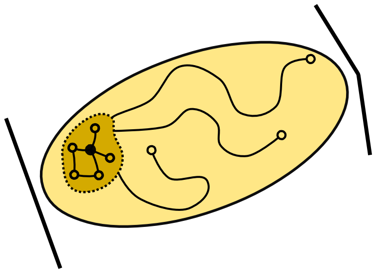
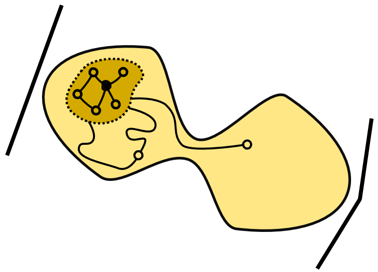
Growing Seed Sets: QW Sampling and st-Connectivity



Simon Apers
Inria, CWI

simon.apers@inria.fr



CWI-Inria Workshop – September 18, 2019 – Amsterdam

Classical vs Quantum Sampling

Classical sample:

- probability distribution $p \in \mathbb{R}^n$
- normalization $\|p\|_1 = 1$
- π = uniform distribution

Classical vs Quantum Sampling

Classical sample:

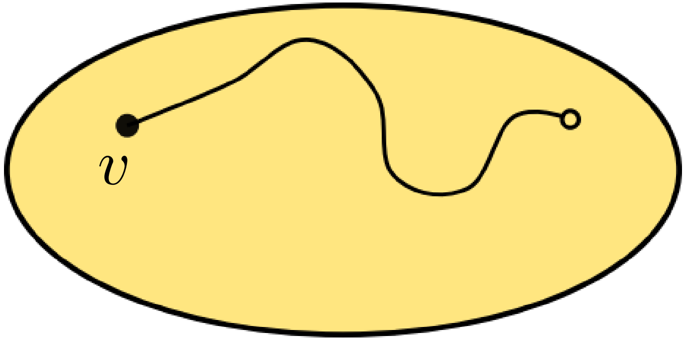
- probability distribution $p \in \mathbb{R}^n$
- normalization $\|p\|_1 = 1$
- π = uniform distribution

Quantum sample:

- quantum state $|q\rangle \in \mathbb{C}^n$
- normalization $\||q\rangle\|_2 = 1$
- $|\pi\rangle$ = uniform superposition

Random Walk Sampling

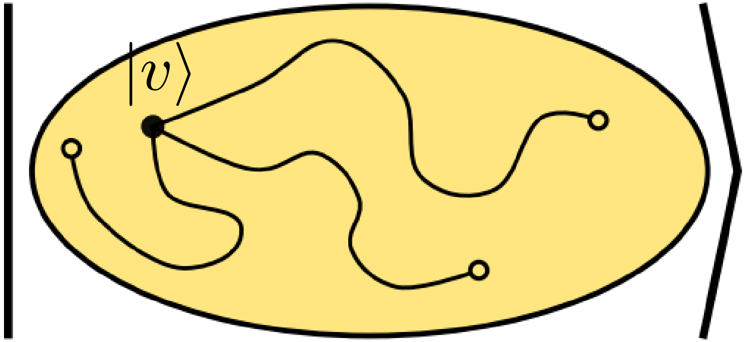
- initial node v, t-step RW $P^t v$
- stationary distribution π and $P^t v \to \pi$
- many applications in graph problems, statistical physics, $\ldots$



** unless stated otherwise, all graphs are regular, bounded degree expanders*

Quantum Walk Sampling

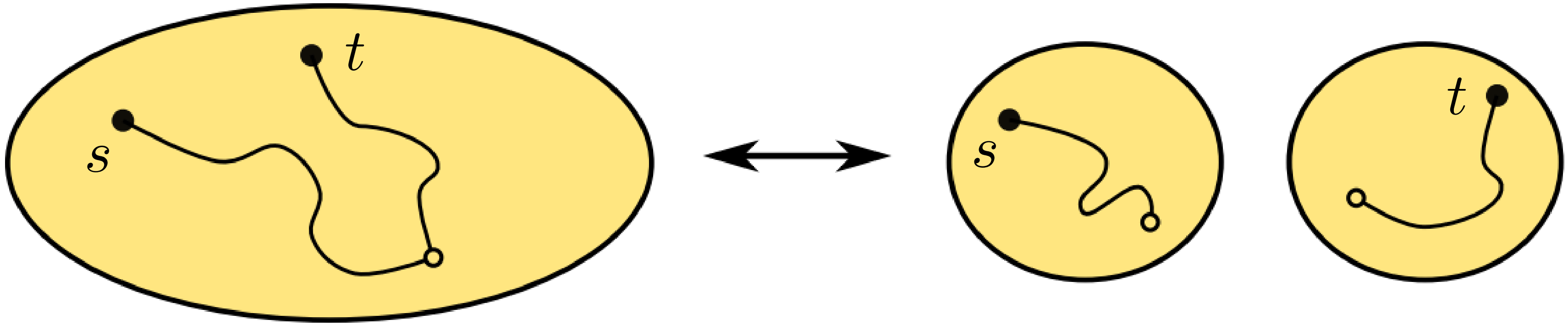
- quantum sample of RW distribution: $|P^t v\rangle = P^t|v\rangle / \|P^t|v\rangle\|$
- use QWs to create $|P^t v\rangle \to |\pi\rangle$. Complexity?
- many applications in element distinctness, formula evaluation, . . .



st-Connectivity

Classical: $O(n^{1/2})$

- use RWs from s and t
  to sample $\pi^{(s)}$ and $\pi^{(t)}$
- look for collision
  using $O(n^{1/2})$ samples



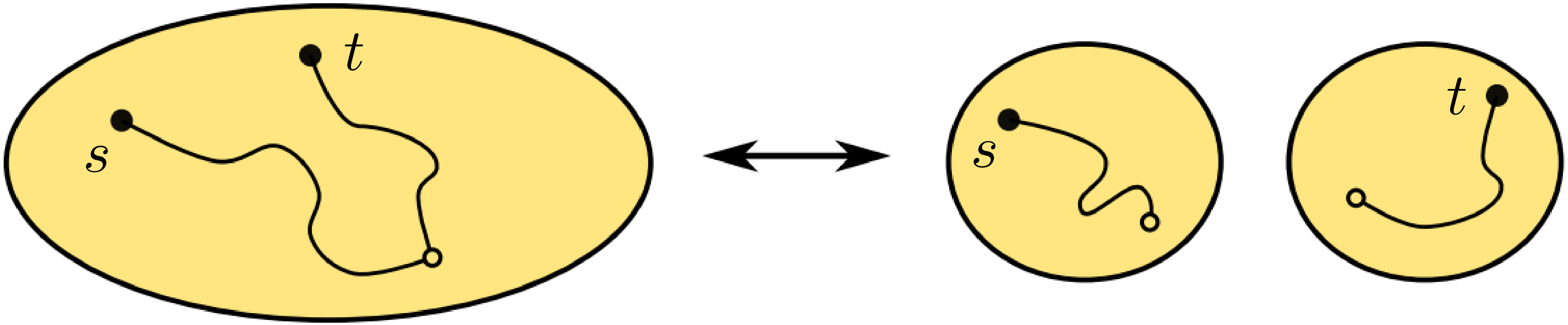
st-Connectivity

Classical: $O(n^{1/2})$

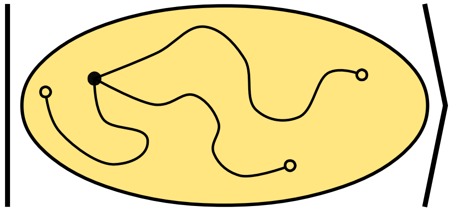
- use RWs from s and t to sample $\pi^{(s)}$ and $\pi^{(t)}$
- look for collision using $O(n^{1/2})$ samples

Quantum: ?

