Quantum-walk-based search algorithms on Johnson graphs

Hajime Tanaka

(joint work with M. Sabri, P. Lugão, and R. Portugal)

Research **C**enter for **P**ure and **A**pplied **M**athematics
Graduate **S**chool of **I**nformation **S**ciences
Tohoku University

April 25, 2024

2nd International Conference on Graph Theory and Combinatorics

De La Salle University

How I started this work

- I am a researcher specializing in **distance-regular graphs** and **association schemes**.
- Etsuo Segawa (a specialist in quantum walks) invited Portugal to Tohoku U in Jan–Feb 2018, and Portugal gave lectures on quantum-walk-based search algorithms.
- Sabri was a student of Segawa and became my Ph.D. student in Sep 2019.

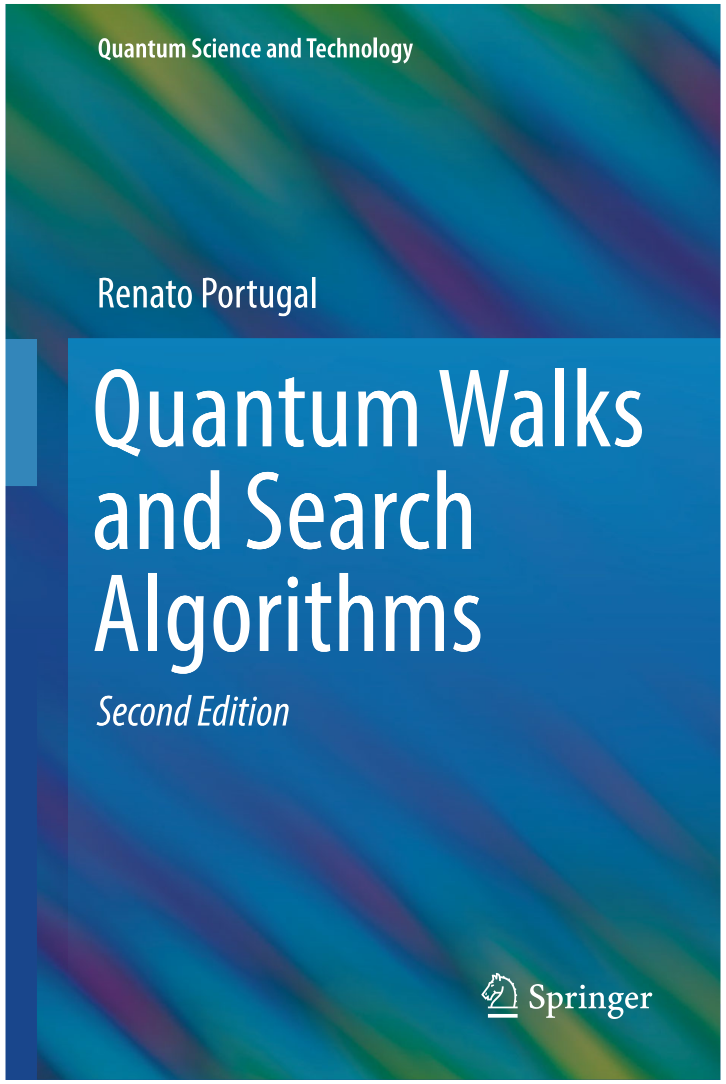
$\Longrightarrow$ I started studying quantum walks.

Reference

Renato Portugal

Quantum Walks and Search Algorithms (2nd edition)

Springer, Cham, 2018.



Some postulates in quantum physics

- a quantum system $\longleftrightarrow$ $\mathscr{H}$: a Hilbert space
- a state of the system $\longleftrightarrow$ $|v\rangle \in \mathscr{H}$ s.t. $\| |v\rangle \| = 1$

Remark. The "ket" symbol $|\cdot\rangle$ is used to mean vectors in $\mathscr{H}$. The inner product of $|u\rangle, |v\rangle \in \mathscr{H}$ is denoted $\langle u | v \rangle$. linear

antilinear

- an evolution of the system $\longleftrightarrow$ $U|v\rangle$ unitary operator
- a (projective) measurement $\longleftrightarrow$ $\{|\phi_\ell\rangle\}_{\ell=1}^n$: an ONB of $\mathscr{H}$

