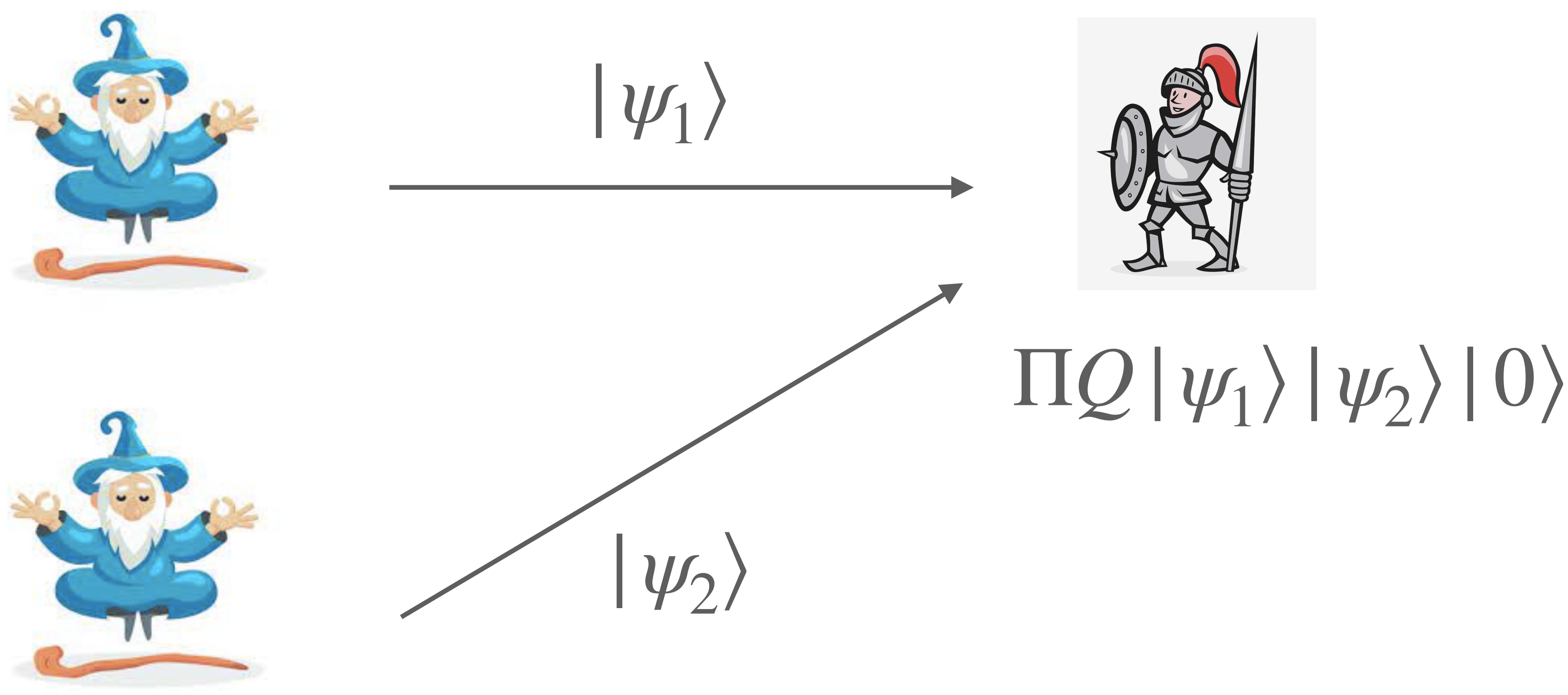


Multiple Merlins



Power of $\mathbf{QMA}(2)$, as a complexity class?

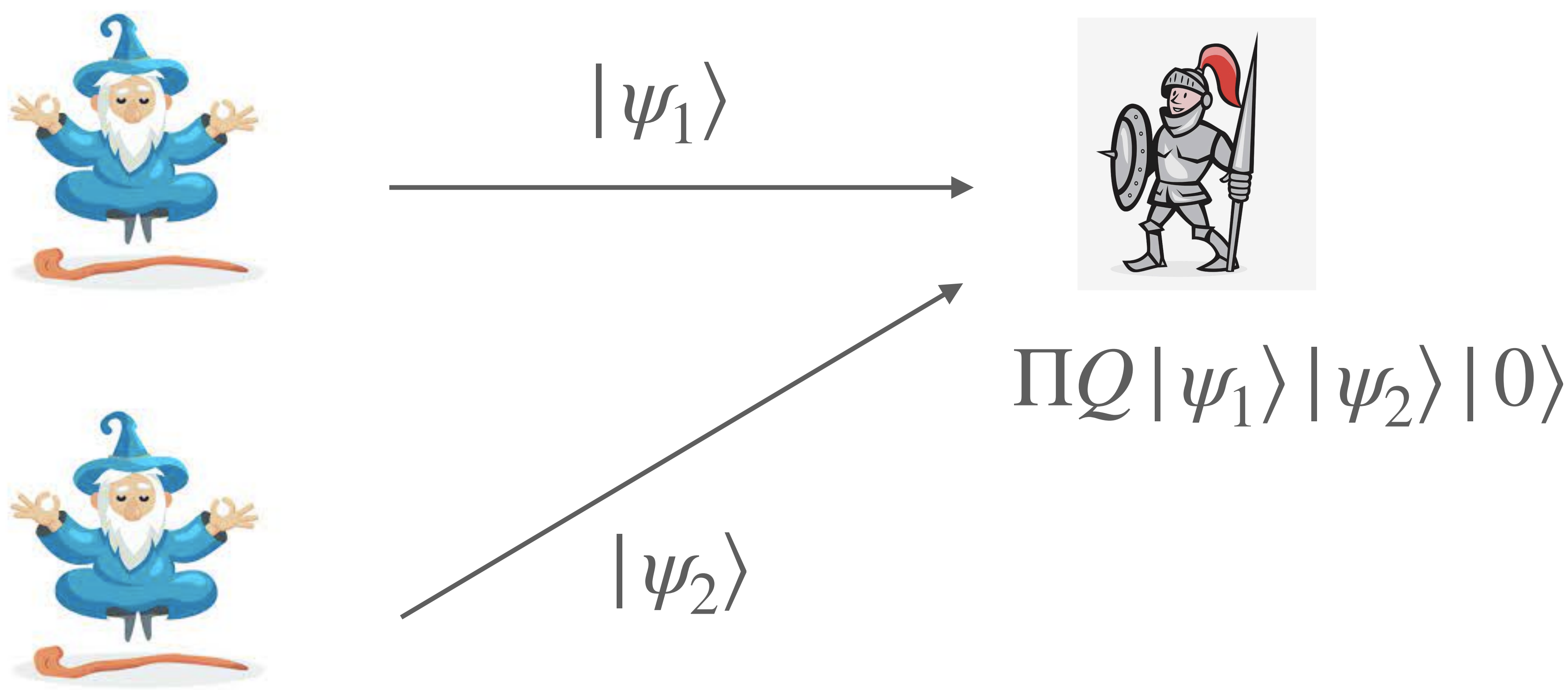
Multiple Merlins



Power of $\mathrm{QMA}(2)$, as a complexity class?

$$\mathrm{QMA} \subseteq \mathrm{QMA}(2)$$

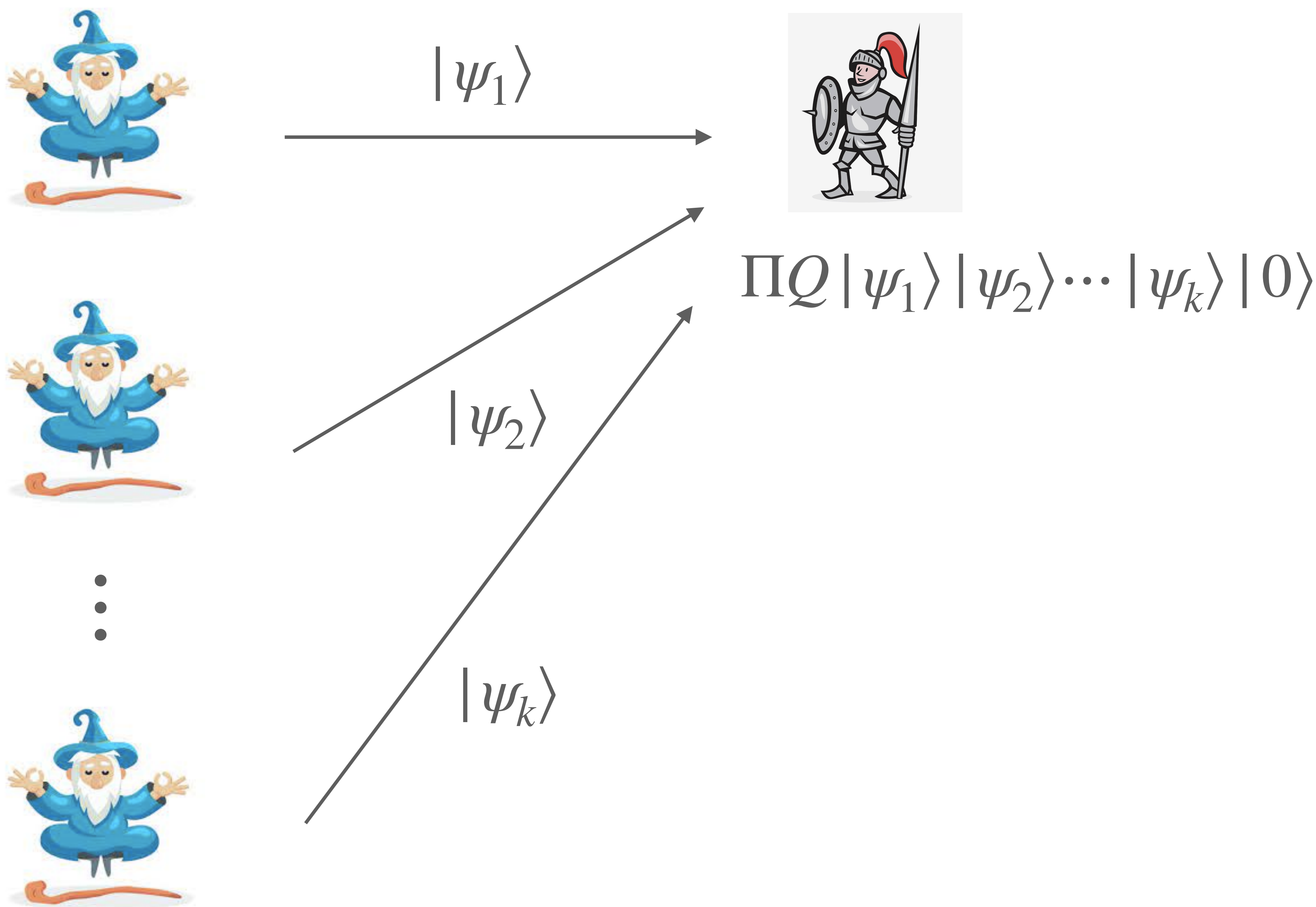
Multiple Merlins



Power of $\mathrm{QMA}(2)$, as a complexity class?

$$\mathrm{QMA} \subseteq \mathrm{QMA}(2) \subseteq \mathrm{NEXP}$$

More Merlins = More power?



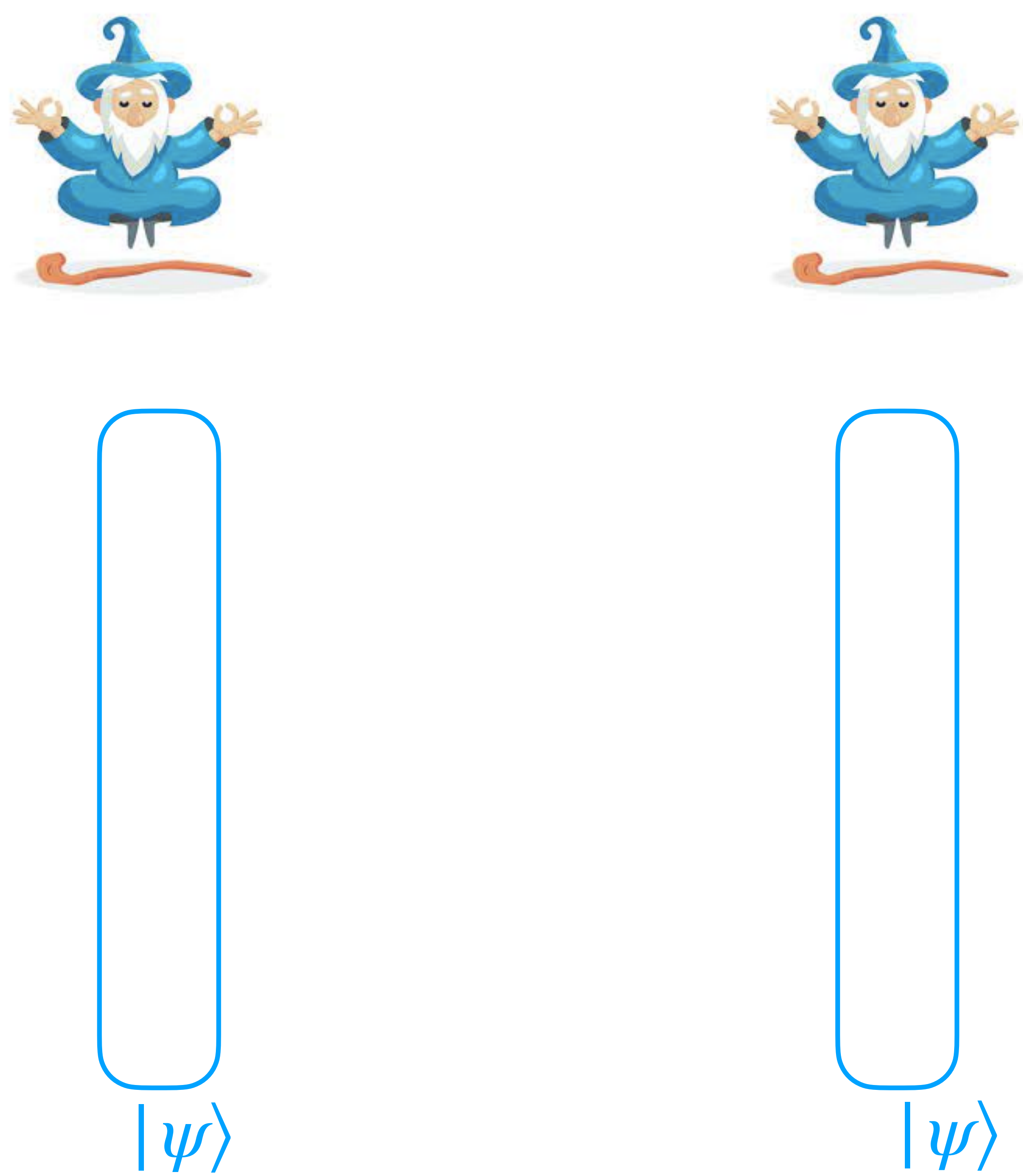
More Merlins = More power?

Product test [Harrow-Montanaro 10]

Given (copies of) pure state $|\psi\rangle \in H_1 \otimes \cdots \otimes H_k$, is it a product state, i.e. $|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots |\phi_k\rangle$?

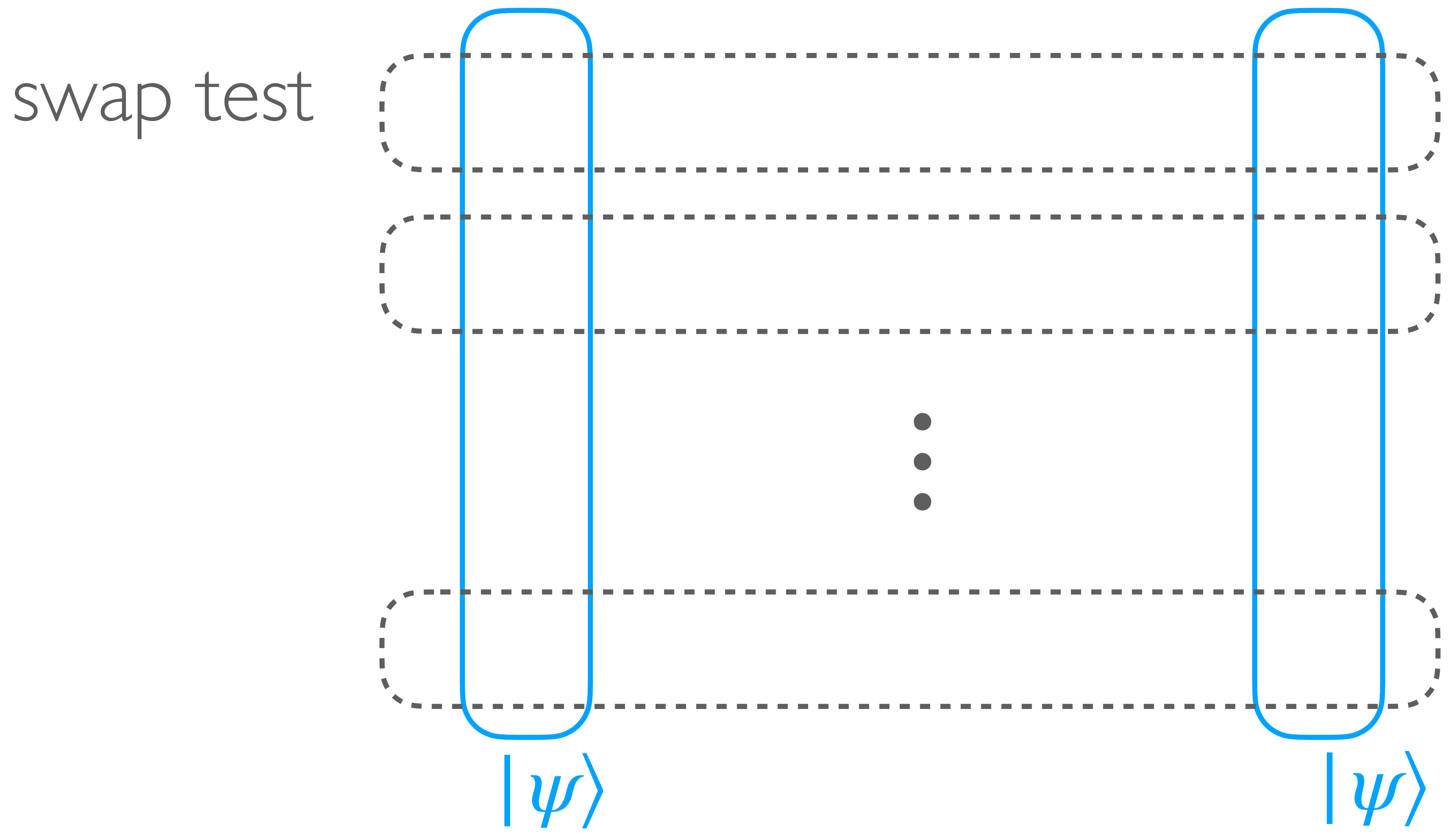
More Merlins = More power?

Product test [Harrow-Montanaro 10]



More Merlins = More power?

Product test [Harrow-Montanaro 10]



More Merlins = More power?