- use QWs from s and t to create $|\pi^{(s)}\rangle$ and $|\pi^{(t)}\rangle$
- do "swap test" using $O(1)$ samples



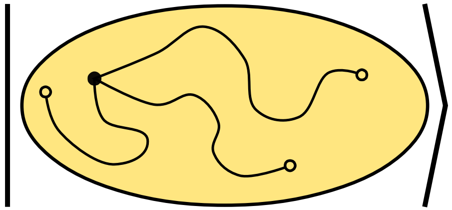
Quantum Sampling



?

complexity of generating quantum sample $|\pi\rangle$

Quantum Sampling

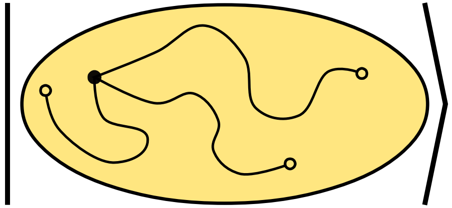


? complexity of generating quantum sample $|\pi\rangle$

folklore scheme: [Watrous'98]

- t-step QW creates *subnormalized* quantum sample $P^t|v\rangle + |\Gamma\rangle$

Quantum Sampling

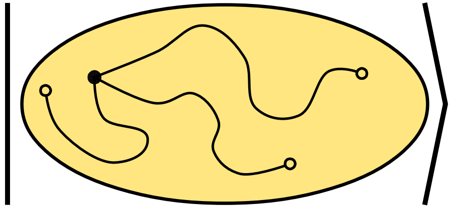


? complexity of generating quantum sample $|\pi\rangle$

folklore scheme: [Watrous'98]

- t-step QW creates *subnormalized* quantum sample $P^t|v\rangle + |\Gamma\rangle$
- use "amplitude amplification" to obtain $|P^t v\rangle = P^t|v\rangle / \|P^t|v\rangle\|$

Quantum Sampling



?

complexity of generating quantum sample $|\pi\rangle$

folklore scheme: [Watrous'98]

- t-step QW creates *subnormalized* quantum sample $P^t|v\rangle + |\Gamma\rangle$
- use "amplitude amplification" to obtain $|P^t v\rangle = P^t|v\rangle / \|P^t|v\rangle\|$

$\rightarrow$ complexity: $O(\|P^t|v\rangle\|^{-1}) \in O(n^{1/2})$ copies of $P^t|v\rangle + |\Gamma\rangle$

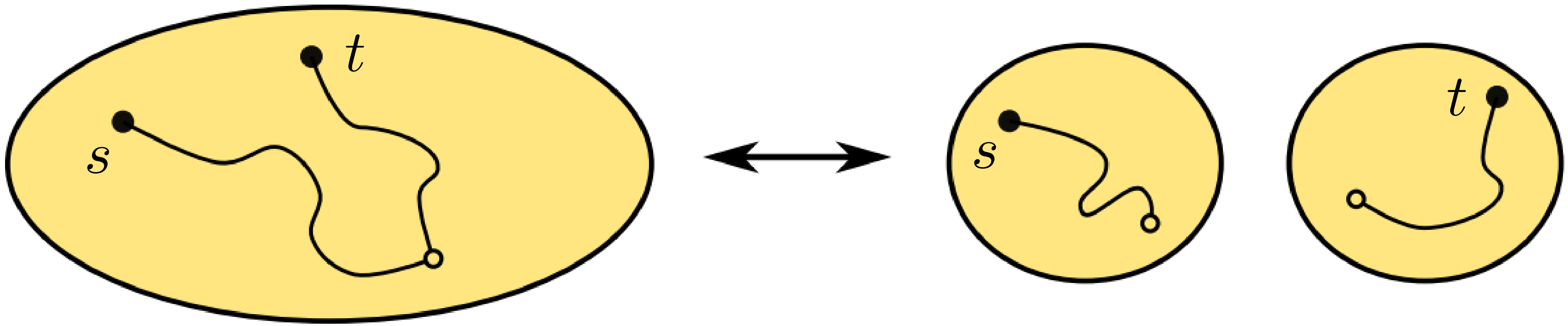
st-Connectivity

Classical: $O(n^{1/2})$

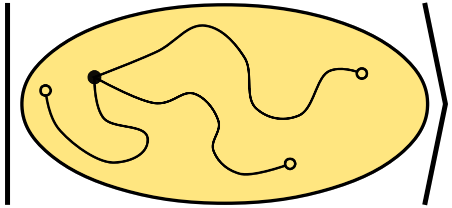
- use RWs from s and t to sample $\pi^{(s)}$ and $\pi^{(t)}$
- look for collision using $O(n^{1/2})$ samples

Quantum: $O(n^{1/2})$

- use QWs from s and t to create $|\pi^{(s)}\rangle$ and $|\pi^{(t)}\rangle$
- do "swap test" using $O(1)$ samples



Quantum Sampling



?

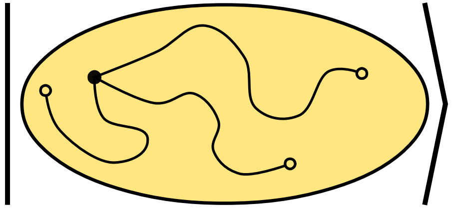
complexity of generating quantum sample $|\pi\rangle$

main bottleneck of folklore approach:

number of samples

$$\|P^t|v\rangle\|^{-1} \approx |\langle\pi|v\rangle|^{-1} \approx n^{1/2}$$

Quantum Sampling



?