Theorem. (Harrow-Montanaro 10)

Suppose $\max_{\text{product state } \phi} |\langle \psi, \phi \rangle|^2 = 1 - \epsilon < 1$,

Then $|\psi\rangle$ pass product test w.p. $\leq 1 - \Theta(\epsilon)$.

Cor. $\mathrm{QMA}_m(k) \subseteq \mathrm{QMA}_{km}(2)$**.**

Pf. Let the 2 provers simulate k provers.

Apply one of the following test

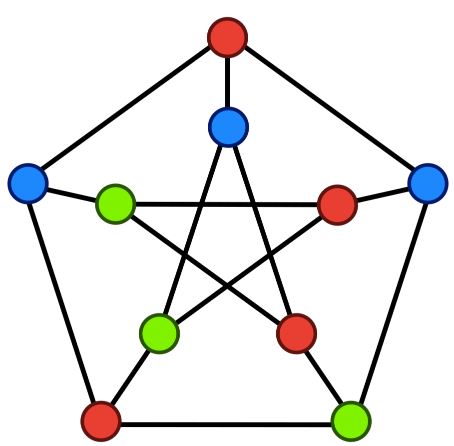
- product test
- the verification V on one proof

Blier-Tapp's QMA(2) *protocol for 3COL*

Blier-Tapp's QMA(2) *protocol for 3COL*

Merlin: (faithful)

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

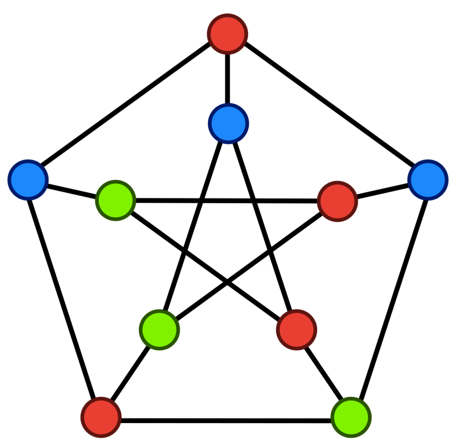


a 3 coloring instance

Blier-Tapp's QMA(2) *protocol for 3COL*

Merlin: (faithful)

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



a 3 coloring instance

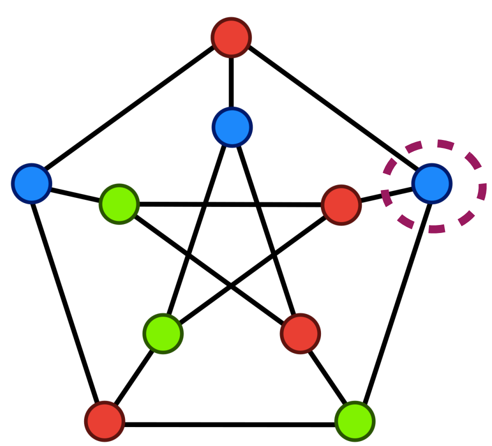
Arthur: (receives $|\psi_1\rangle, |\psi_2\rangle$)

- check equality
- make measurements
  - if same vertex observed, consistent color
  - if adjacent vertices observed, distinct colors

Blier-Tapp's QMA(2) *protocol for 3COL*

Merlin: (faithful)

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



a 3 coloring instance

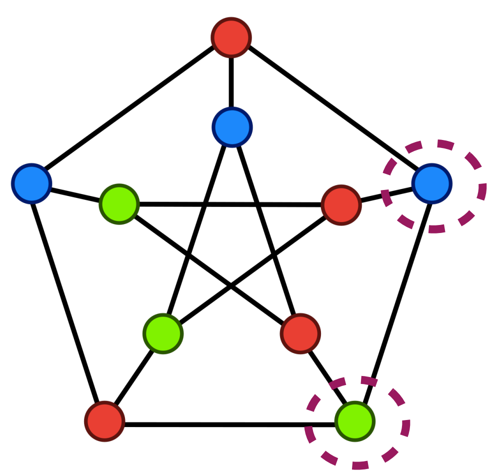
Arthur: (receives $|\psi_1\rangle, |\psi_2\rangle$)

- check equality
- make measurements
    - if same vertex observed, consistent color
    - if adjacent vertices observed, distinct colors

Blier-Tapp's QMA(2) *protocol for 3COL*

Merlin: (faithful)

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



a 3 coloring instance

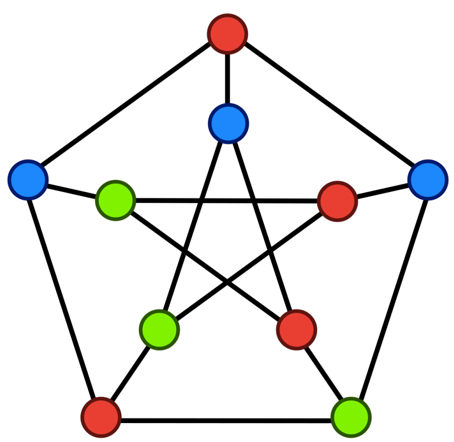
Arthur: (receives $|\psi_1\rangle, |\psi_2\rangle$)

- check equality
- make measurements
  - if same vertex observed, consistent color
  - if adjacent vertices observed, distinct colors

Blier-Tapp's QMA(2) *protocol for 3COL*

Merlin: (faithful)

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



a 3 coloring instance

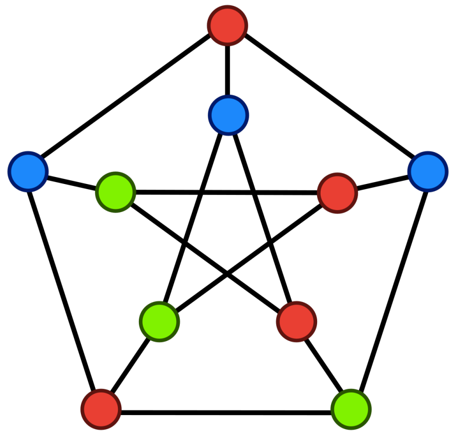
Arthur: (receives $|\psi_1\rangle, |\psi_2\rangle$)

- check equality
- make measurements
  - if same vertex observed, consistent color
  - if adjacent vertices observed, distinct colors
- "all present"

Blier-Tapp's QMA(2) *protocol for 3COL*

Merlin: (faithful)

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



a 3 coloring instance

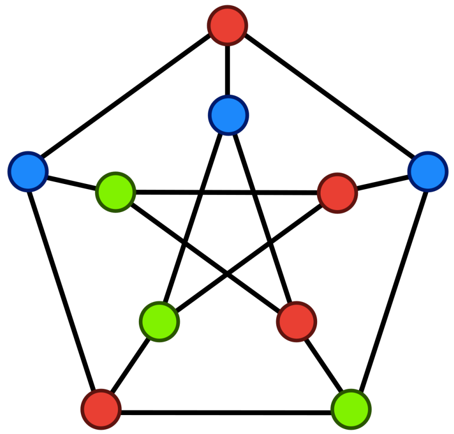
Arthur: (receives $|\psi_1\rangle, |\psi_2\rangle$)

- check equality
- make measurements
  - if same vertex observed, consistent color
  - if adjacent vertices observed, distinct colors
- "all present"
  1. already, $|\psi\rangle \approx \sum_{i \in [n]} \alpha_i |i\rangle |c_i\rangle$
  2. compare with $\sum_{i \in [n]} |i\rangle$

Blier-Tapp's QMA(2) *protocol for 3COL*

Merlin: (faithful)

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



Theorem.
$\mathrm{NP} \subseteq \mathrm{QMA}_{\log}(2)$ with a
a 1 v.s. $1 - 1/\mathrm{poly}(n)$ gap.

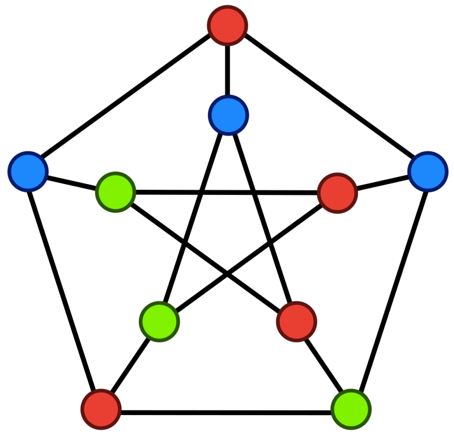
Arthur: (receives $|\psi_1\rangle, |\psi_2\rangle$)

- check equality
- make measurements
  - if same vertex observed, consistent color
  - if adjacent vertices observed, distinct colors
- "all present"
  1. already, $|\psi\rangle \approx \sum_{i\in[n]} \alpha_i |i\rangle |c_i\rangle$
  2. compare with $\sum_{i\in[n]} |i\rangle$

Blier-Tapp's QMA(2) *protocol for 3COL*

Merlin: (faithful)

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



Theorem.
NP $\subseteq$ $\mathrm{QMA_{log}}(2)$ with a
a 1 v.s. $1 - 1/\mathrm{poly}(n)$ gap.

not ideal

Arthur: (receives $|\psi_1\rangle, |\psi_2\rangle$)

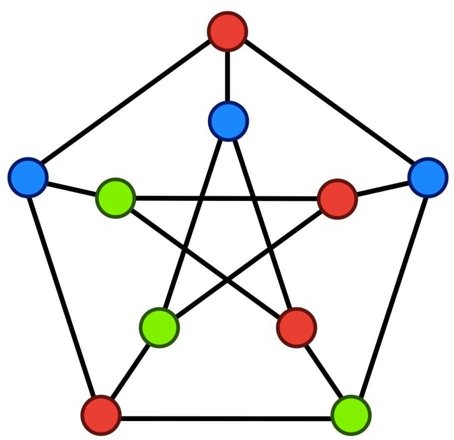
- check equality
- make measurements
  - if same vertex observed, consistent color
  - if adjacent vertices observed, distinct colors
- "all present"

1. already, $|\psi\rangle \approx \sum_{i\in[n]} \alpha_i |i\rangle |c_i\rangle$
2. compare with $\sum_{i\in[n]} |i\rangle$

Blier-Tapp's QMA(2) *protocol for 3COL*

Merlin: (faithful)

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



Theorem.
NP $\subseteq$ QMA$_{\log}$(2) with a
a 1 v.s. $1 - 1/\text{poly}(n)$ gap.

not ideal

Arthur: (receives $|\psi_1\rangle, |\psi_2\rangle$)

- check equality
- make measurements
  - if same vertex observed, consistent color
  - if adjacent vertices observed, distinct colors

local

- "all present"

1. already, $|\psi\rangle \approx \sum_{i \in [n]} \alpha_i |i\rangle|c_i\rangle$
2. compare with $\sum_{i \in [n]} |i\rangle$

Non-negative amplitudes

Roadmap: *Global* protocols for

with a *constant* gap.

Non-negative amplitudes

Roadmap: *Global* protocols for

- Small-set expansion problem
- Unique games problem
- Constraint satisfaction problem

with a *constant* gap.

Non-negative amplitudes

Roadmap: *Global* protocols for

- Small-set expansion problem
- Unique games problem
- Constraint satisfaction problem

} "expansion, robustness" +non-negativity

with a *constant* gap.

Non-negative amplitudes

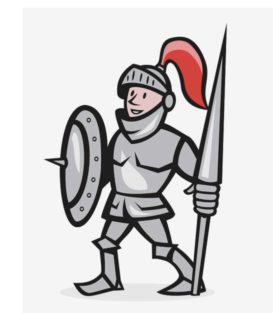
Roadmap: *Global* protocols for

- **Small-set expansion problem**
- Unique games problem
- Constraint satisfaction problem

with a *constant* gap.

Quantum Merlin-Arthur (QMA$^+$)

$|\psi\rangle$



$\Pi Q|\psi\rangle|0\rangle$

$$|\psi\rangle = \sum_i \alpha_i |i\rangle, \quad \alpha_i \geq 0$$

Quantum Merlin-Arthur (QMA^+)

$|\psi\rangle$

$\Pi Q|\psi\rangle|0\rangle$

$$|\psi\rangle = \sum_i \alpha_i |i\rangle, \quad \alpha_i \geq 0$$

(Completeness) "∃ a valid coloring":

benign Merlins will convince Arthur w.p. $\geq c$

(Soundness) "∄ valid coloring":

no adversarial Merlins can fool Arthur w.p. $\leq s$

the **gap** is $c - s = \Omega(1)$.

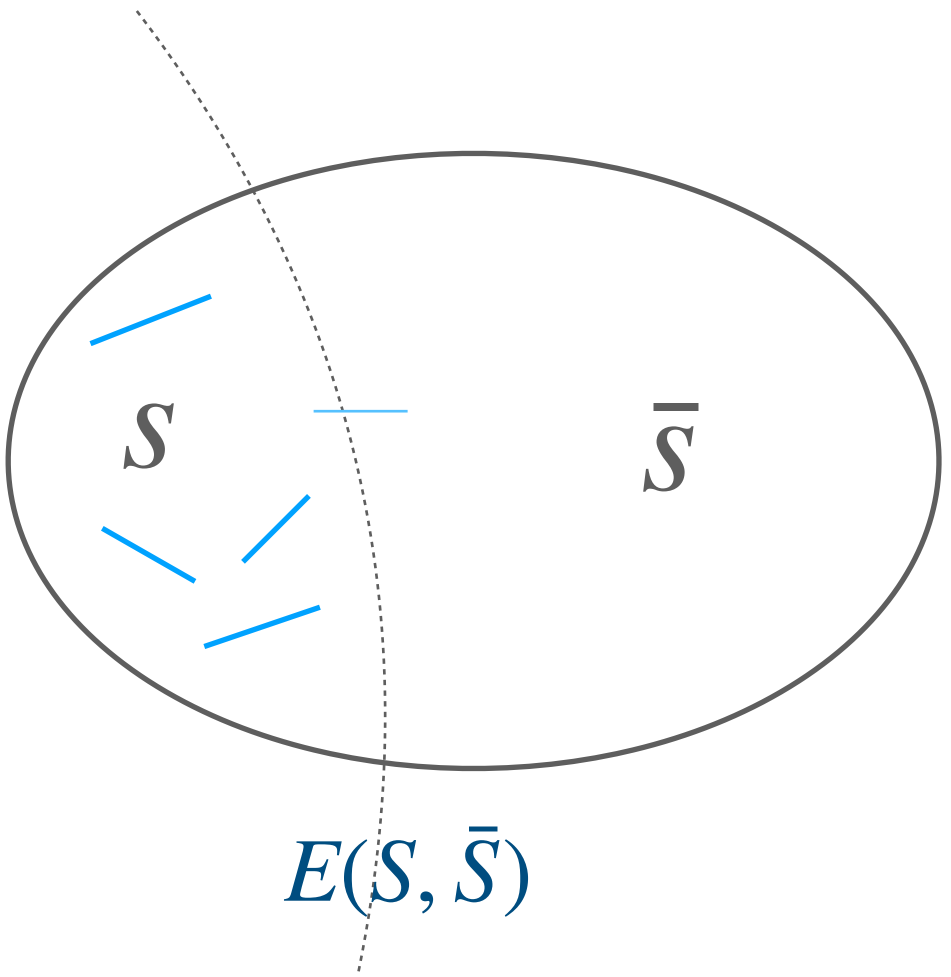
Small-set expansion (SSE) problem

Def. Small-Set Expansion

d-regular graph G,

(**yes**): exists S, $|S| \leq \delta n$,

$$\frac{|E(S,\bar{S})|}{d|S|} \approx 0.$$



Small-set expansion (SSE) problem

Def. Small-Set Expansion

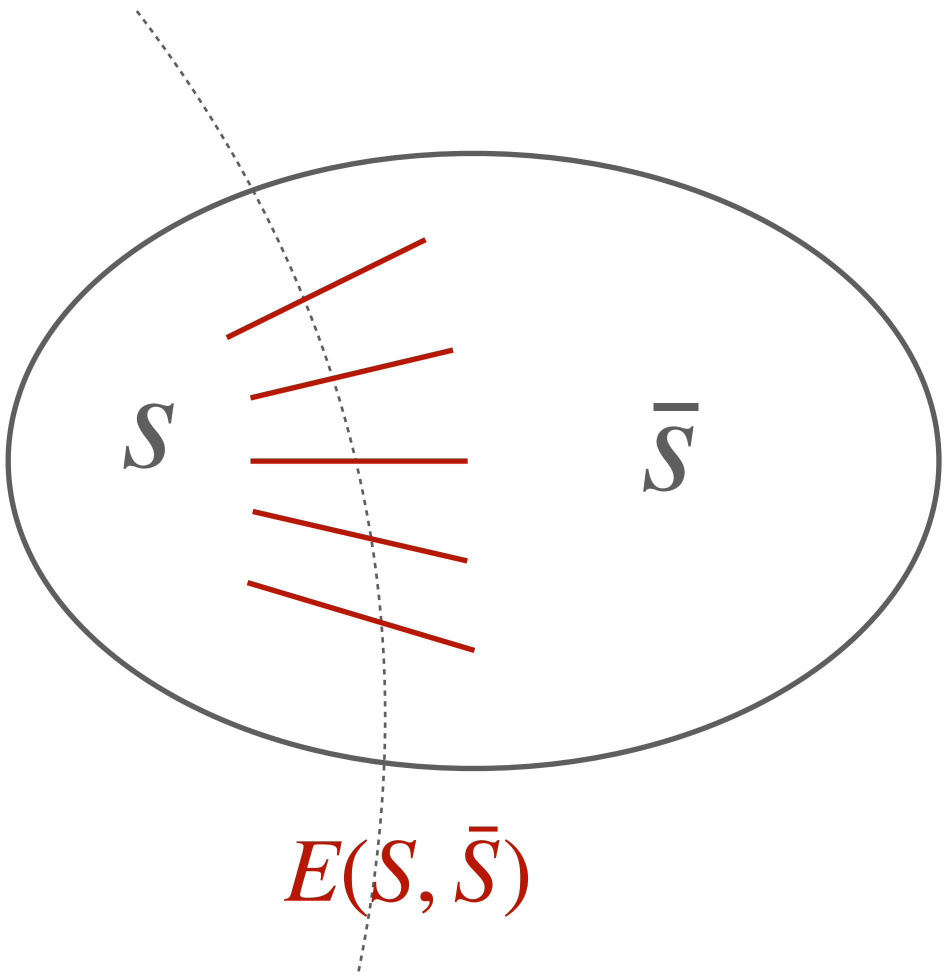
d-regular graph G,

(yes): exists S, $|S| \le \delta n$,

$$\frac{|E(S,\bar{S})|}{d|S|} \approx 0.$$

(no): for all S, $|S| \le \delta n$,

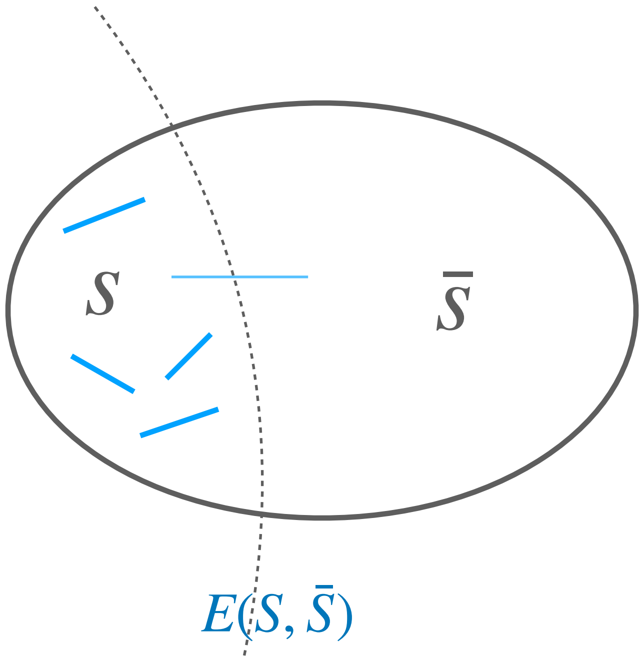
$$\frac{|E(S,\bar{S})|}{d|S|} \approx 1.$$