complexity of generating quantum sample $|\pi\rangle$

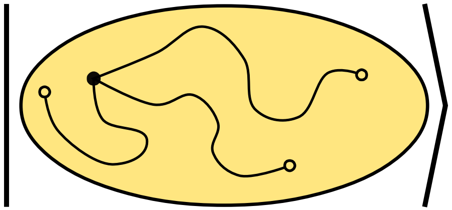
main bottleneck of folklore approach:

number of samples

$$\|P^t|v\rangle\|^{-1} \approx |\langle\pi|v\rangle|^{-1} \approx n^{1/2}$$

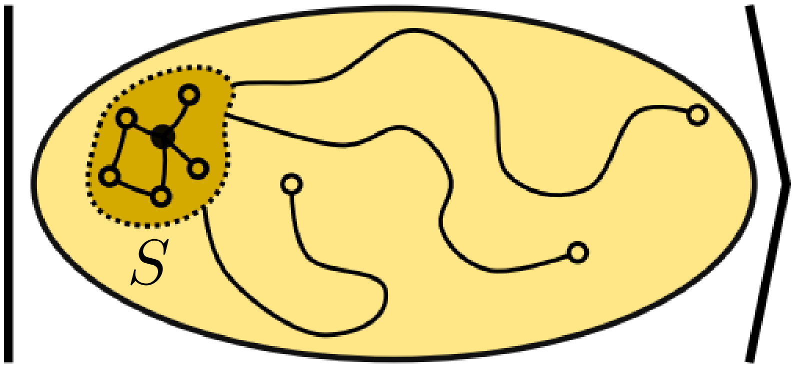
improve projection on $|\pi\rangle$
by (classically) growing seed set from v

Quantum Sampling



?

complexity of generating quantum sample $|\pi\rangle$

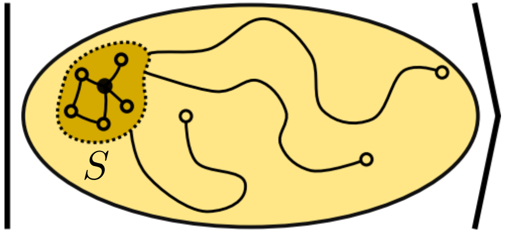


improve projection on $|\pi\rangle$
by (classically) growing seed set from v

$$S \subset \mathcal{V},\ |S| = n^{1/3}:$$

$$\|P^t|\pi_S\rangle\| \geq |\langle\pi|\pi_S\rangle| \geq n^{-1/3}$$

Quantum Sampling



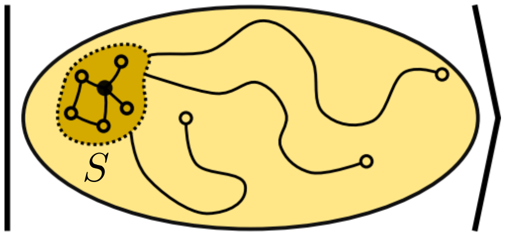
?

complexity of generating quantum sample $|P^t v\rangle$

improved scheme:

- classically "grow" seed set S of size $n^{1/3}$

Quantum Sampling



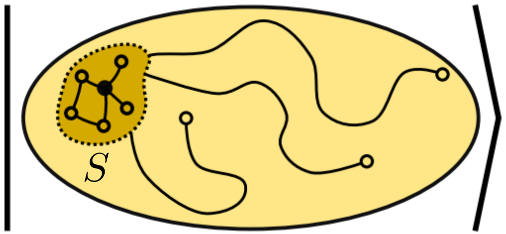
?

complexity of generating quantum sample $|P^t v\rangle$

improved scheme:

- classically “grow” seed set S of size $n^{1/3}$
- t-step QW creates *subnormalized* quantum sample $P^t|\pi_S\rangle + |\Gamma\rangle$

Quantum Sampling



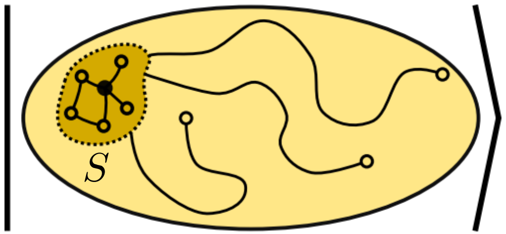
?

complexity of generating quantum sample $|P^t v\rangle$

improved scheme:

- classically "grow" seed set S of size $n^{1/3}$
- t-step QW creates *subnormalized* quantum sample $P^t|\pi_S\rangle + |\Gamma\rangle$
- use "amplitude amplification" to obtain $|P^t\pi_S\rangle = P^t|\pi_S\rangle / \| P^t|\pi_S\rangle \|$

Quantum Sampling



?

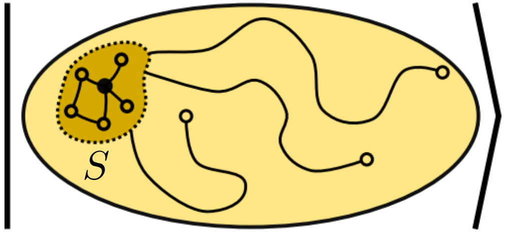
complexity of generating quantum sample $|P^t v\rangle$

improved scheme:

- classically “grow” seed set S of size $n^{1/3}$
- t-step QW creates *subnormalized* quantum sample $P^t|\pi_S\rangle + |\Gamma\rangle$
- use “amplitude amplification” to obtain $|P^t \pi_S\rangle = P^t|\pi_S\rangle / \|P^t|\pi_S\rangle\|$

complexity: $O(\|P^t|\pi_S\rangle\|^{-1}) \in O(n^{1/3})$ copies of $P^t|\pi_S\rangle + |\Gamma\rangle$

Quantum Sampling



?

complexity of generating quantum sample $|P^t v\rangle$

improved scheme:

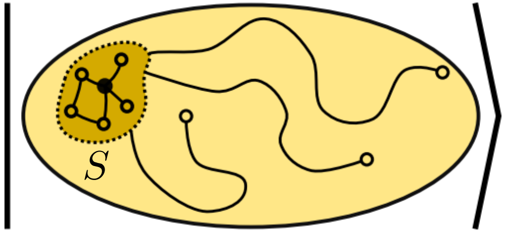
- classically “grow” seed set S of size $n^{1/3}$

quantum sample $|\pi\rangle$ in $O(n^{1/3})$ QW steps

- t-step QW c … $_S\rangle + |\Gamma\rangle$
- use “amplitude amplification” to obtain $|P^t \pi_S\rangle = P^t|\pi_S\rangle / \| P^t |\pi_S\rangle \|$

complexity: $O(\| P^t|\pi_S\rangle\|^{-1}) \in O(n^{1/3})$ copies of $P^t|\pi_S\rangle + |\Gamma\rangle$

Quantum Sampling



?

complexity of generating quantum sample $|P^t v\rangle$

improved scheme:

- classically "grow" seed set S of size $n^{1/3}$
- t-step QW c … $s\rangle + |\Gamma\rangle$
- use "a … $s\rangle\|$

complexity: $O(\|\Gamma \ldots |\pi_S\rangle\| \ldots) \in O(n \ldots)$ copies of $\Gamma \ldots |\pi_S\rangle + |\Gamma\rangle$

quantum sample $|\pi\rangle$ in $O(n^{1/3})$ QW steps

space-time tradeoff: exchange $(1, n^{1/2})$ for $(n^{1/3}, n^{1/3})$

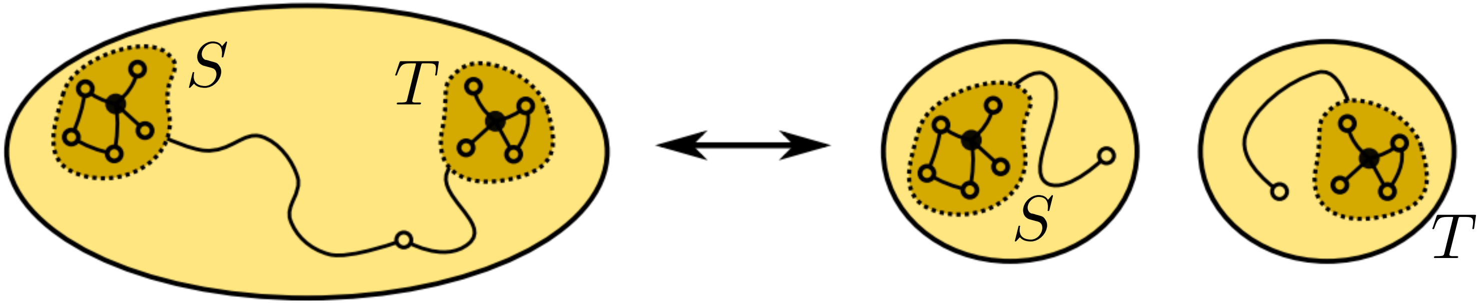
st-Connectivity

Classical: $O(n^{1/2})$

- use RWs from s, t to sample $\pi^{(s)}, \pi^{(t)}$
- look for collision using $O(n^{1/2})$ samples

Quantum: $O(n^{1/3})$

- grow seed sets S, T from s, t
- use QWs from $|\pi_S\rangle, |\pi_T\rangle$ to create $|\pi^{(s)}\rangle, |\pi^{(t)}\rangle$
- do "swap test" using $O(1)$ samples

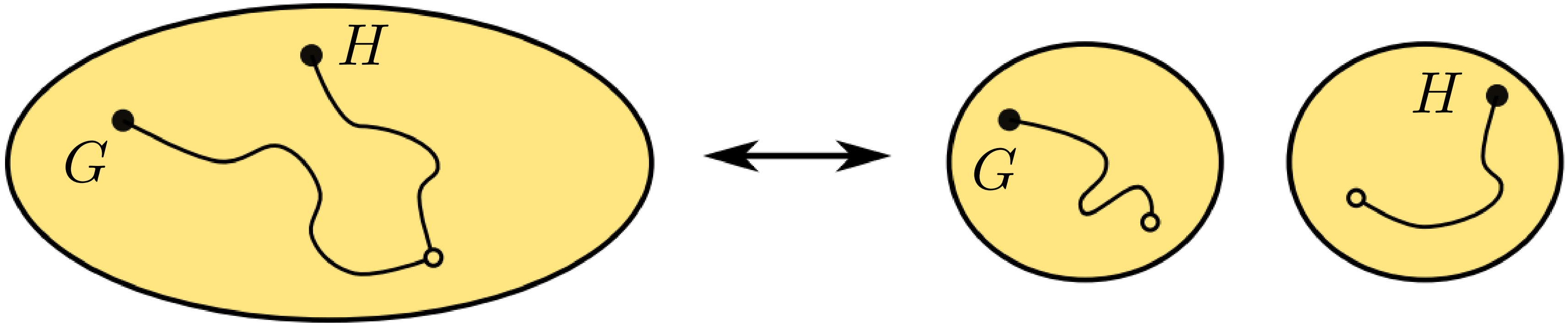


Graph Isomorphism

instance of st-connectivity:
pairwise permutations describe RW over isomorphisms

$$G \to G' \to G'' \to \dots$$

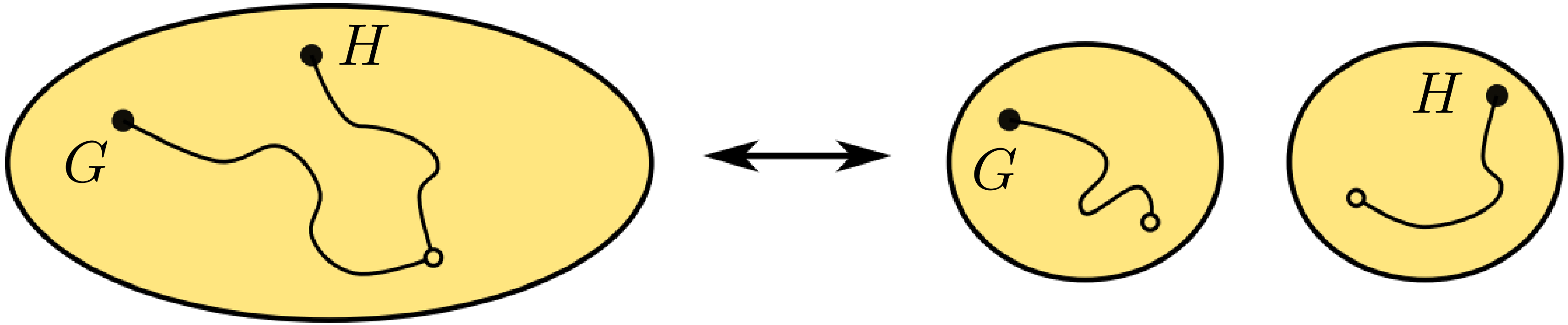
? is there permutation that turns G into H?



Graph Isomorphism

quantum approach:

1. create superpositions $|G\rangle, |H\rangle$ over isomorphisms of G, H
2. compare states using swap test



Graph Isomorphism

quantum approach:

1. create superpositions $|G\rangle, |H\rangle$ over isomorphisms of G, H
2. compare states using swap test

- [AMRR'11]: $\Omega(2^{n/2})$ lower bound for generalized approach

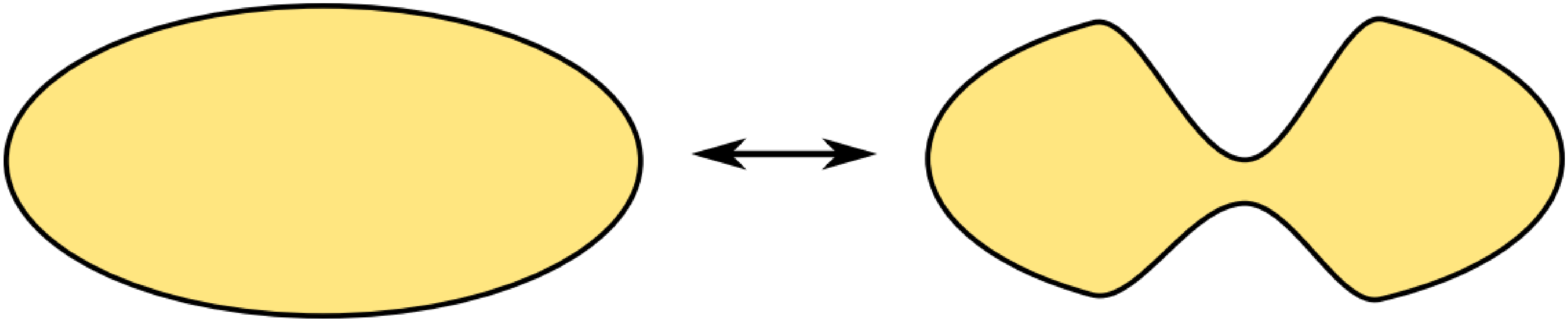
Graph Isomorphism

quantum approach:

1. create superpositions $|G\rangle, |H\rangle$ over isomorphisms of G, H
2. compare states using swap test

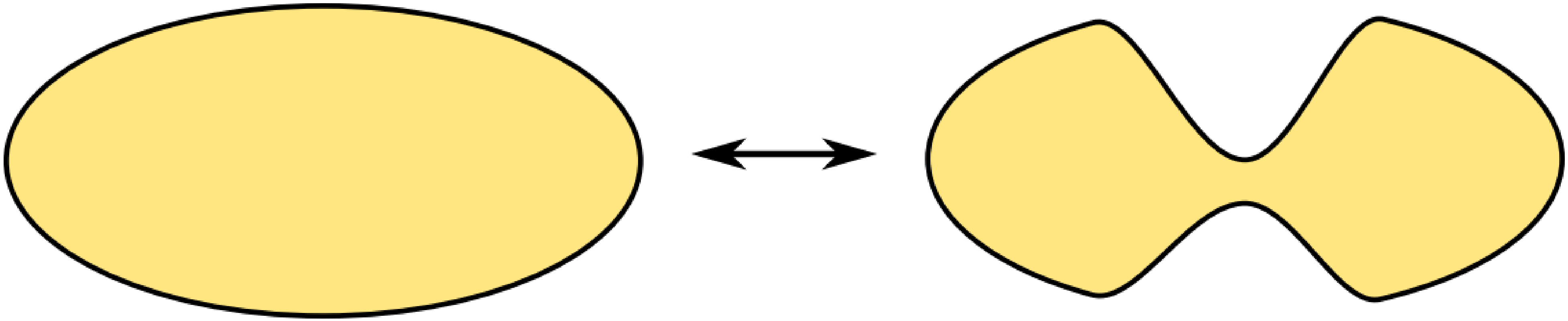
- [AMRR'11]: $\Omega(2^{n/2})$ lower bound for generalized approach
- this work: $O(2^{n/3})$ using QW sampling

Expansion Testing



$$\Phi = \min_{\mathcal{S} \subset \mathcal{V} : |\mathcal{S}| \leq n/2} |\partial \mathcal{S}| / |\mathcal{S}|$$

Expansion Testing



$$\Phi = \min_{\mathcal{S}\subset\mathcal{V}:|\mathcal{S}|\leq n/2} |\partial\mathcal{S}|/|\mathcal{S}|$$

[Goldreich-Ron'97]:

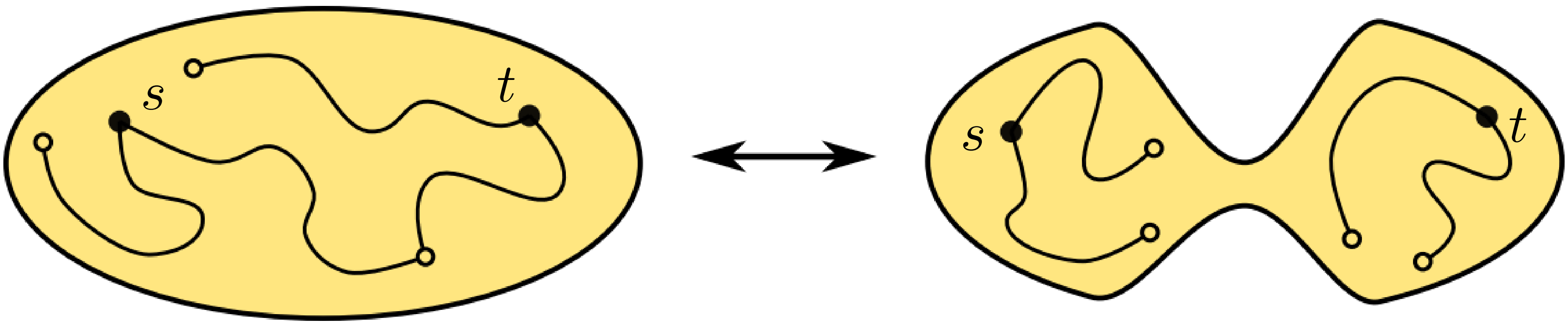
does G have expansion $\geq \Upsilon$, or is G far from any such graph?

Expansion Testing

GR expansion tester:

- pick uniformly random nodes s, t
- perform RWs of length Υ^{-2}
- count collisions between $O(n^{1/2})$ samples

if none, `reject`; otherwise, `accept`



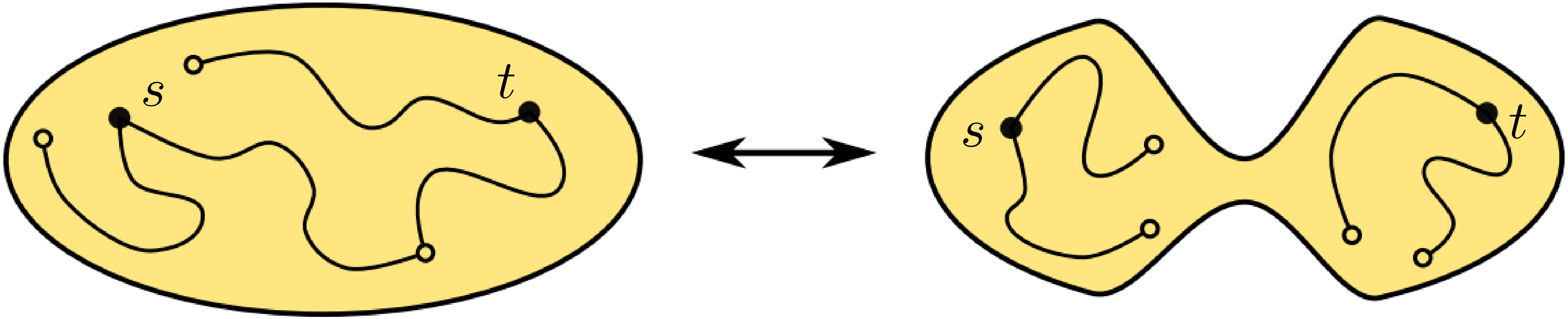
Expansion Testing

GR expansion tester:

$O(n^{1/2}\Upsilon^{-2})$

- pick uniformly random nodes s, t
- perform RWs of length Υ^{-2}
- count collisions between $O(n^{1/2})$ samples

if none, `reject`; otherwise, `accept`

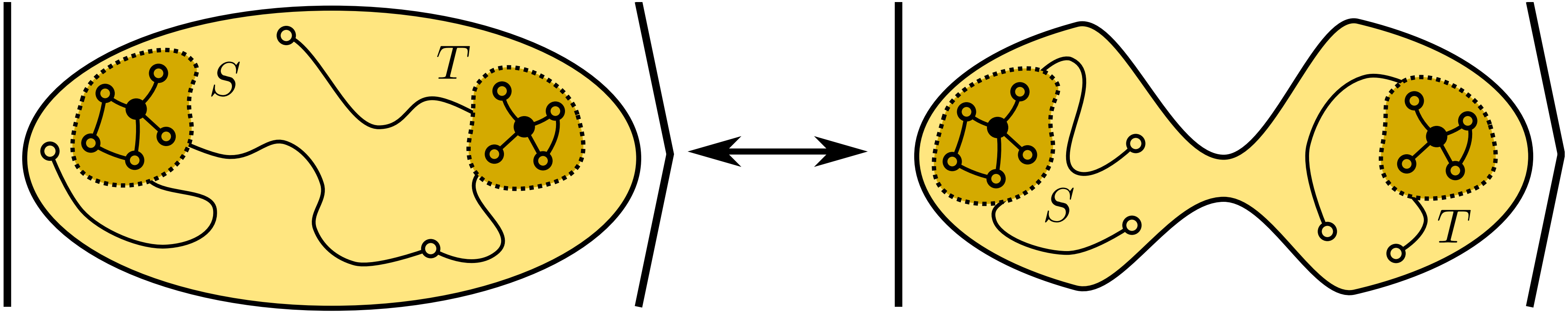


Expansion Testing

quantum expansion tester:
[arXiv:1907.02369]

- pick uniformly random nodes s, t
- "grow" seed sets S, T from s, t
- create $|P^\tau \pi_S\rangle, |P^\tau \pi_T\rangle$ for $T = \Upsilon^{-2}$
- compare states with swap test

if disjoint, `reject`; otherwise, `accept`



How to Grow a Seed Set?

◇ use tool from local graph clustering!

How to Grow a Seed Set?

◇ use tool from local graph clustering!

“evolving set process”

[Andersen-Oveis Gharan-Peres-Trevisan’12]

How to Grow a Seed Set?

◇ use tool from local graph clustering!

“evolving set process”

[Andersen-Oveis Gharan-Peres-Trevisan’12]

= Markov chain on node subsets:

How to Grow a Seed Set?

$\diamond$ use tool from local graph clustering!

“evolving set process”

[Andersen-Oveis Gharan-Peres-Trevisan’12]

= Markov chain on node subsets: from $\mathcal{S} \subseteq \mathcal{V}$

- pick $Z \in [0, 1]$ u.a.r.
- $\forall u \in \mathcal{V} : u \in \mathcal{S}'$ iff $|E(u, \mathcal{S})|/d(u) \geq Z$

How to Grow a Seed Set?

$\diamond$ use tool from local graph clustering!

“evolving set process”

[Andersen-Oveis Gharan-Peres-Trevisan’12]

= Markov chain on node subsets: from $\mathcal{S} \subseteq \mathcal{V}$

- pick $Z \in [0, 1]$ u.a.r.
- $\forall u \in \mathcal{V} : u \in \mathcal{S}'$ iff $|E(u, \mathcal{S})|/d(u) \geq Z$

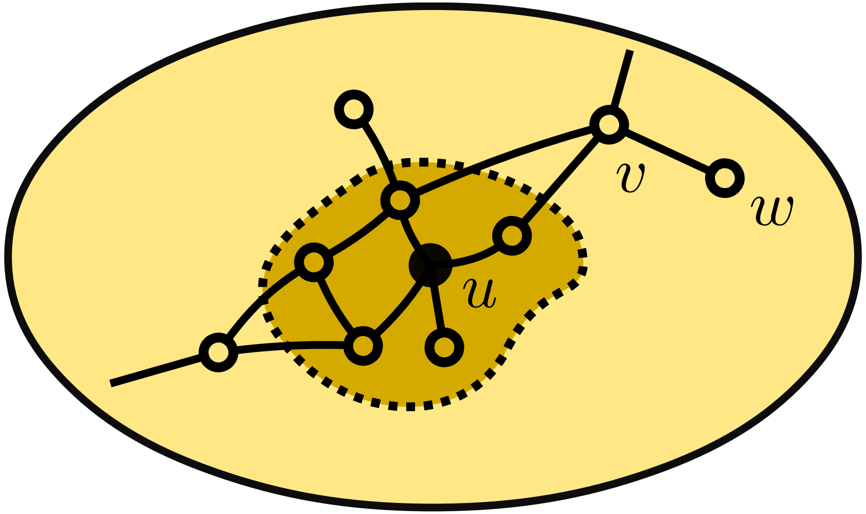
↓ only boundary $\partial\mathcal{S}$ changes

How to Grow a Seed Set?

◇ use tool from local graph clustering!

“evolving set process”

[Andersen-Oveis Gharan-Peres-Trevisan’12]



from $\mathcal{S} \subseteq \mathcal{V}$

- pick $Z \in [0,1]$ u.a.r.
- $\forall u \in \mathcal{V} : u \in \mathcal{S}'$ iff $|E(u,\mathcal{S})|/d(u) \geq Z$