A QMA$^+$(2) *protocol for SSE*

Merlin: (faithful in yes case)

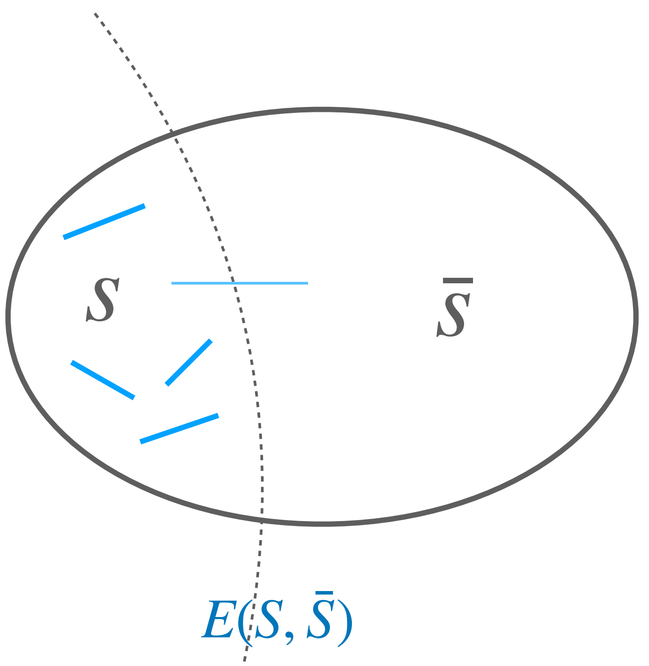
$$|\psi\rangle = \frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle$$



A $\text{QMA}^+(2)$ *protocol for SSE*

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle$$



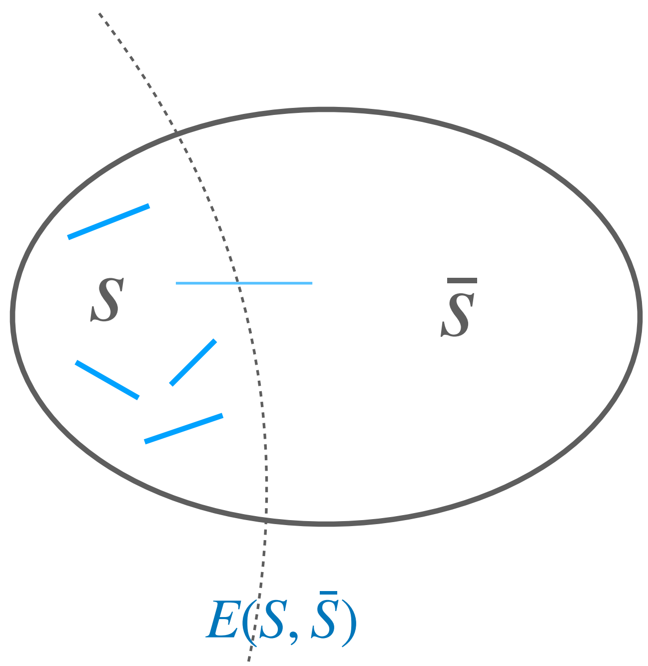
Arthur: (receives many $|\psi\rangle$)

- check equality

A $\mathrm{QMA}^+(2)$ *protocol for SSE*

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle$$

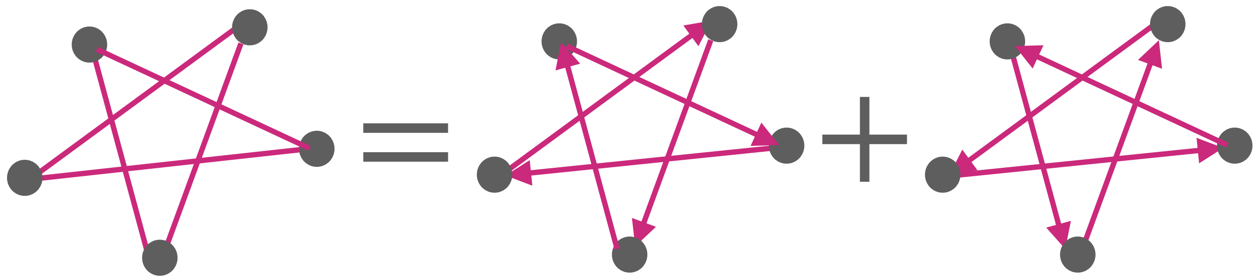


Arthur: (receives many $|\psi\rangle$)

- check equality

Fact. d-regular graph G, can be seen as d permutations

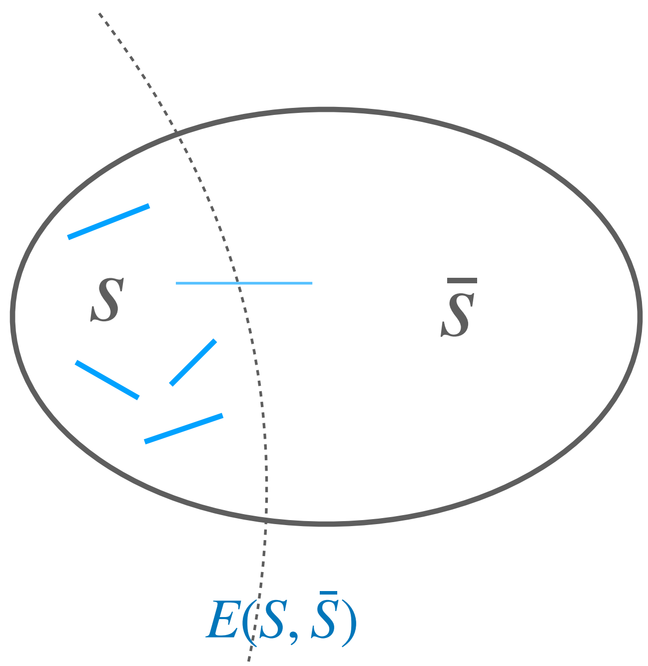
$$A_G = \sum_{r \in [d]} M_r.$$



A QMA$^+$(2) *protocol for SSE*

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle$$

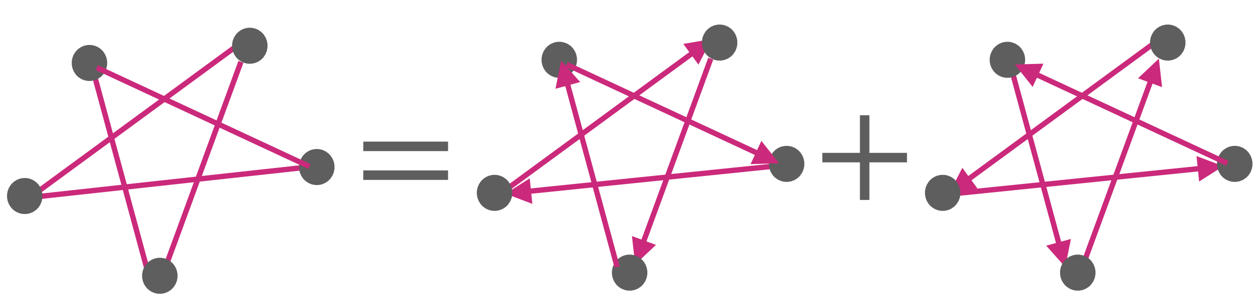


Arthur: (receives many $|\psi\rangle$)

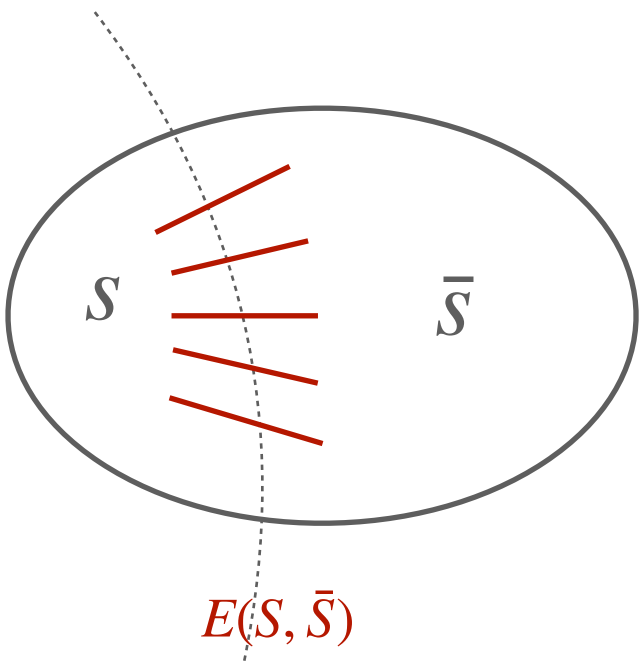
- check equality
- take a random M_r, apply it to $|\psi\rangle$; compare $M_r|\psi\rangle$ with $|\psi\rangle$

Fact. d-regular graph G, can be seen as d permutations

$$A_G = \sum_{r \in [d]} M_r.$$



A QMA$^+$(2) *protocol for SSE*



Merlin: (faithful in yes case)

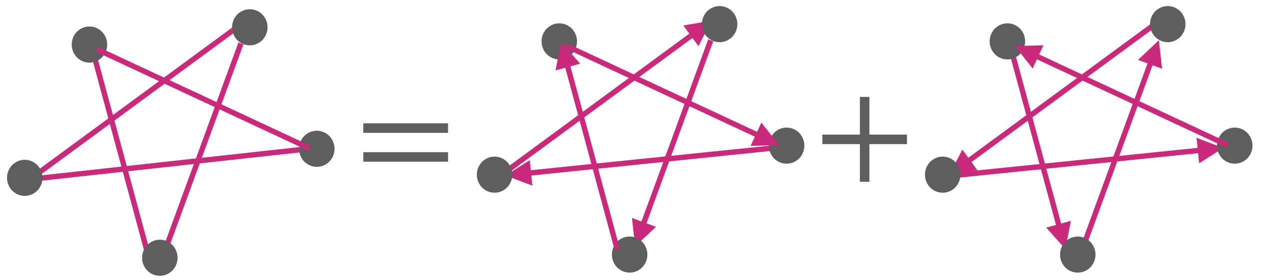
$$|\psi\rangle = \frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle$$

Arthur: (receives many $|\psi\rangle$)

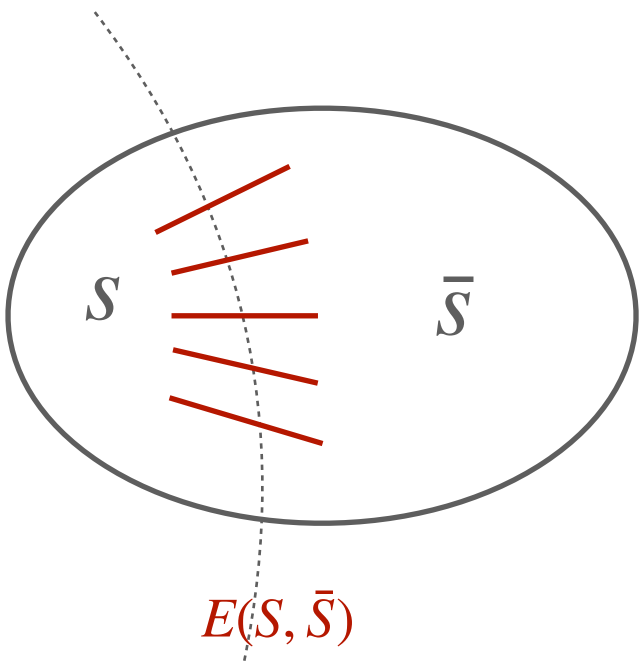
- check equality
- take a random M_r, apply it to $|\psi\rangle$; compare $M_r|\psi\rangle$ with $|\psi\rangle$

Fact. d-regular graph G, can be seen as d permutations

$$A_G = \sum_{r \in [d]} M_r.$$



A QMA$^+$(2) *protocol for SSE*



Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle$$

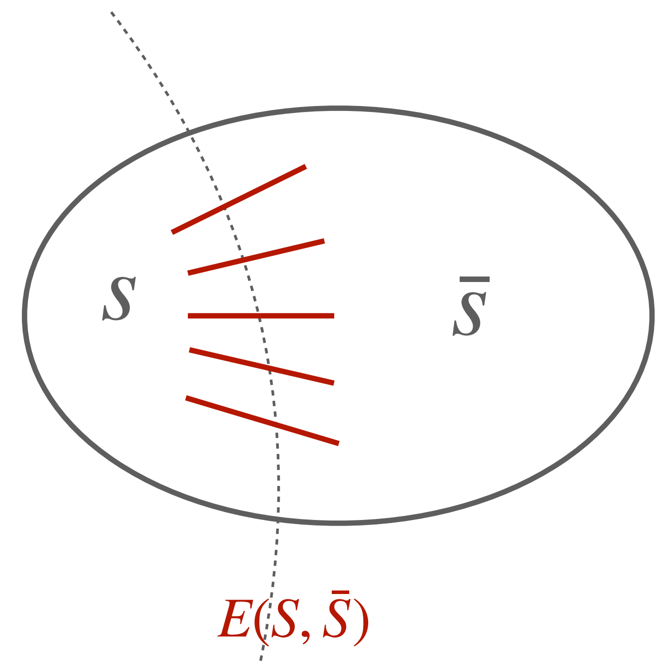
Arthur: (receives many $|\psi\rangle$)

- check equality
- take a random M_r, apply it to $|\psi\rangle$; compare $M_r|\psi\rangle$ with $|\psi\rangle$
- sparsity test

A $\text{QMA}^+(2)$ *protocol for SSE*

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle$$



Arthur: (receives many $|\psi\rangle$)

- check equality
- take a random M_r, apply it to $|\psi\rangle$; compare $M_r|\psi\rangle$ with $|\psi\rangle$
- sparsity test

Theorem 1.
$\text{SSE} \in \text{QMA}^+_{\log}(2)$, with a $\Omega(1)$ gap

Sparsity Test

Goal: test if $|\psi\rangle$ is a uniform superposition of an arbitrary subset S of $[n]$ (of size δn for some given const δ.)

$$|\psi\rangle = \frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle .$$

Sparsity Test

Protocol:

Let $|\mu\rangle = \frac{1}{\sqrt{n}} \sum_i |i\rangle$.

- Ask for many copies of (expected form)

  $$|\psi\rangle = \frac{1}{\sqrt{|S|}} \sum_{i\in S} |i\rangle, \qquad |\psi^C\rangle = \frac{1}{\sqrt{n-|S|}} \sum_{i\notin S} |i\rangle .$$

- Estimate

  $\tilde{\alpha} = \langle\psi|\psi^C\rangle^2$, $\tilde{\delta} = \langle\psi|\mu\rangle^2$, $\tilde{\beta} = \langle\psi^C|\mu\rangle^2$.

ACCEPT if $\tilde{\alpha} \approx 0$, $\tilde{\delta} + \tilde{\beta} \approx 1$

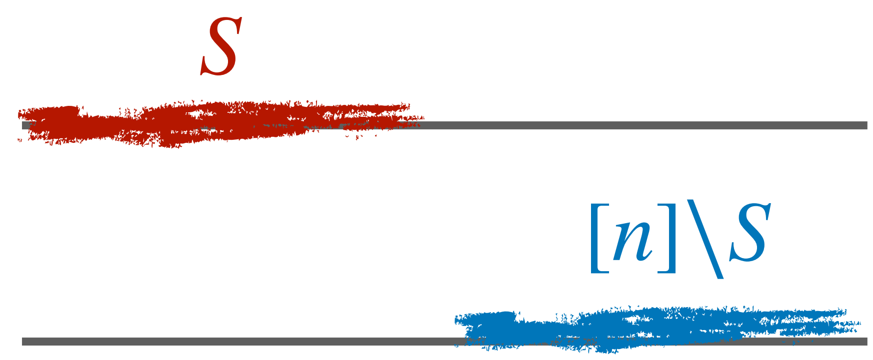
Sparsity Test

Lemma. If $|\psi\rangle$ passes sparsity test, $|\psi\rangle \approx$ a subset state

Pf. If $\langle\psi|\psi^C\rangle \approx 0$

$|\psi\rangle$

$|\psi^C\rangle$



Sparsity Test

Lemma. If $|\psi\rangle$ passes sparsity test, $|\psi\rangle \approx$ a subset state

Pf. If $\langle\psi|\psi^C\rangle \approx 0$ non-negativity

Sparsity Test

Lemma. If $|\psi\rangle$ passes sparsity test, $|\psi\rangle \approx$ a subset state

non-negativity

Pf. If $\langle\psi|\psi^C\rangle \approx 0$

By Cauchy-Schwarz,

$$\langle\psi|\mu\rangle^2 \leq \frac{|S|}{n}, \qquad \langle\psi^C|\mu\rangle^2 \leq 1 - \frac{|S|}{n},$$

equality holds when $|\psi\rangle$ is the uniform superposition over S.

Roadmap: *Global, coherent* protocols for

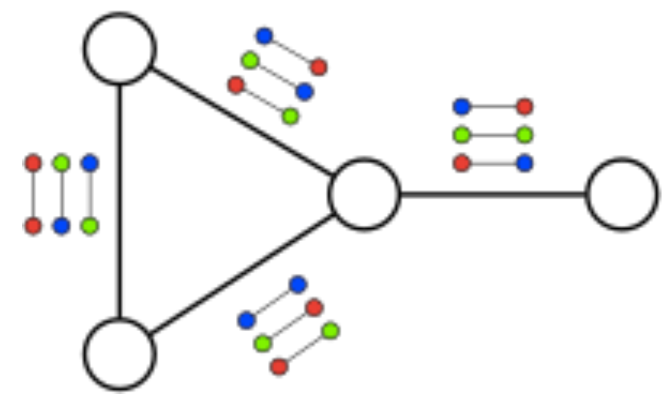
- Small-set expansion problem
- **Unique games problem**
- Constraints satisfiability problem

with a *constant* gap.

Unique games

(d-regular graph) G, for each edge e, bijection $f_{(u,v)} : \Sigma \rightarrow \Sigma$.

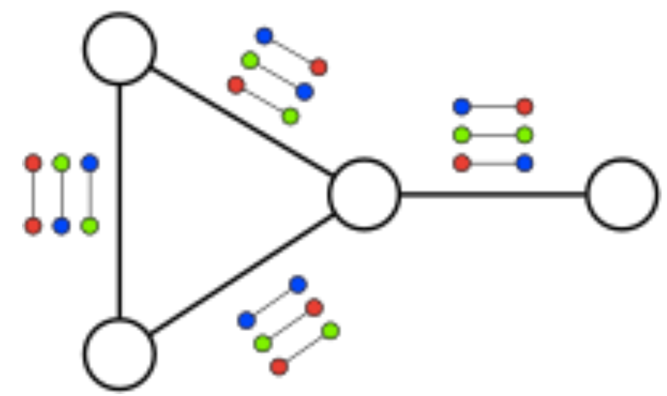
$$\text{val}(G) = \max_{\ell} \mathbf{E}_{(u,v)\in G}[\mathbf{1}_{f_{(u,v)}(\ell(u))=\ell(v)}]$$



Unique games

(d-regular graph) G, for each edge e, bijection $f_{(u,v)} : \Sigma \to \Sigma$.

$$\text{val}(G) = \max_{\ell} \mathbf{E}_{(u,v)\in G}[\mathbf{1}_{f_{(u,v)}(\ell(u))=\ell(v)}]$$



Def. $(1-\eta, \gamma)$**-UG**

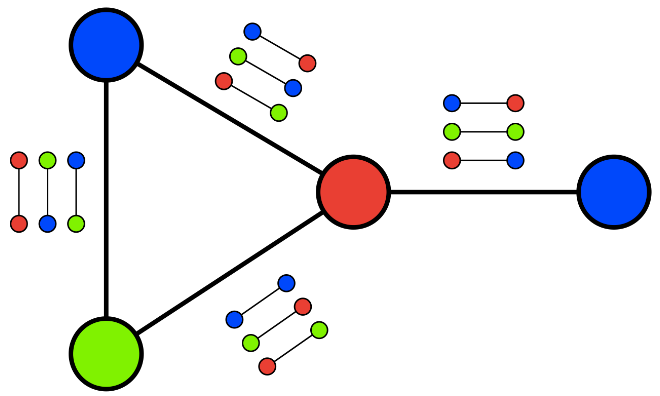
(yes): $\text{val}(G) \geq 1 - \eta$

(no): $\text{val}(G) \leq \gamma$

A QMA$^+$(2) *protocol for UG*

Merlin: (faithful in yes case)

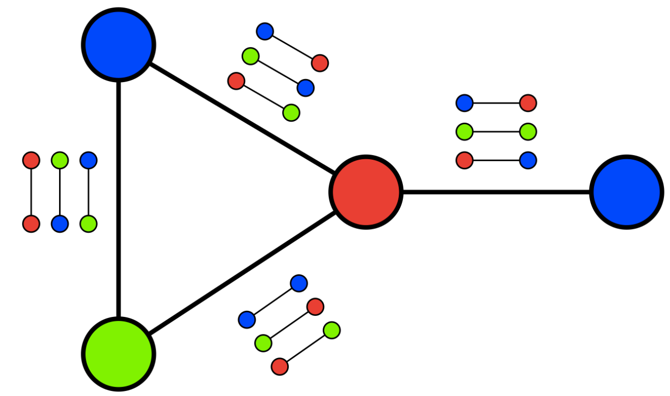
$$|\psi\rangle = \sum_{v \in G} |v\rangle |\ell(v)\rangle$$



A QMA$^+$(2) *protocol for UG*

Merlin: (faithful in yes case)

$$|\psi\rangle = \sum_{v \in G} |v\rangle |\ell(v)\rangle$$



Arthur: (receives copies of $|\psi\rangle$)

- check equality
- take a random M_r, e.g. (u, v) is an edge in M_r,

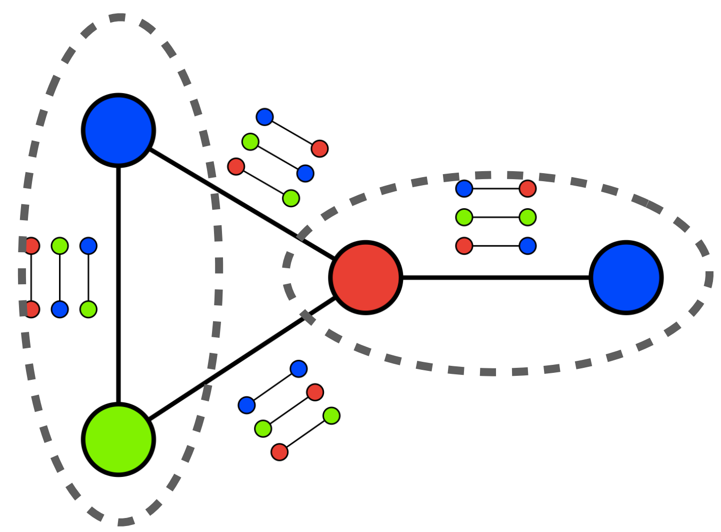
$$\mathcal{T}_r : |u\rangle|\ell\rangle \mapsto |v\rangle|f_{(u,v)}(\ell)\rangle$$

compare $\mathcal{T}_r|\psi\rangle$ and $|\psi\rangle$

A $\mathrm{QMA}^{+}(2)$ *protocol for UG*

Merlin: (faithful in yes case)

$$|\psi\rangle = \sum_{v \in G} |v\rangle |\ell(v)\rangle$$



Arthur: (receives copies of $|\psi\rangle$)

- check equality
- take a random M_r, e.g. (u, v) is an edge in M_r,

  $\mathcal{T}_r : |u\rangle |\ell\rangle \mapsto |v\rangle |f_{(u,v)}(\ell)\rangle$

  compare $\mathcal{T}_r |\psi\rangle$ and $|\psi\rangle$

A QMA$^+$(2) *protocol for UG*

Merlin: (faithful in yes case)

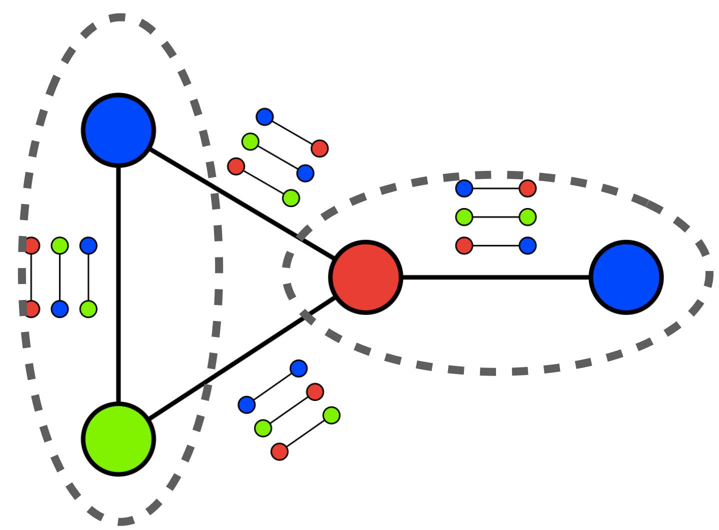
$$|\psi\rangle = \sum_{v \in G} |v\rangle |\ell(v)\rangle$$

Arthur: (receives copies of $|\psi\rangle$)

- check equality
- take a random M_r, e.g. (u, v) is an edge in M_r,

$$\mathscr{T}_r : |u\rangle|\ell\rangle \mapsto |v\rangle|f_{(u,v)}(\ell)\rangle$$

compare $\mathscr{T}_r|\psi\rangle$ and $|\psi\rangle$



ASSUME $|\psi\rangle$ encodes a valid assignment, then:
In the yes case, $\mathscr{T}_r|\psi\rangle \approx |\psi\rangle$;
In the no case, $\mathscr{T}_r|\psi\rangle \perp |\psi\rangle$

A $\mathrm{QMA}^+(2)$ *protocol for UG*

Merlin: (faithful in yes case)

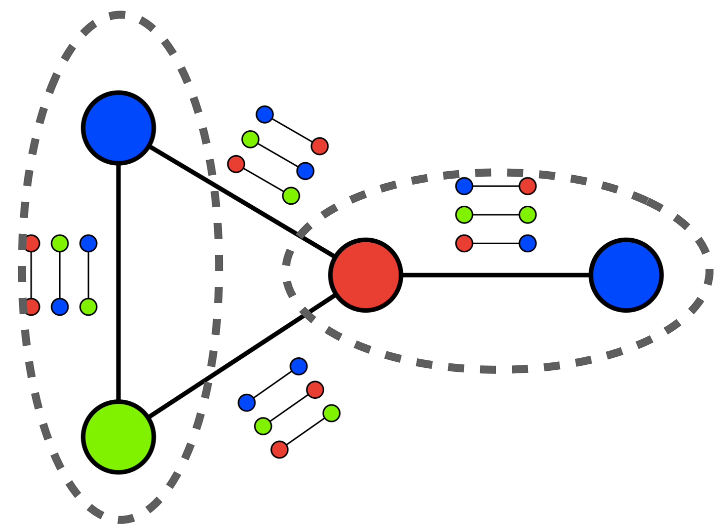
$$|\psi\rangle = \sum_{v \in G} |v\rangle |\ell(v)\rangle$$

Arthur: (receives copies of $|\psi\rangle$)

- check equality
- take a random M_r, e.g. (u, v) is an edge in M_r,

  $$\mathcal{T}_r : |u\rangle|\ell\rangle \mapsto |v\rangle|f_{(u,v)}(\ell)\rangle$$

  compare $\mathcal{T}_r|\psi\rangle$ and $|\psi\rangle$
- validity test



A QMA$^+$(2) *protocol for UG*

Merlin: (faithful in yes case)

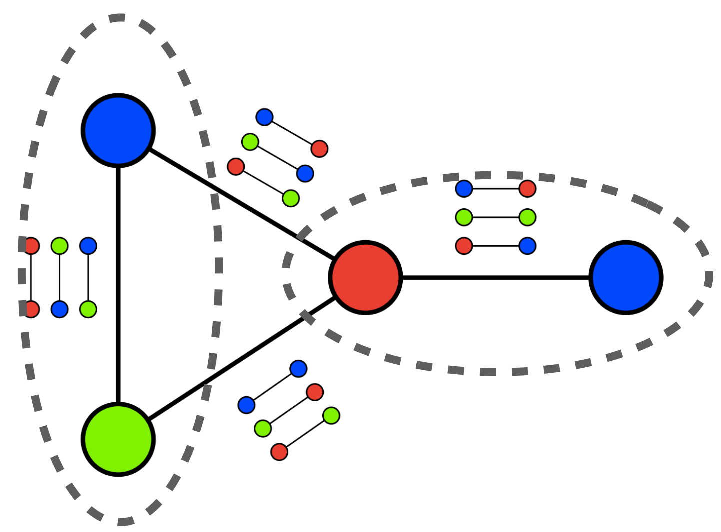
$$|\psi\rangle = \sum_{v \in G} |v\rangle |\ell(v)\rangle$$

Arthur: (receives copies of $|\psi\rangle$)

- check equality
- take a random M_r, e.g. (u, v) is an edge in M_r,

  $$\mathcal{T}_r : |u\rangle|\ell\rangle \mapsto |v\rangle|f_{(u,v)}(\ell)\rangle$$

  compare $\mathcal{T}_r|\psi\rangle$ and $|\psi\rangle$
- validity test



Theorem 2.
UG $\in$ QMA$^+_{\log}$(2), with a $\Omega(1)$ gap

A $\mathrm{QMA}^{+}(2)$ *protocol for UG*

Merlin: (faithful in yes case)

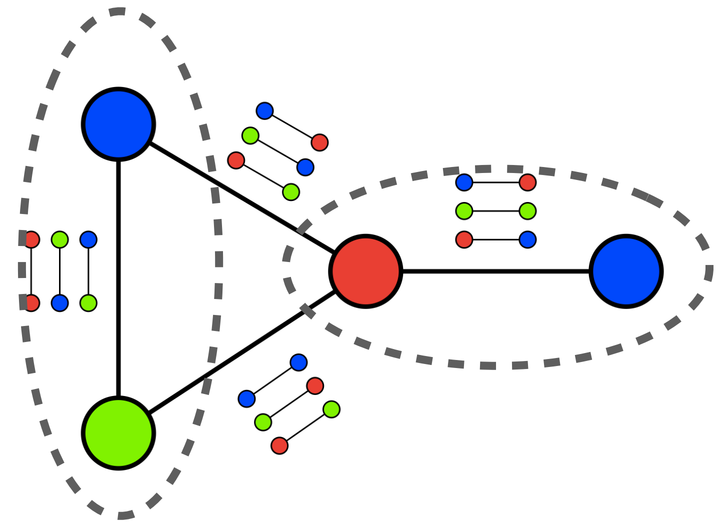
$$|\psi\rangle = \sum_{v \in G} |v\rangle |\ell(v)\rangle$$

Arthur: (receives copies of $|\psi\rangle$)

- check equality
- take a random M_r, e.g. (u, v) is an edge in M_r,

  $$\mathcal{T}_r : |u\rangle|\ell\rangle \mapsto |v\rangle|f_{(u,v)}(\ell)\rangle$$

  compare $\mathcal{T}_r|\psi\rangle$ and $|\psi\rangle$
- validity test



Theorem 2.
$\mathrm{UG} \in \mathrm{QMA}^{+}_{\log}(2)$, with a $\Omega(1)$ gap

Cor.
$\mathrm{NP} \subseteq \mathrm{QMA}^{+}_{\log}(2)$, with a $\Omega(1)$ gap

A $\mathrm{QMA}^+(2)$ *protocol for UG*

Merlin: (faithful in yes case)

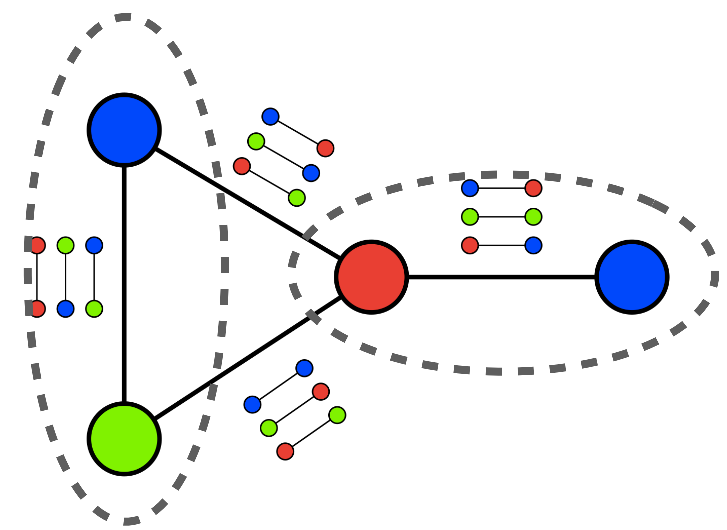
$$|\psi\rangle = \sum_{v \in G} |v\rangle |\ell(v)\rangle$$

Arthur: (receives copies of $|\psi\rangle$)

- check equality
- take a random M_r, e.g. (u, v) is an edge in M_r,

  $$\mathcal{T}_r : |u\rangle |\ell\rangle \mapsto |v\rangle |f_{(u,v)}(\ell)\rangle$$

  compare $\mathcal{T}_r|\psi\rangle$ and $|\psi\rangle$
- validity test



Theorem 2.
$\mathrm{UG} \in \mathrm{QMA}^+_{\log}(2)$, with a $\Omega(1)$ gap

Cor.
$\mathrm{NP} \subseteq \mathrm{QMA}^+_{\log}(2)$, with a $\Omega(1)$ gap

as $(1/2,\gamma)$-UG is NP-hard

Validity Test

Assume: n variables $x_i \in \Sigma$, where Σ is of constant size
Goal: test if

$$|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle |x_i\rangle .$$

(some valid assignment)

Validity Test

Protocol:

- Suppose $|\psi\rangle$ in addition with some $|\psi^C\rangle$ can pass sparsity test, furthermore $\langle\psi|\mu\rangle^2 \approx \frac{1}{|\Sigma|}$. Thus,

$$|\psi\rangle \approx \frac{1}{\sqrt{|S|}} \sum_{(i,x_i)\in S} |i\rangle|x_i\rangle .$$

Validity Test

Protocol:

- Suppose $|\psi\rangle$ in addition with some $|\psi^C\rangle$ can pass sparsity test, furthermore $\langle\psi|\mu\rangle^2 \approx \frac{1}{|\Sigma|}$. Thus,

$$|\psi\rangle \approx \frac{1}{\sqrt{|S|}} \sum_{(i,x_i)\in S} |i\rangle|x_i\rangle .$$

Need to make sure all is are present

Validity Test

Protocol:

- Suppose $|\psi\rangle$ in addition with some $|\psi^C\rangle$ can pass sparsity test, furthermore $\langle\psi|\mu\rangle^2 \approx \frac{1}{|\Sigma|}$. Thus,

$$|\psi\rangle \approx \frac{1}{\sqrt{|S|}} \sum_{(i,x_i)\in S} |i\rangle|x_i\rangle .$$

Need to make sure all is are present

- Apply Fourier transform to the second register, and measure it.

Validity Test

Protocol:

- Suppose $|\psi\rangle$ in addition with some $|\psi^C\rangle$ can pass sparsity test, furthermore $\langle\psi|\mu\rangle^2 \approx \frac{1}{|\Sigma|}$. Thus,

$$|\psi\rangle \approx \frac{1}{\sqrt{|S|}} \sum_{(i,x_i)\in S} |i\rangle|x_i\rangle \, .$$

Need to make sure all is are present

- Apply Fourier transform to the second register, and measure it.

ACCEPT if the probability p_0 of observe 0

$$p_0 < \frac{1}{|\Sigma|} + \epsilon \, .$$

Validity Test

Lemma. If $|\psi\rangle$ passes sparsity test & validity test,
$|\psi\rangle \approx$ encode a valid assignment.

Pf. Compare $|i\rangle|x_i\rangle$ v.s. $\sum_{j=1}^{k} \frac{1}{\sqrt{k}} |i\rangle|x_i^j\rangle$

Validity Test

Lemma. If $|\psi\rangle$ passes sparsity test & validity test, $|\psi\rangle \approx$ encode a valid assignment.

Pf. Compare $|i\rangle|x_i\rangle$ v.s. $\sum_{j=1}^{k} \frac{1}{\sqrt{k}} |i\rangle|x_i^j\rangle$

↑

$$p_0 = \frac{1}{|\Sigma|}$$

Validity Test

Lemma. If $|\psi\rangle$ passes sparsity test & validity test, $|\psi\rangle \approx$ encode a valid assignment.

Pf. Compare $|i\rangle|x_i\rangle$ v.s. $\sum_{j=1}^{k} \frac{1}{\sqrt{k}} |i\rangle|x_i^j\rangle$

$$p_0 = \frac{1}{|\Sigma|} \qquad\qquad p_0 = \frac{k}{|\Sigma|}$$

Validity Test

Lemma. If $|\psi\rangle$ passes sparsity test & validity test, $|\psi\rangle \approx$ encode a valid assignment.

Pf. Compare $|i\rangle|x_i\rangle$ v.s. $\sum_{j=1}^{k} \frac{1}{\sqrt{k}} |i\rangle|x_i^j\rangle$

$$p_0 = \frac{1}{|\Sigma|} \qquad\qquad p_0 = \frac{k}{|\Sigma|}$$

Thus, if $|\psi\rangle$ is far from being valid, then prob. of observing 0 is $\gg 1/|\Sigma|$.