only boundary $\partial\mathcal{S}$ changes

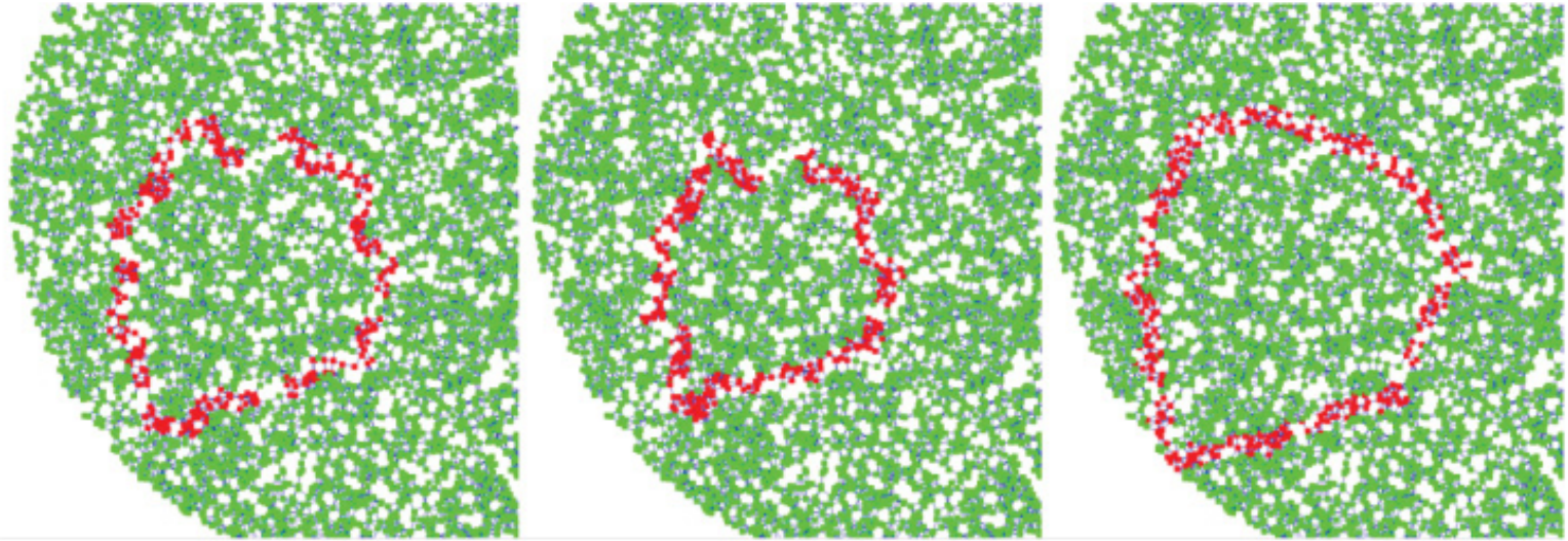
$|E(u,\mathcal{S})|/d(u) = 1, \ |E(v,\mathcal{S})|/d(v) = 1/2, \ |E(w,\mathcal{S})|/d(w) = 0$

How to Grow a Seed Set?

◇ use tool from local graph clustering!

“evolving set process”

[Andersen-Oveis Gharan-Peres-Trevisan’12]



232 steps | 235 steps | 273 steps

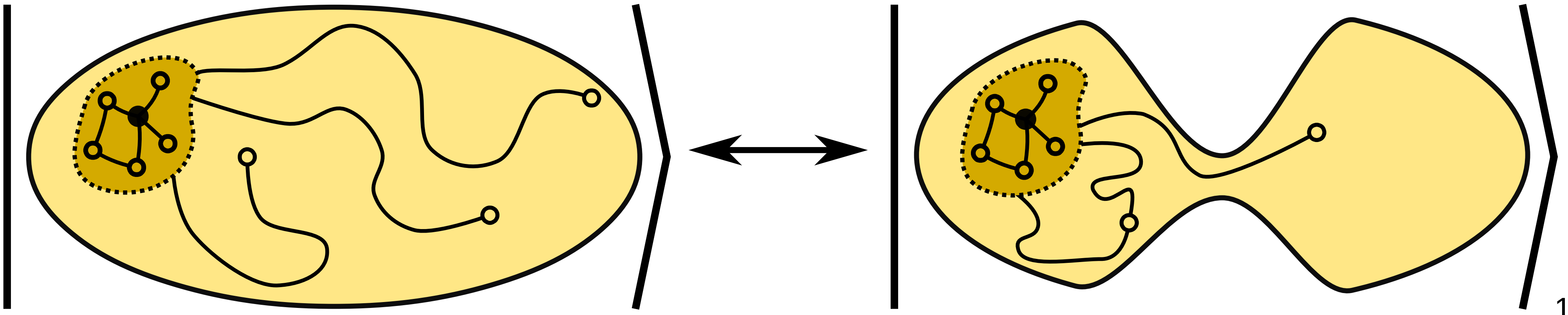
How to Grow a Seed Set?

◇ use tool from local graph clustering!

"evolving set process"

[Andersen-Oveis Gharan-Peres-Trevisan'12]

prop.: ESP returns a set of size $n^{1/3}$ within cluster in $O(n^{1/3}\Upsilon^{-1})$ steps

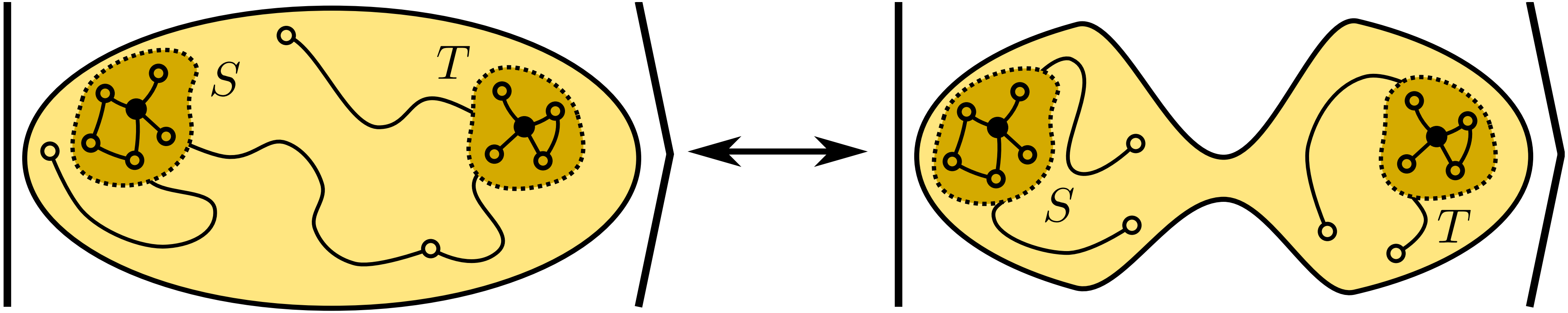


Expansion Testing

quantum expansion tester:
[arXiv:1907.02369]

- pick uniformly random nodes s, t
- "grow" seed sets S, T from s, t
- create $|P^\tau \pi_S\rangle, |P^\tau \pi_T\rangle$ for $T = \Upsilon^{-2}$
- compare states with swap test

if disjoint, `reject`; otherwise, `accept`



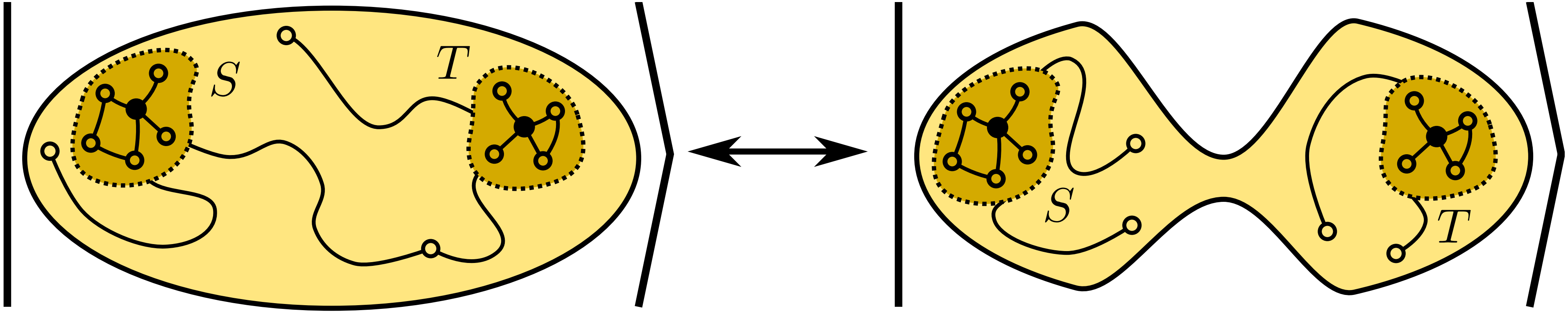
Expansion Testing

quantum expansion tester:
[arXiv:1907.02369]