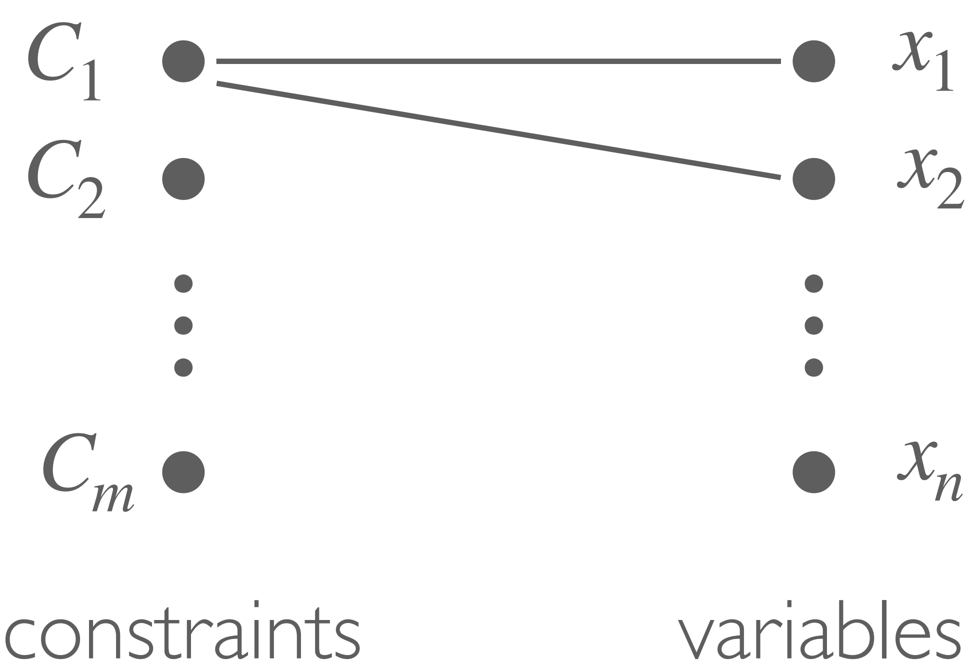
Roadmap: *Global* protocols for

- Small-set expansion problem
- Unique games problem
- **Constraint satisfaction problem**

with a *constant* gap.

Classical, NP-complete problems

A k-constraint satisfaction problem (CSP):

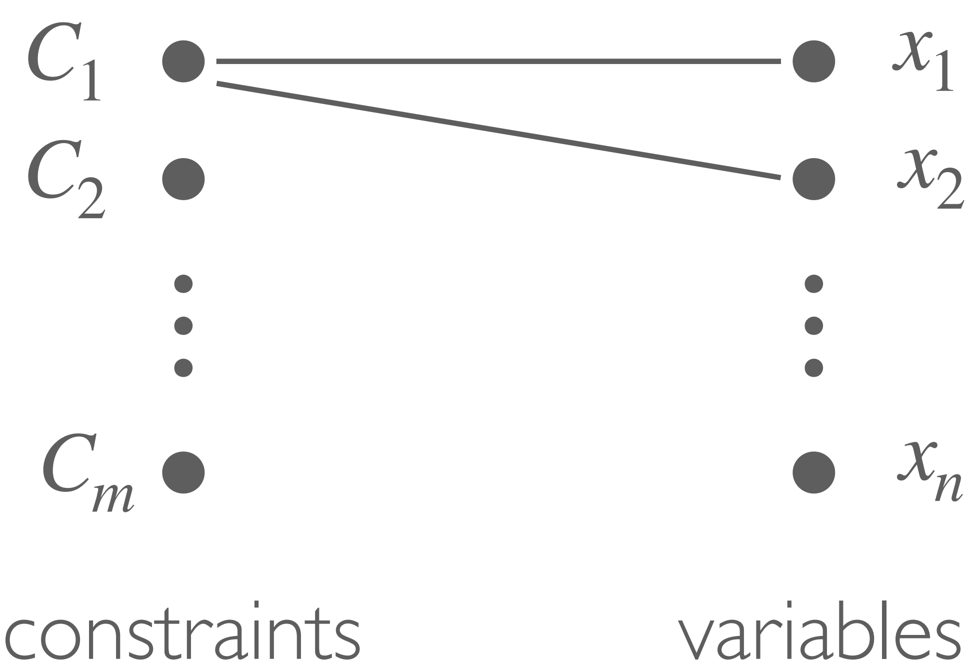


Each constraint $C_i(x_{i_1}, x_{i_2}, \ldots, x_{i_k})$

- depends on k variables
- *arbitrary* predicate
- $x_i \in \Sigma_i$, *constant* size alphabet

Classical, NP-complete problems

A k-constraint satisfaction problem (CSP):



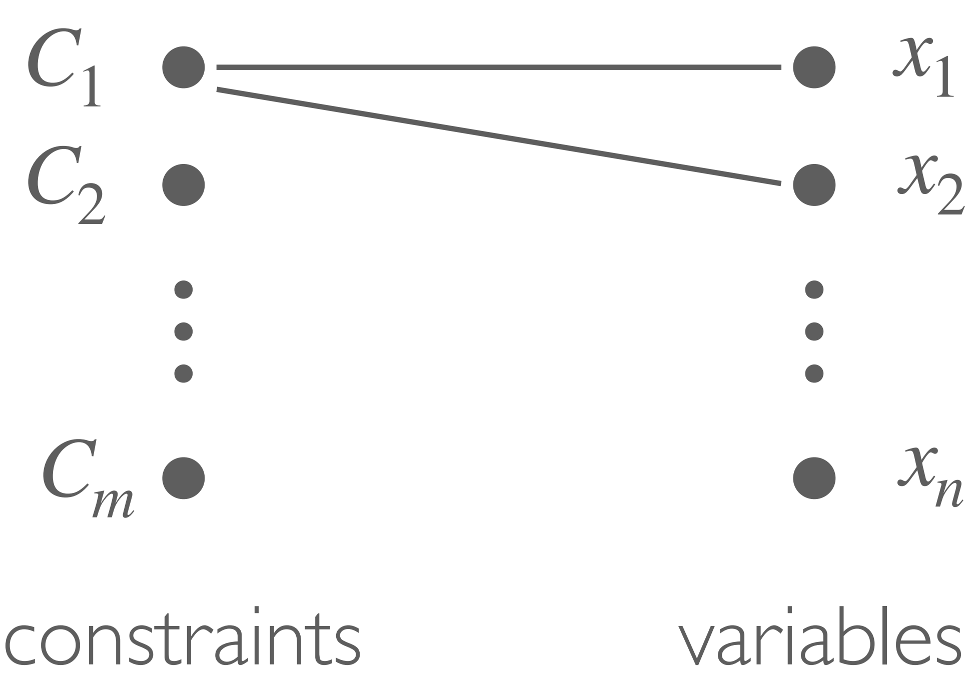
Question:
is there assignment that satisfies all constraints?

Each constraint $C_i(x_{i_1}, x_{i_2}, \ldots, x_{i_k})$

- depends on k variables
- *arbitrary* predicate
- $x_i \in \Sigma_i$, *constant* size alphabet

Classical, NP-complete problems

A k-constraint satisfaction problem (CSP):



Question:
is there assignment that satisfies all constraints?

distinguish whether 1 or $\leq \epsilon$

PCP theorem.

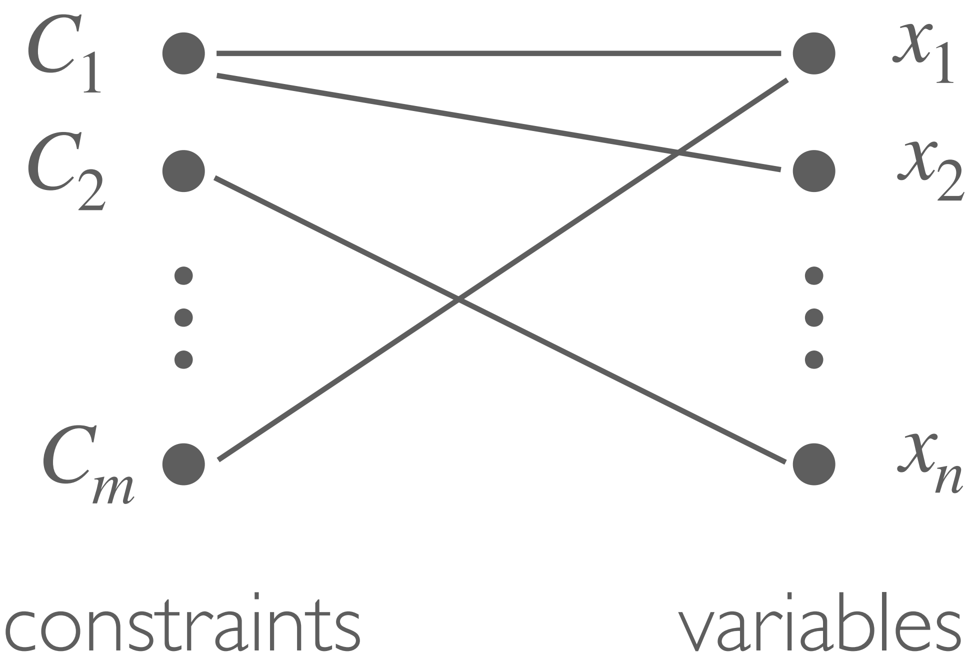
Each constraint $C_i(x_{i_1}, x_{i_2}, \ldots, x_{i_k})$

- depends on k variables
- *arbitrary* predicate
- $x_i \in \Sigma_i$, *constant* size alphabet

NP-complete k-CSP

A general k-CSP (PCP theorem)

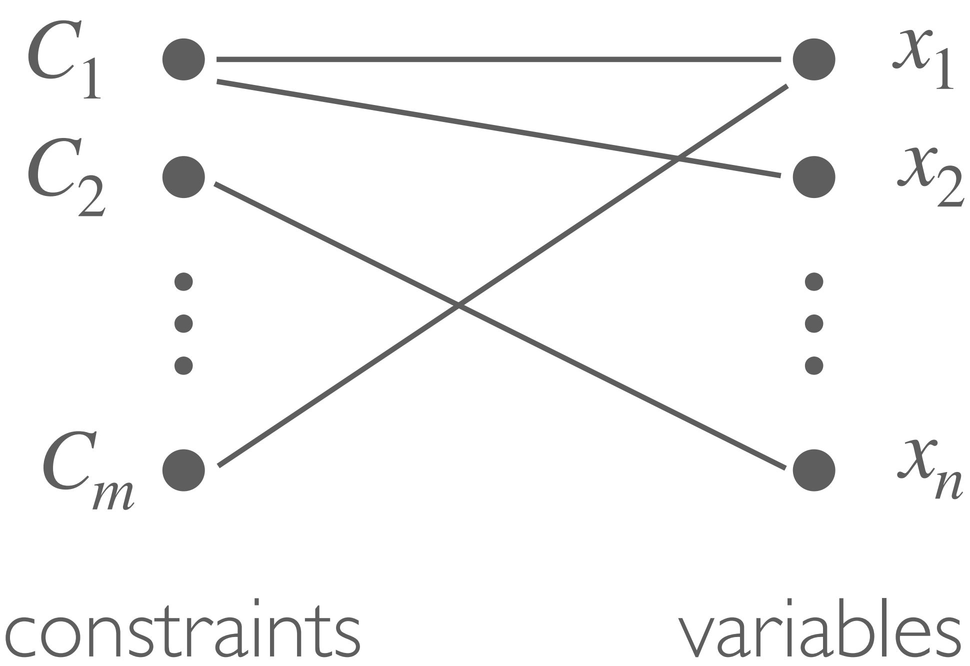
PCP 1 v.s. ϵ
NP-hard



$\mathrm{QMA}^+(2)$ *protocol for k-CSP*

Merlin: (faithful in yes case)

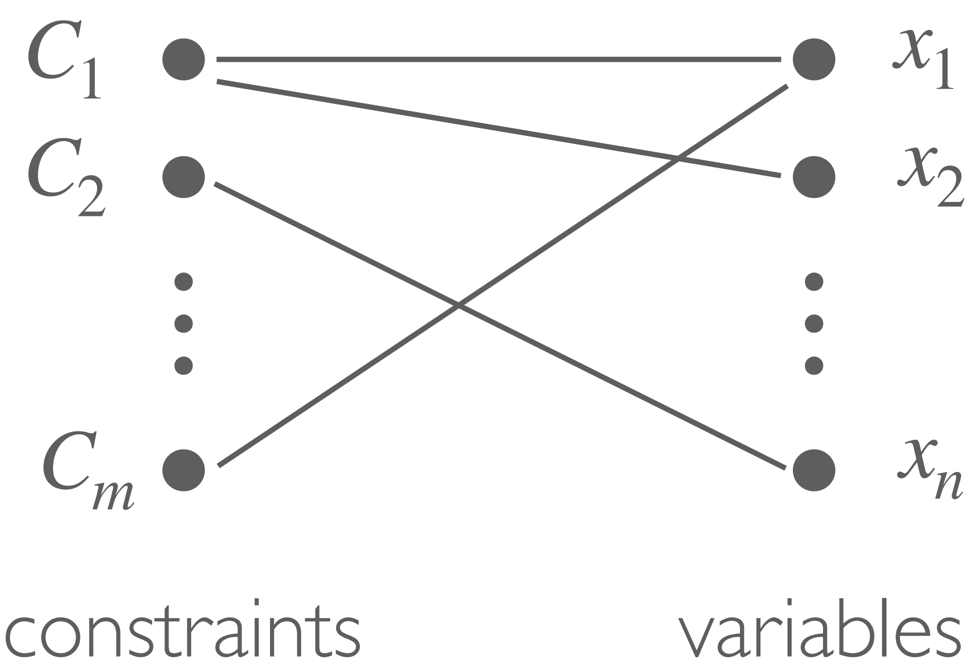
$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \dots v_{i,k}\rangle$$



$\mathrm{QMA}^+(2)$ *protocol for k-CSP*

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \ldots v_{i,k}\rangle$$



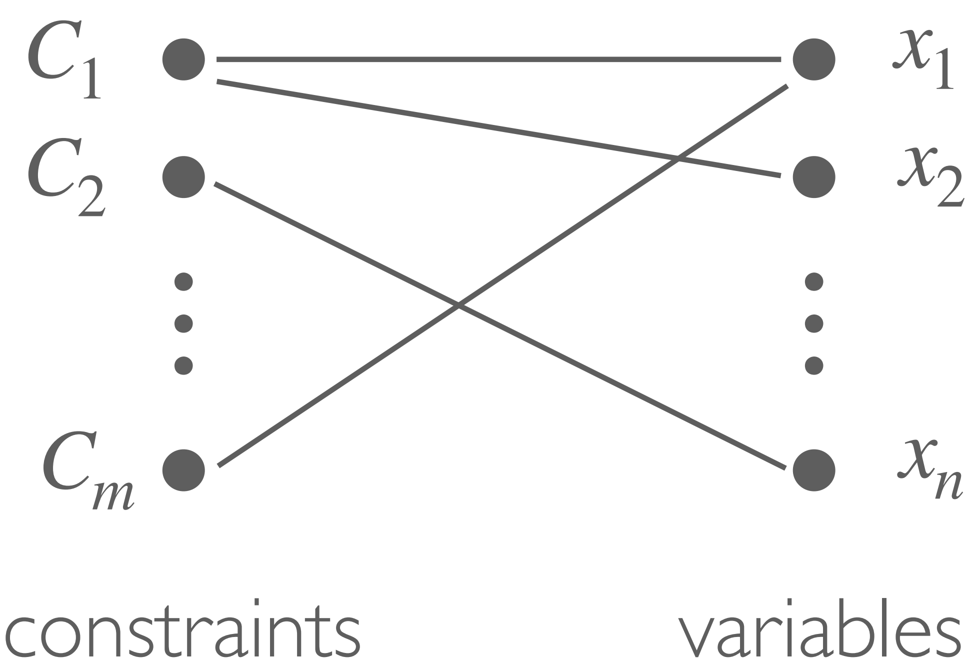
First, it's easy to verify the constraints,

$$|C_i\rangle |v_1 v_2 \ldots v_k\rangle |0\rangle \mapsto |C_i\rangle |v_1 v_2 \ldots v_k\rangle |C_i(v_1 v_2 \ldots v_k)\rangle.$$

$\text{QMA}^+(2)$ *protocol for k-CSP*

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \ldots v_{i,k}\rangle$$



First, it's easy to verify the constraints,

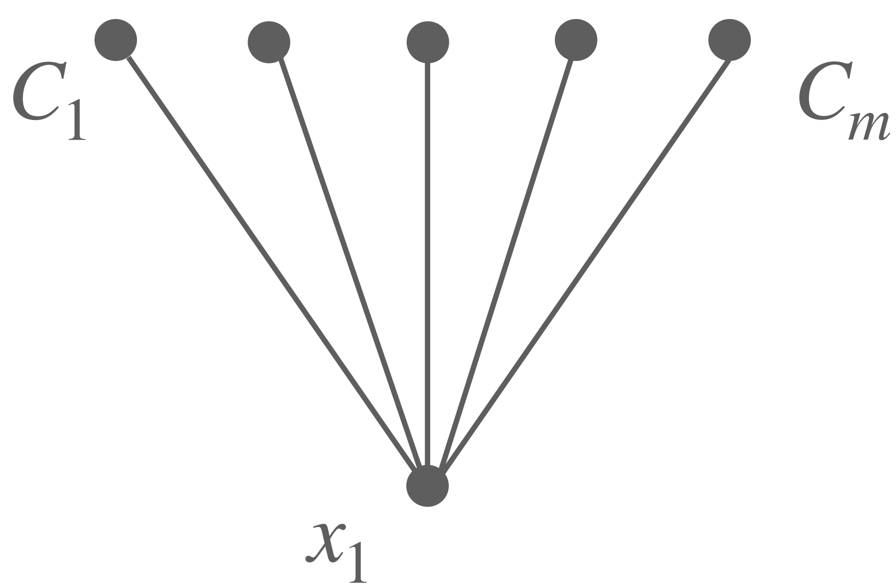
$$|C_i\rangle |v_1 v_2 \ldots v_k\rangle |0\rangle \mapsto |C_i\rangle |v_1 v_2 \ldots v_k\rangle |C_i(v_1 v_2 \ldots v_k)\rangle.$$

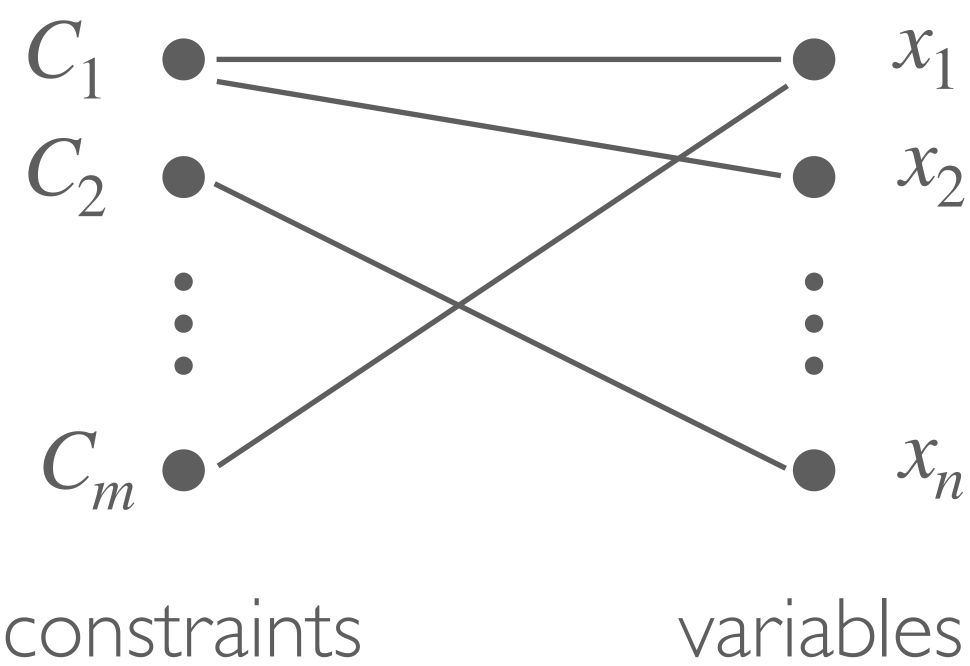
Consistency?

Regularization

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \ldots v_{i,k}\rangle$$

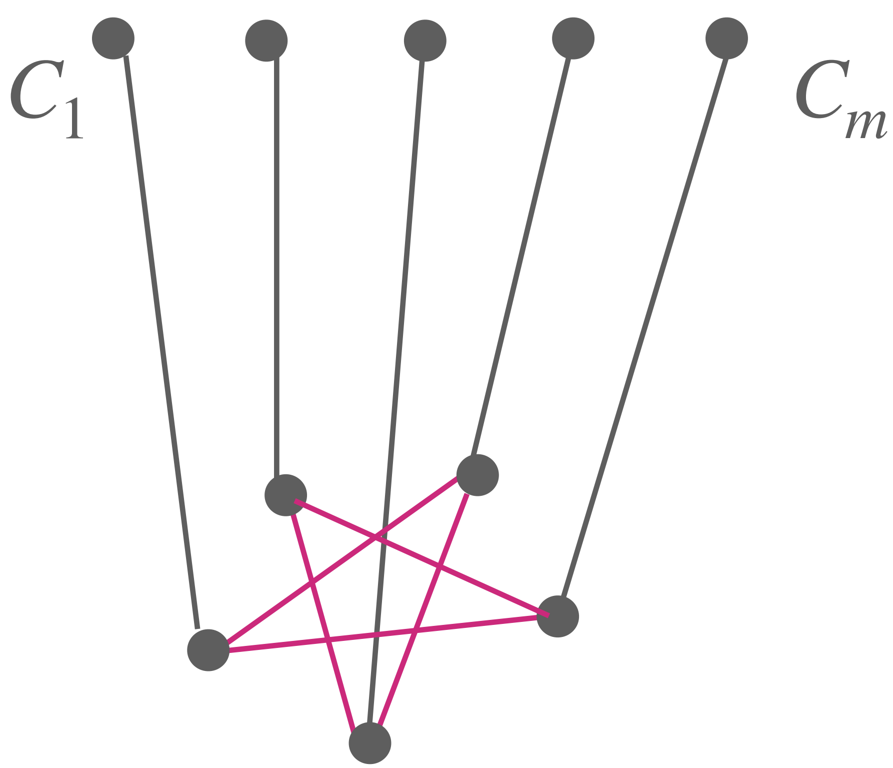


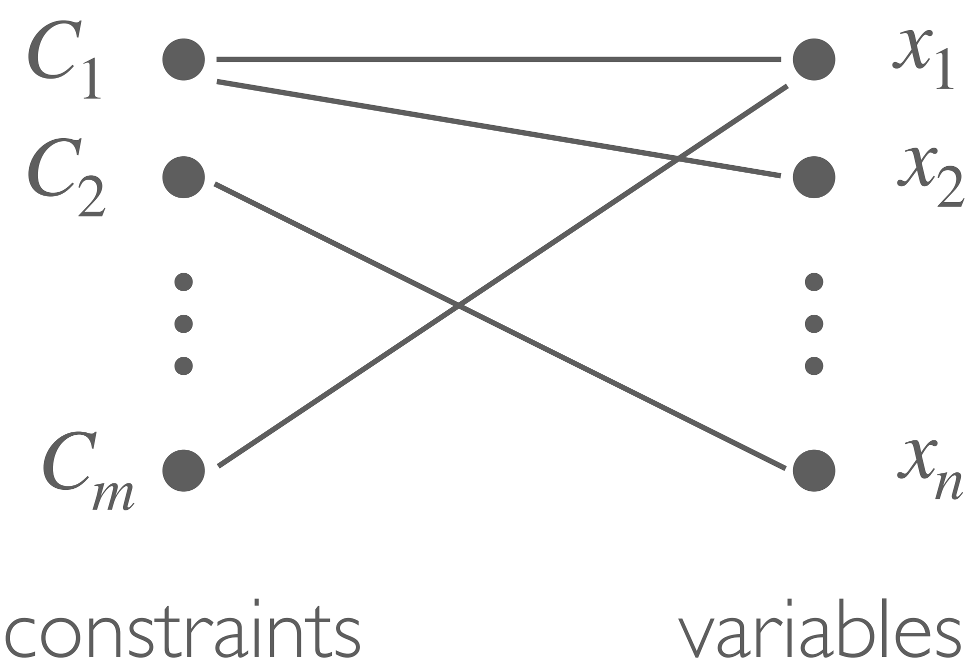


Regularization

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \ldots v_{i,k}\rangle$$

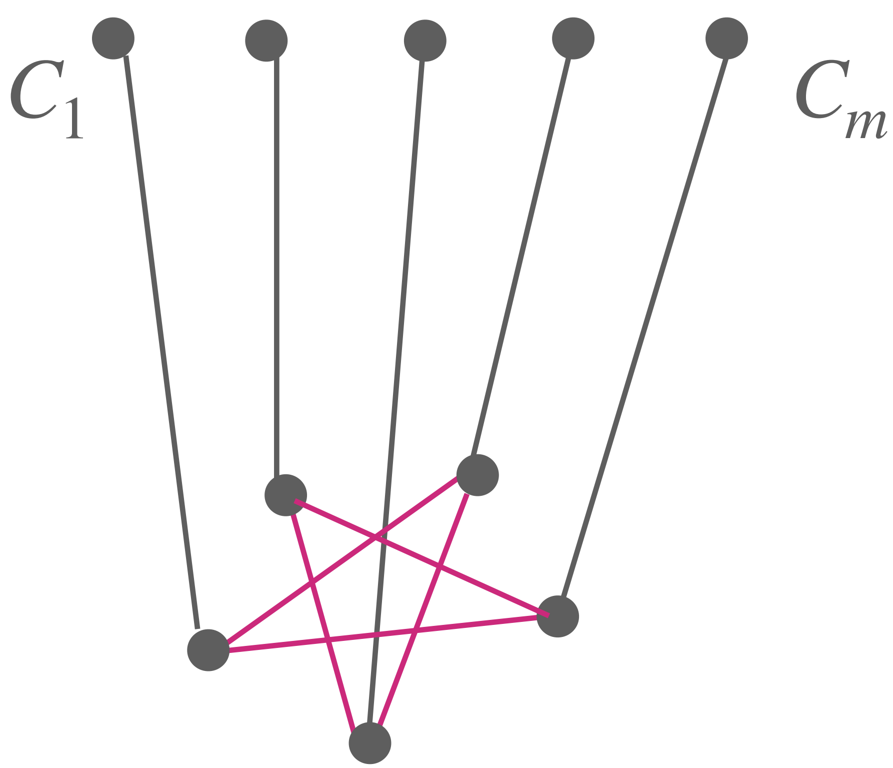




Regularization

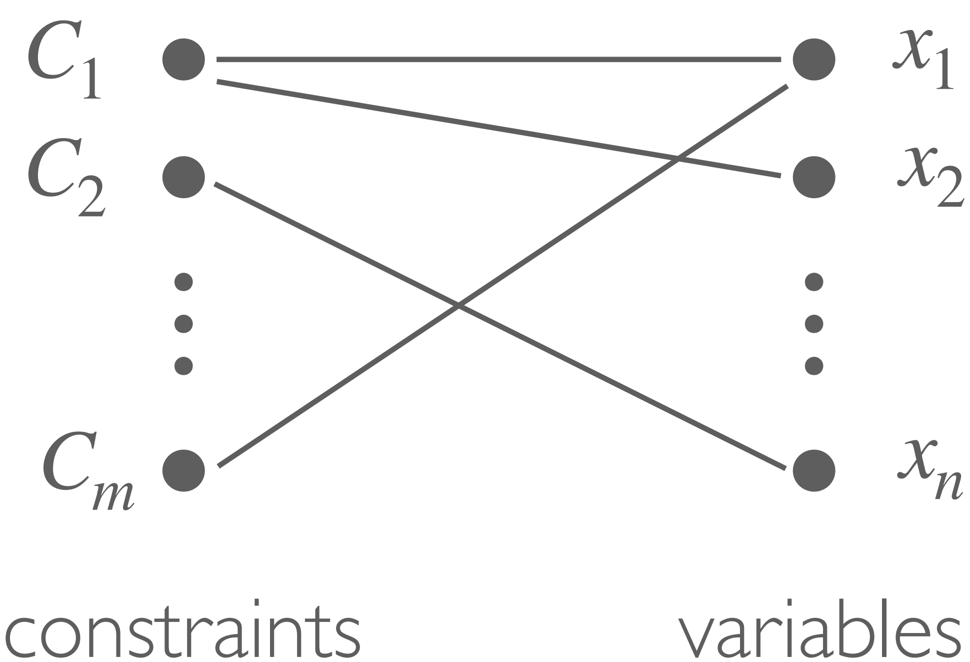
Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle\, |v_{i,1} v_{i,2} \ldots v_{i,k}\rangle$$



Expander:

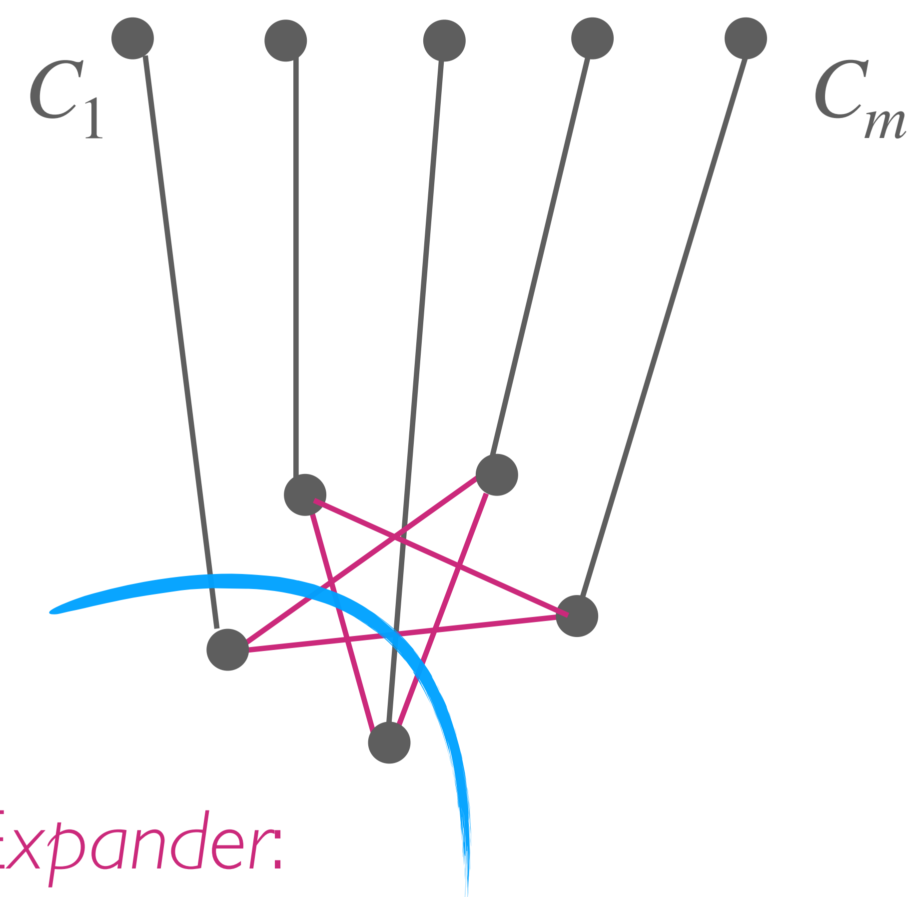
1. d-regular graph
2. expansion



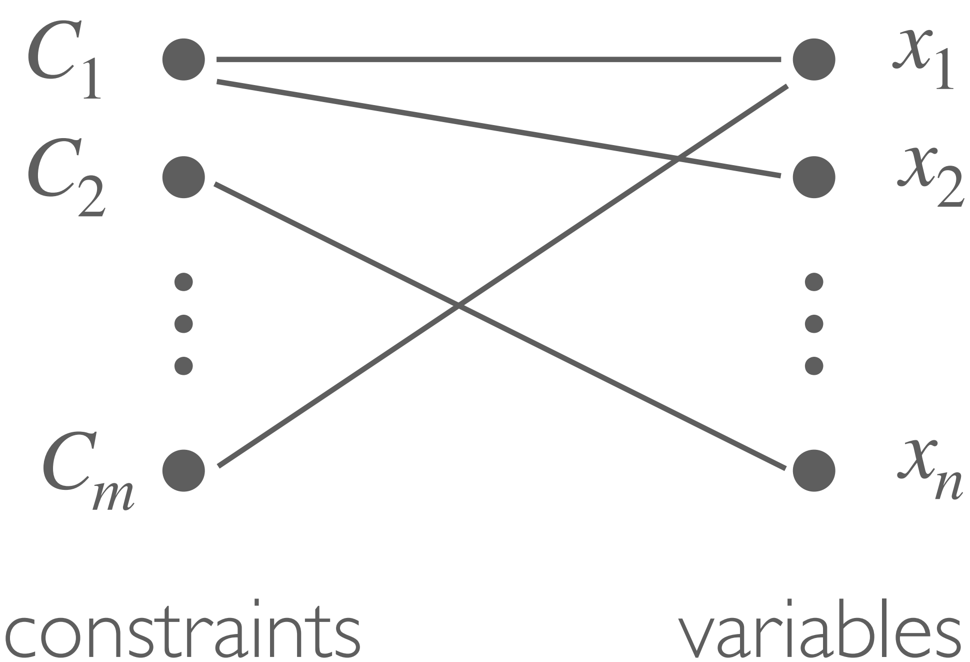
Regularization

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \ldots v_{i,k}\rangle$$



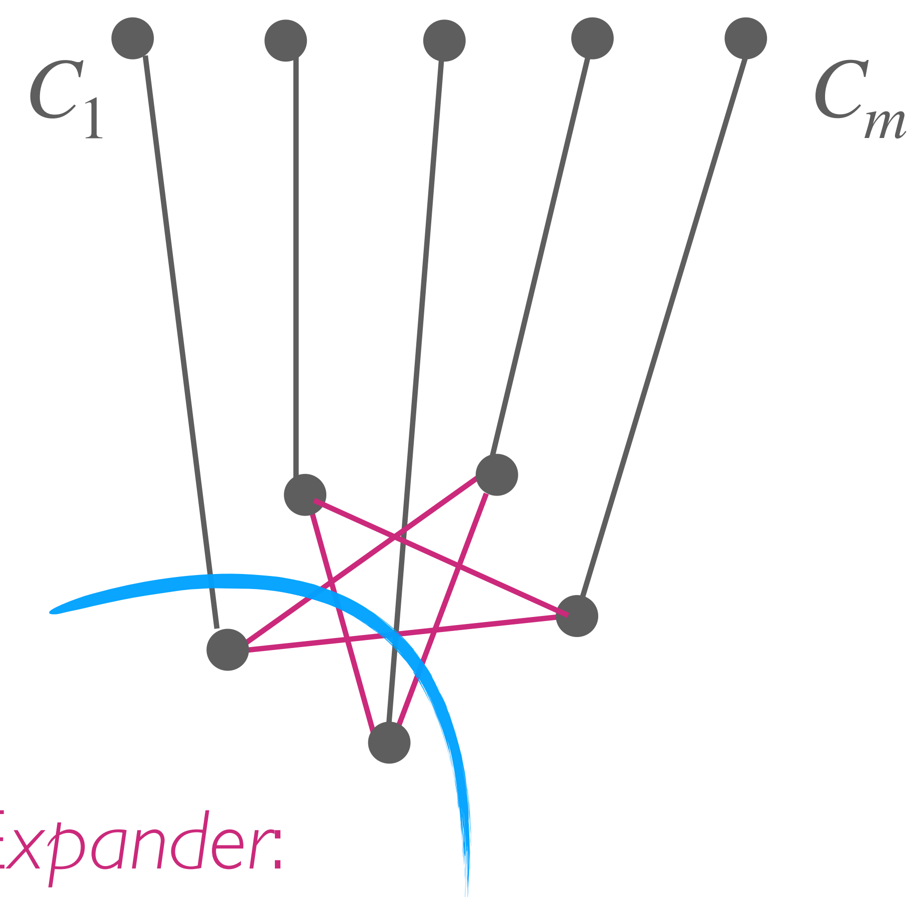
Expander:
1. d-regular graph
2. expansion



Regularization

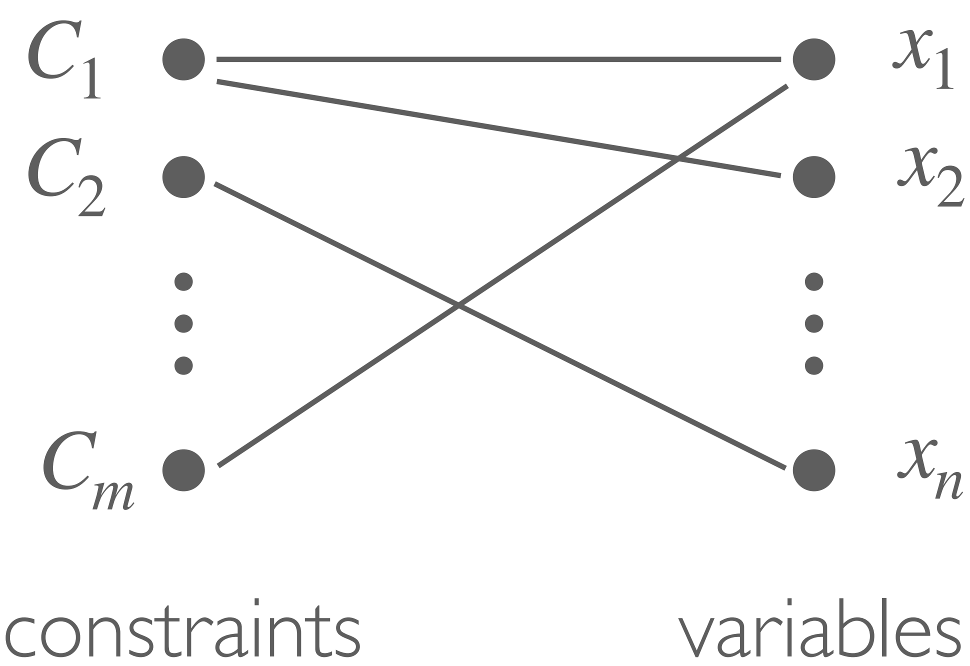
Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \ldots v_{i,k}\rangle$$