$O(n^{1/3}\Upsilon^{-2})$

- pick uniformly random nodes s, t
- "grow" seed sets S, T from s, t
- create $|P^\tau \pi_S\rangle, |P^\tau \pi_T\rangle$ for $T = \Upsilon^{-2}$
- compare states with swap test

if disjoint, `reject`; otherwise, `accept`

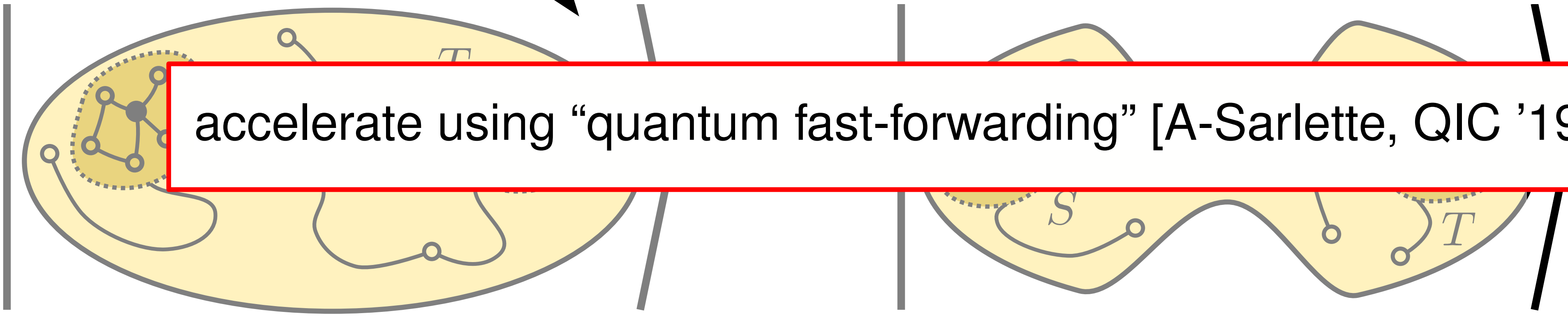


Expansion Testing

quantum expansion tester:
[arXiv:1907.02369]

- pick uniformly random nodes s, t
- "grow" seed sets S, T from s, t
- create $|P^\tau \pi_S\rangle, |P^\tau \pi_T\rangle$ for $T = \Upsilon^{-2}$
- compare states with swap test

if disjoint, `reject`; otherwise, `accept`



accelerate using "quantum fast-forwarding" [A-Sarlette, QIC '19]

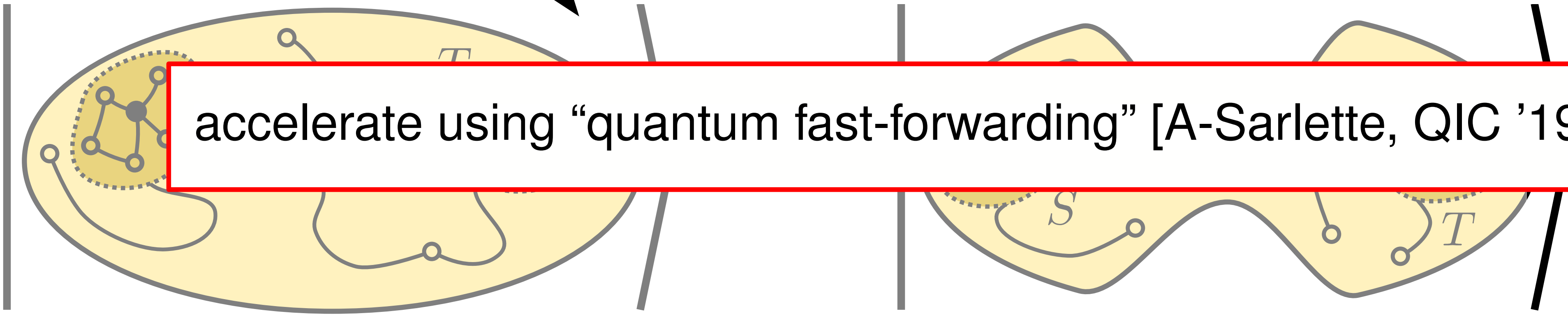
Expansion Testing

quantum expansion tester:
[arXiv:1907.02369]

$O(n^{1/3}\Upsilon^{-1})$

- pick uniformly random nodes s, t
- "grow" seed sets S, T from s, t
- create $|P^\tau \pi_S\rangle, |P^\tau \pi_T\rangle$ for $T = \Upsilon^{-2}$
- compare states with swap test

if disjoint, `reject`; otherwise, `accept`

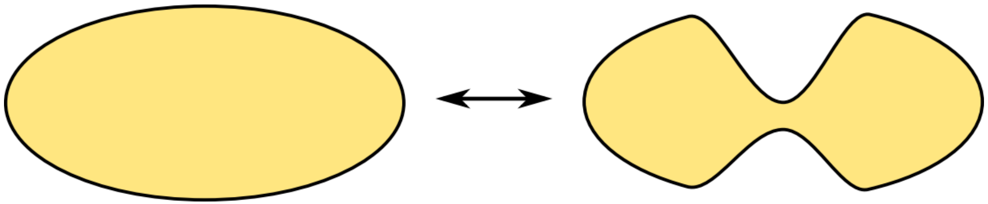


accelerate using "quantum fast-forwarding" [A-Sarlette, QIC '19]

Expansion Testing

[Goldreich-Ron'97]:

does G have expansion $\geq \Upsilon$,
or is G far from any such graph?



[Goldreich-Ron '00]	$O(n^{1/2}\Upsilon^{-2})$ (conj.)	RW collision counting
[CS '07], [KS '07], [NS '07]	$O(n^{1/2}\Upsilon^{-2})$	prove conjecture
[Ambainis-Childs-Liu '10]	$O(n^{1/3}\Upsilon^{-2})$ (q)	element distinctness
[A-Sarlette '18]	$O(n^{1/2}\Upsilon^{-1})$ (q)	QFF
[A '19]	$O(n^{1/3}\Upsilon^{-1})$ (q)	QFF and seed sets