Expander:

1. d-regular graph
2. expansion

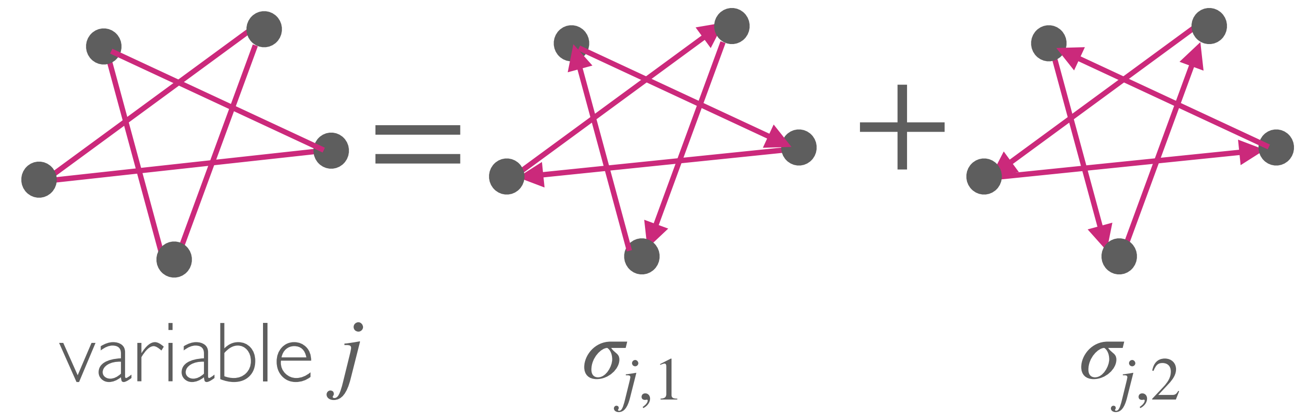


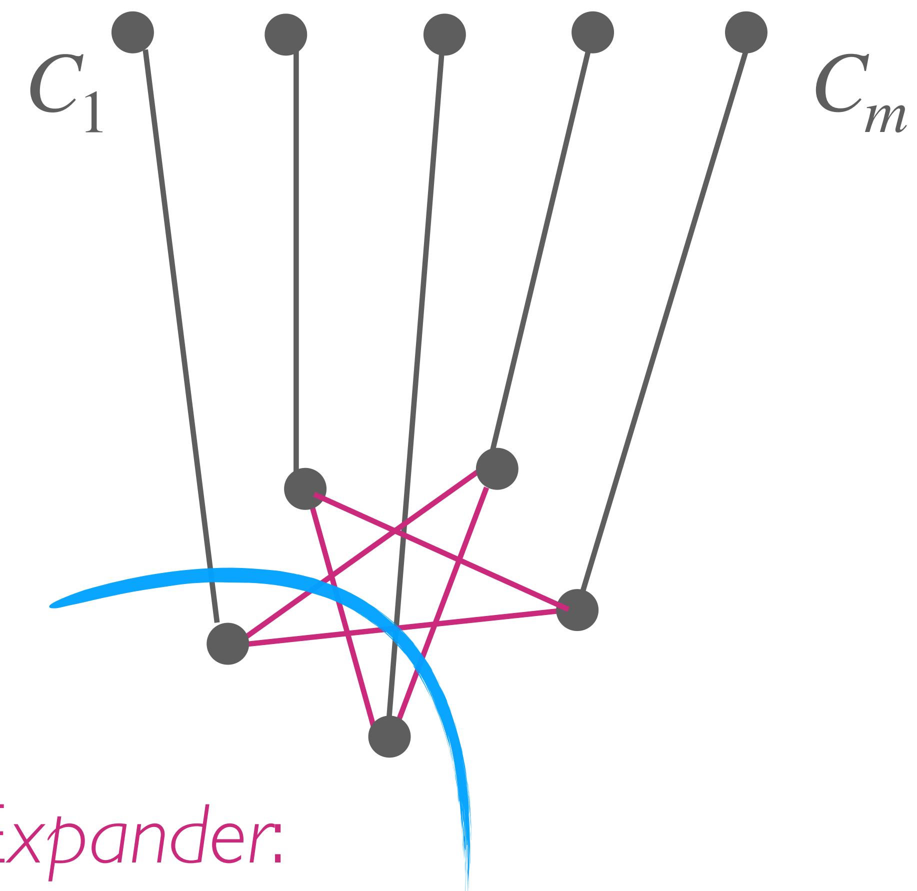
Expansion property ensures in the soundness case, a const. fraction of constraints are not satisfiable.

Regularization

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \dots v_{i,k}\rangle$$





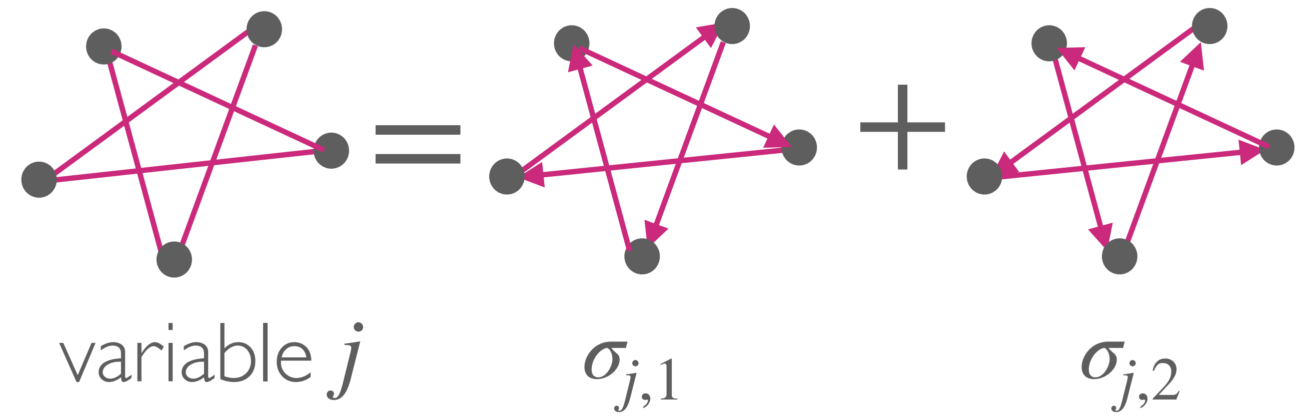
Expander:

1. d-regular graph
2. expansion

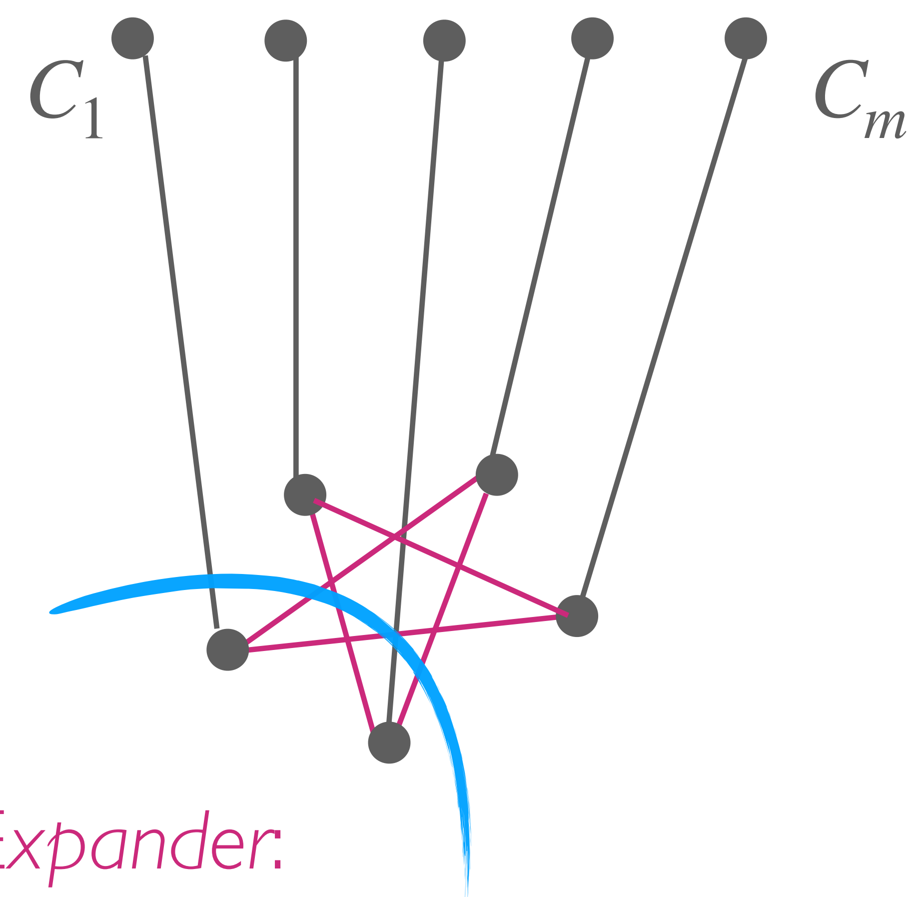
Regularization

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \ldots v_{i,k}\rangle$$



$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \ldots v_{i,k}\rangle$$



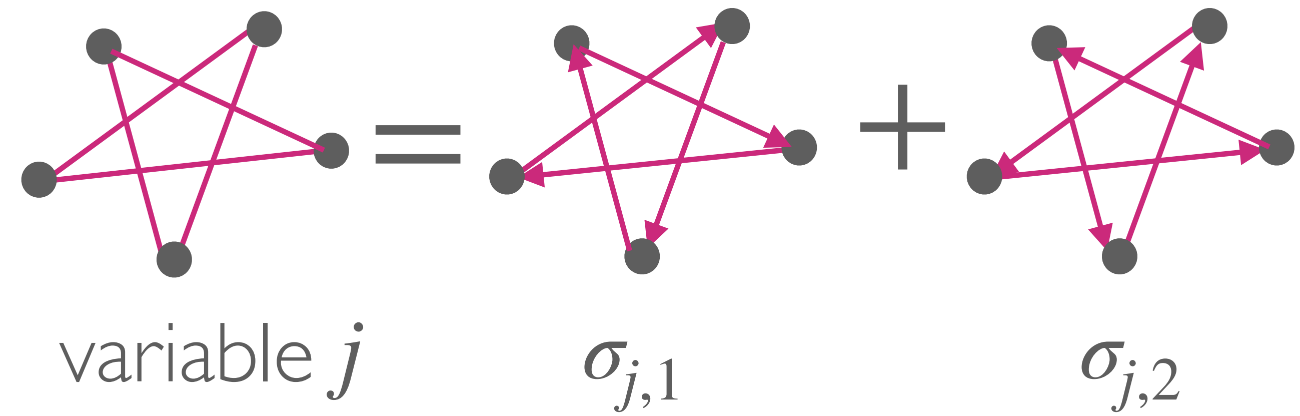
Expander:

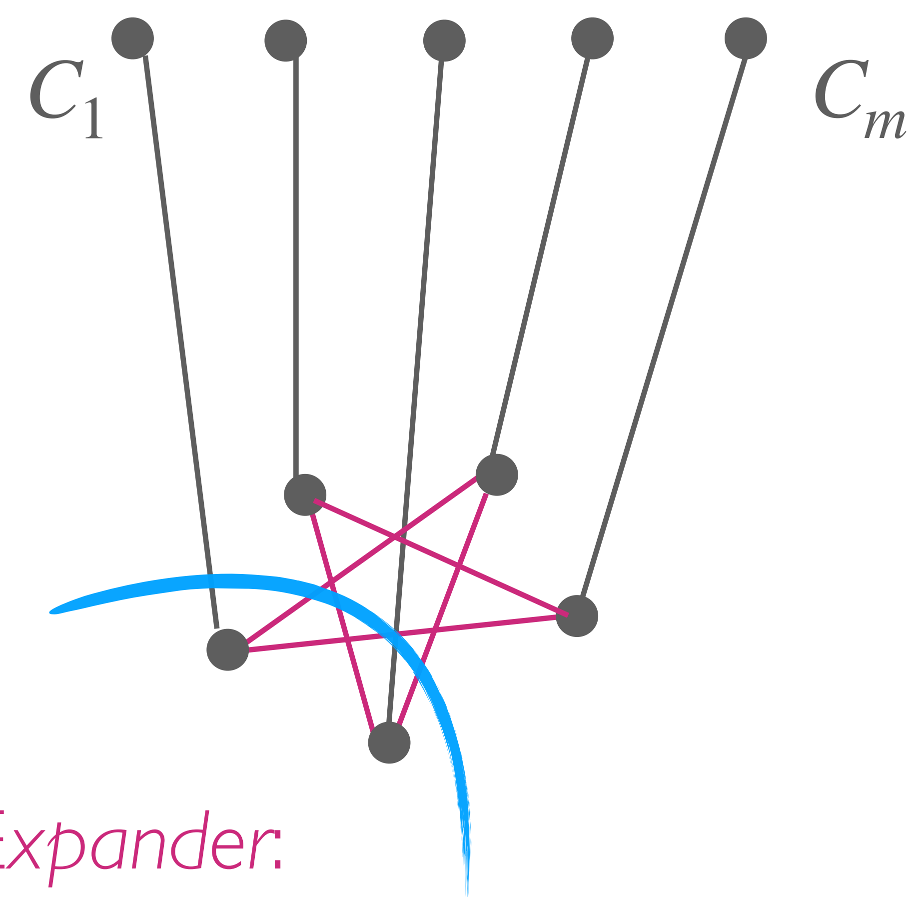
1. d-regular graph
2. expansion

Regularization

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \dots v_{i,k}\rangle$$





$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \dots v_{i,k}\rangle$$

(from C_i and v, we know the variables and its value)

$$\mapsto \frac{1}{\sqrt{mq}} \sum_{i} \sum_{j \in C_i} |C_i\rangle |j\rangle |x_{i,j}\rangle$$

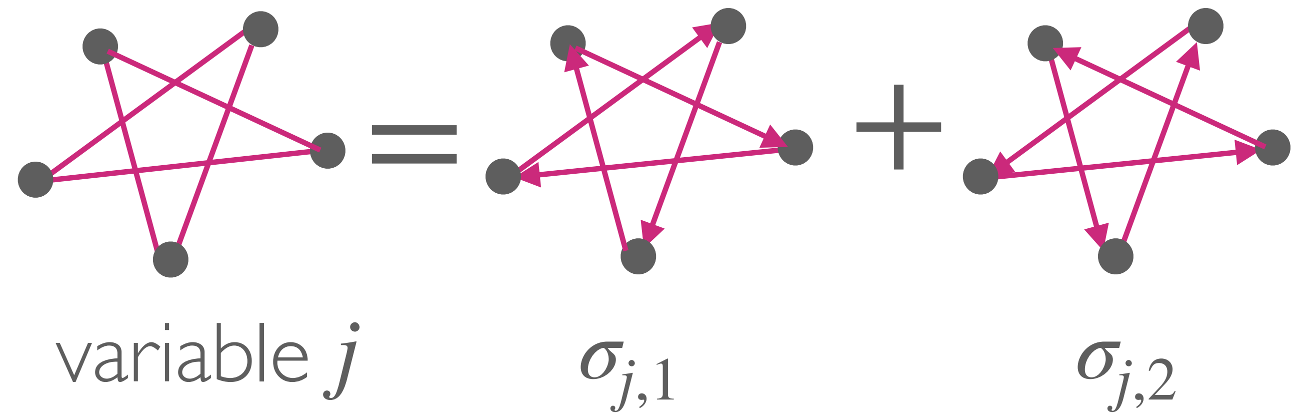
Expander:

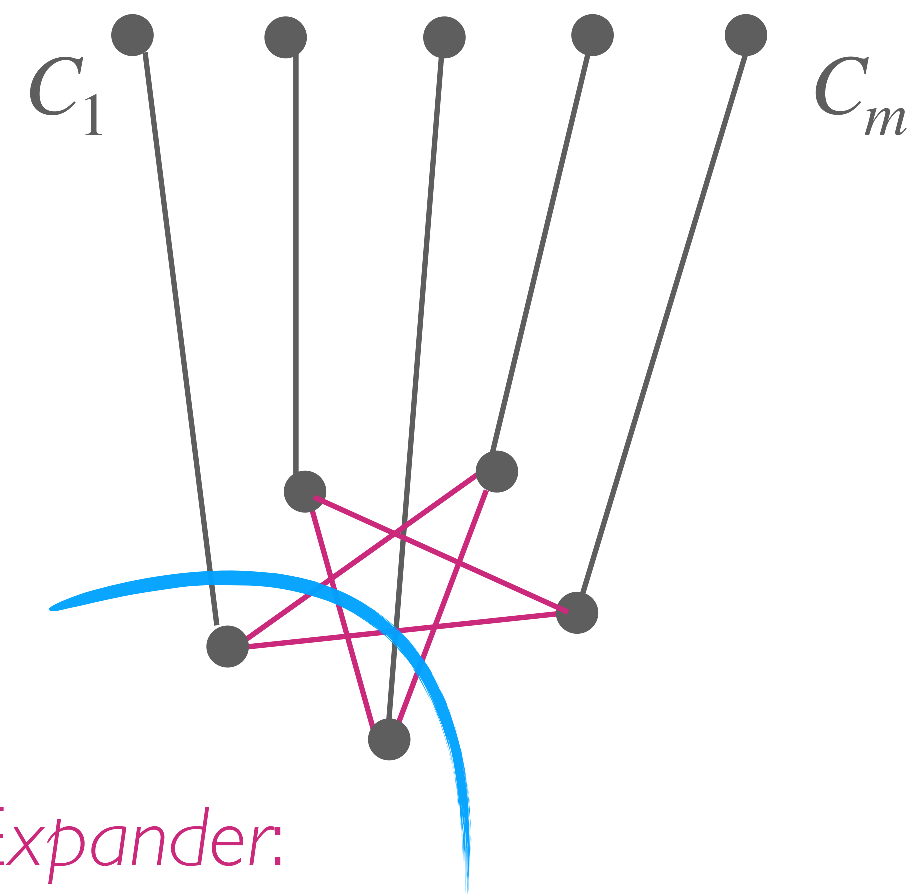
1. d-regular graph
2. expansion

Regularization

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \dots v_{i,k}\rangle$$





Expander:

1. d-regular graph
2. expansion

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \dots v_{i,k}\rangle$$

(from C_i and v, we know the variables and its value)

$$\mapsto \frac{1}{\sqrt{mq}} \sum_{i} \sum_{j \in C_i} |C_i\rangle |j\rangle |x_{i,j}\rangle$$

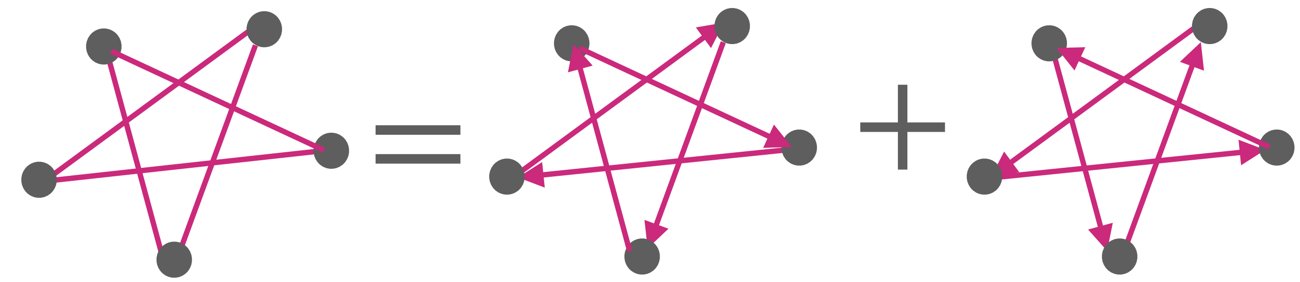
(apply some permutation)

$$\mapsto \frac{1}{\sqrt{mq}} \sum_{i} \sum_{j \in C_i} |C_{\sigma_{j,1}(i)}\rangle |j\rangle |x_{i,j}\rangle$$

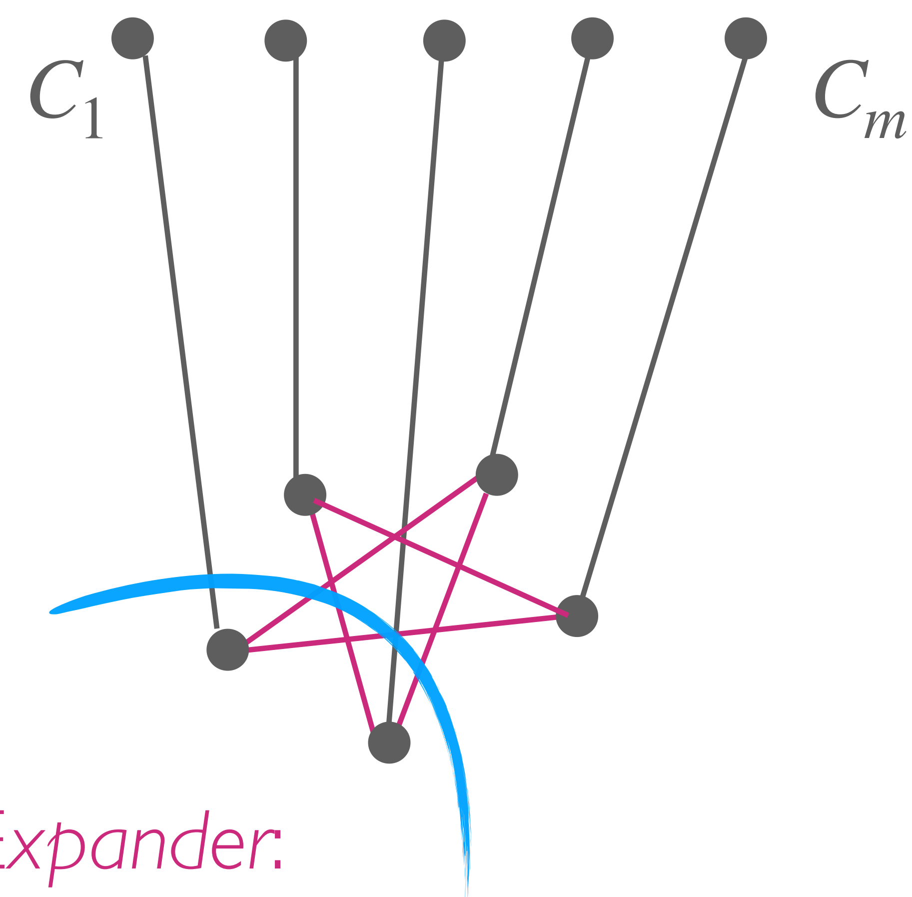
Regularization

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \ldots v_{i,k}\rangle$$



variable j $\sigma_{j,1}$ $\sigma_{j,2}$



$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \ldots v_{i,k}\rangle$$

(from C_i and v, we know the variables and its value)

$$\mapsto \frac{1}{\sqrt{mq}} \sum_{i} \sum_{j \in C_i} |C_i\rangle |j\rangle |x_{i,j}\rangle$$

SwapTest

(apply some permutation)

$$\mapsto \frac{1}{\sqrt{mq}} \sum_{i} \sum_{j \in C_i} |C_{\sigma_{j,1}(i)}\rangle |j\rangle |x_{i,j}\rangle$$

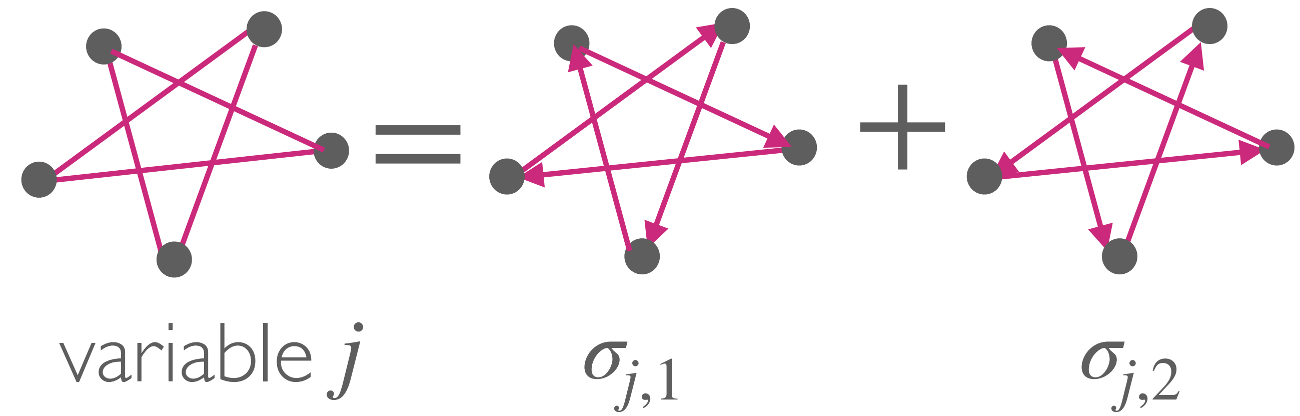
Expander:

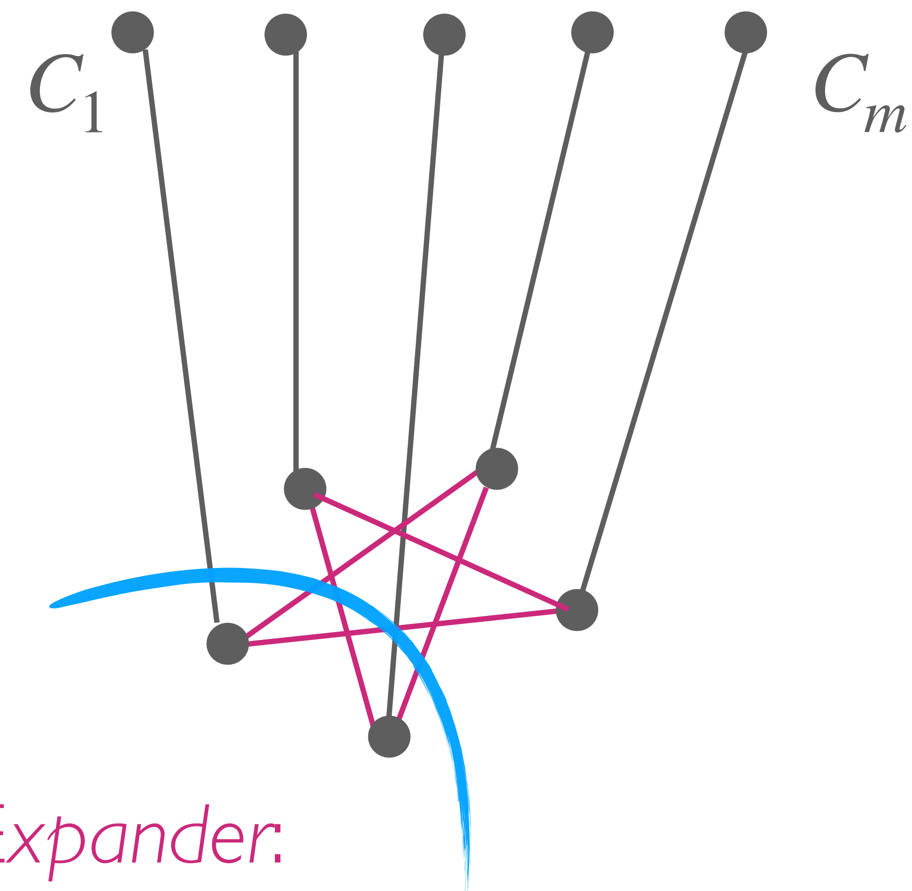
1. d-regular graph
2. expansion

What about NEXP?

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \ldots v_{i,k}\rangle$$





$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \ldots v_{i,k}\rangle$$

(from C_i and v, we know the variables and its value)

$$\mapsto \frac{1}{\sqrt{mq}} \sum_{i} \sum_{j \in C_i} |C_i\rangle |j\rangle |x_{i,j}\rangle$$

(apply some permutation)

$$\mapsto \frac{1}{\sqrt{mq}} \sum_{i} \sum_{j \in C_i} |C_{\sigma_{j,1}(i)}\rangle |j\rangle |x_{i,j}\rangle$$

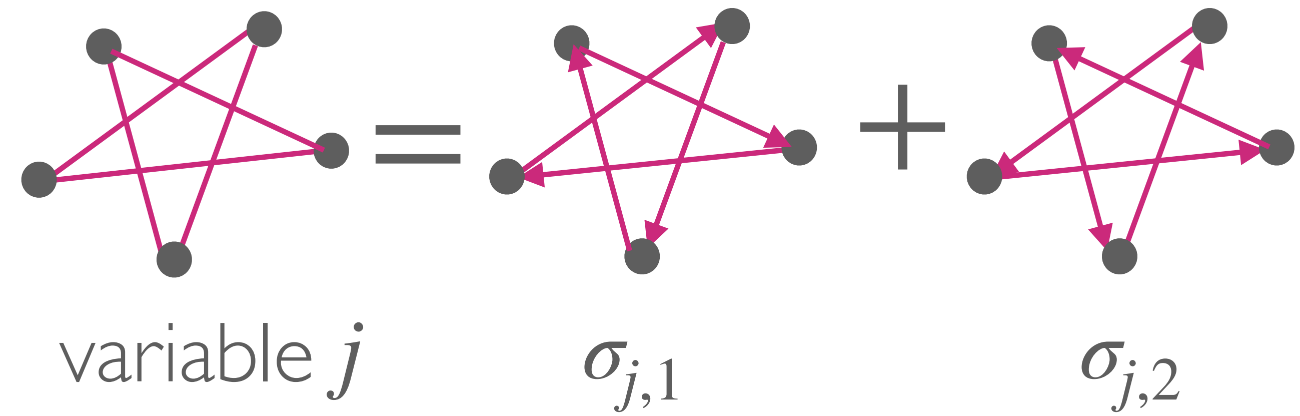
Expander:

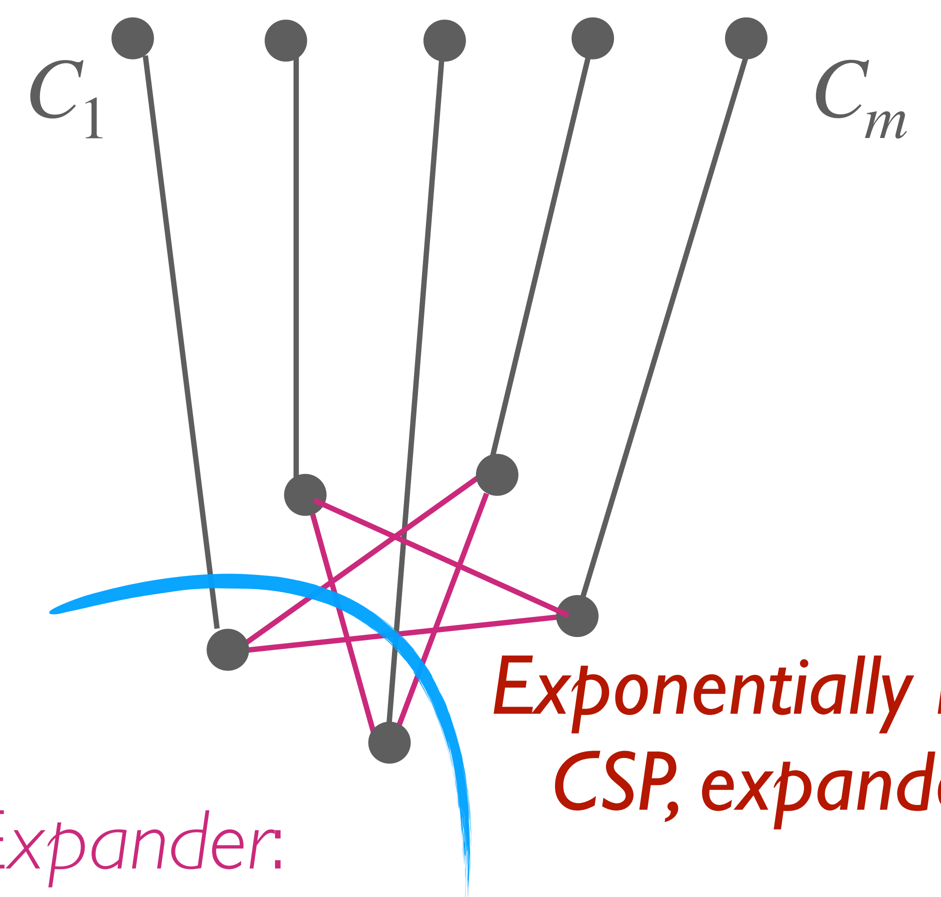
1. d-regular graph
2. expansion

What about NEXP?

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \dots v_{i,k}\rangle$$





Exponentially large CSP, expanders

Expander:

1. d-regular graph
2. expansion

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \dots v_{i,k}\rangle$$

(from C_i and v, we know the variables and its value)

$$\mapsto \frac{1}{\sqrt{mq}} \sum_{i} \sum_{j \in C_i} |C_i\rangle |j\rangle |x_{i,j}\rangle$$

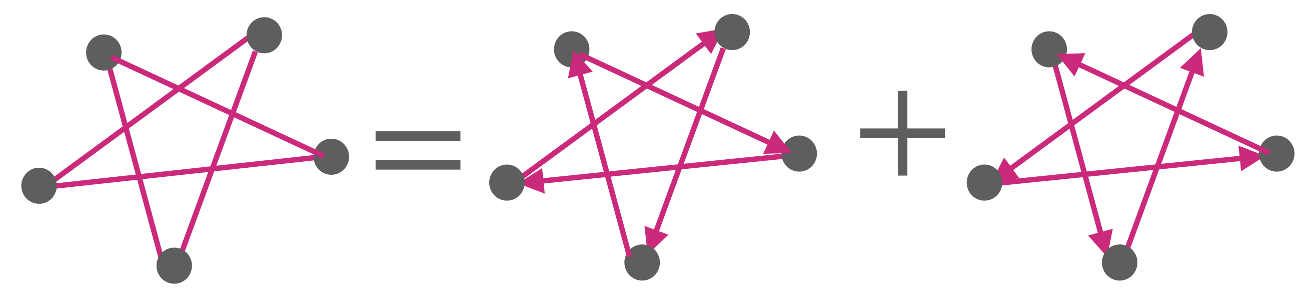
(apply some permutation)

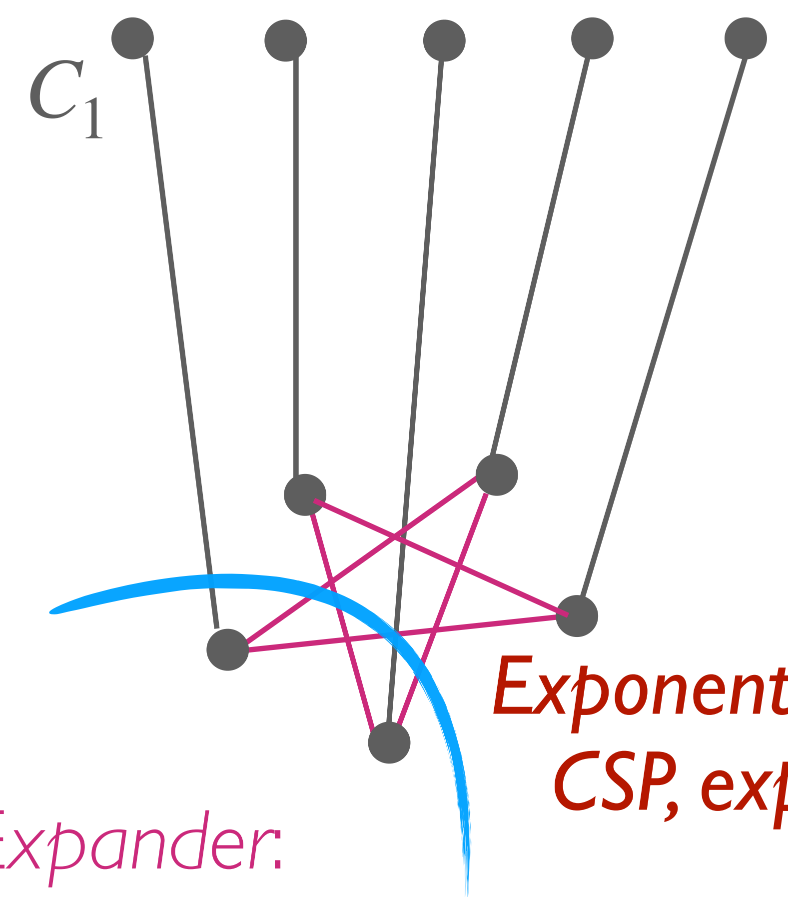
$$\mapsto \frac{1}{\sqrt{mq}} \sum_{i} \sum_{j \in C_i} |C_{\sigma_{j,1}(i)}\rangle |j\rangle |x_{i,j}\rangle$$

What about NEXP?

Merlin: (faithful in yes case)

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \ldots v_{i,k}\rangle$$





Exponentially large CSP, expanders

Expander:
1. d-regular graph
2. expansion

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |C_i\rangle |v_{i,1} v_{i,2} \ldots v_{i,k}\rangle$$

(from C_i and v, we know the variables and its value)

$$\mapsto \frac{1}{\sqrt{mq}} \sum_{i} \sum_{j \in C_i} |C_i\rangle |j\rangle |x_{i,j}\rangle$$

Needs to be efficient

(apply some permutation)

$$\mapsto \frac{1}{\sqrt{mq}} \sum_{i} \sum_{j \in C_i} |C_{\sigma_{j,1}(i)}\rangle |j\rangle |x_{i,j}\rangle$$

Theorem. $\mathrm{NEXP} \subseteq \mathrm{QMA}^+(2)$

Theorem. $\mathrm{NEXP} \subseteq \mathrm{QMA}^{+}(2) \subseteq \mathrm{NEXP}$.

Theorem. $\mathrm{NEXP} \subseteq \mathrm{QMA}^{+}(2) \subseteq \mathrm{NEXP}$**.**

Thank you!