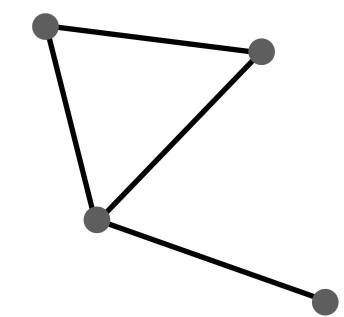
Remark. The outcome of the measurement is one of $1, 2, \ldots, n$. The probability that the outcome is ℓ is $|\langle \phi_\ell | v \rangle|^2$. If we get ℓ, then the state collapses to $|\phi_\ell\rangle$.

$$\sum_{\ell=1}^{n} |\langle \phi_\ell | v \rangle|^2 = \| |v\rangle \|^2 = 1$$

Set-up (continuous-time)

a set of 2-element subsets of $\mathscr{V}$

- $G = (\mathscr{V}, \mathscr{E})$: a finite simple graph, where $|\mathscr{V}| = N$
  - $\mathscr{V}$: the vertex set, where $|\mathscr{V}| = N$
  - $\mathscr{E}$: the edge set



- $\mathscr{H}_{\mathscr{V}} = \mathrm{span}\{\, |x\rangle : x \in \mathscr{V} \,\}$, where $\langle x | y \rangle = \delta_{x,y}$

- $U(t) \;\; (t \in \mathbb{R})$: unitary
- $|\psi(0)\rangle \in \mathscr{H}_{\mathscr{V}}$: the initial state

unit vector

- $|\psi(t)\rangle = U(t)|\psi(0)\rangle$: the state at time $t \in \mathbb{R}$
- $|\langle x | \psi(t)\rangle|^2$: the probability of finding x at time t

Set-up (continuous-time)

- $|\psi(t)\rangle = U(t)|\psi(0)\rangle$
- $|\langle x|\psi(t)\rangle|^2$

- A : the **adjacency matrix** :

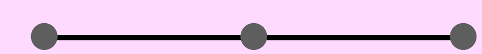
$$A_{x,y} = \begin{cases} 1 & \text{if } x \sim y \\ 0 & \text{otherwise} \end{cases} \qquad (x, y \in \mathscr{V})$$

$|\{y : x \sim y\}|$

diagonal

- D : the **degree matrix** : $D_{x,x} = \deg(x) \quad (x \in \mathscr{V})$

- $L = D - A$: the **Laplacian matrix**



$$L = \begin{bmatrix} 1 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 1 \end{bmatrix}$$

Example.

- $\gamma \in \mathbb{R}_{>0}$
- $U(t) = e^{-i\gamma Lt} \quad (t \in \mathbb{R})$

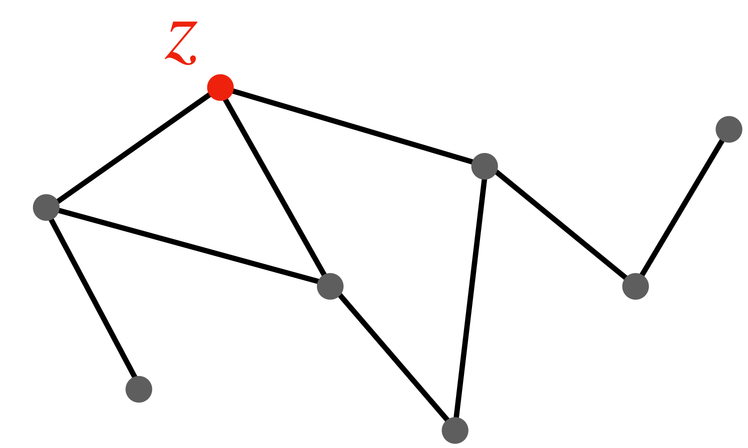
quantization of the transition matrix $e^{-\gamma Lt}$ of the continuous-time random walk with transition rate γ

Set-up (continuous-time)

- $|\psi(t)\rangle = U(t)|\psi(0)\rangle$
- $|\langle x|\psi(t)\rangle|^2$

Example.

- $\gamma \in \mathbb{R}_{>0}$
- $U(t) = e^{-i\gamma L t}$ $(t \in \mathbb{R})$



Example.

- $z \in \mathscr{V}$: a **marked vertex**
- $U'(t) = e^{-iHt}$ $(t \in \mathbb{R})$, with Hamiltonian H of the form

$$H = \gamma L - |z\rangle\langle z| \longleftarrow \text{Childs–Goldstone (2004)}$$

Problem.

Choose $|\psi(0)\rangle \in \mathscr{H}_{\mathscr{V}}$, $\gamma \in \mathbb{R}_{>0}$, $t \in \mathbb{R}_{>0}$ that maximize the finding probability $|\langle z|\psi(t)\rangle|^2$!!

$O(\sqrt{N})$

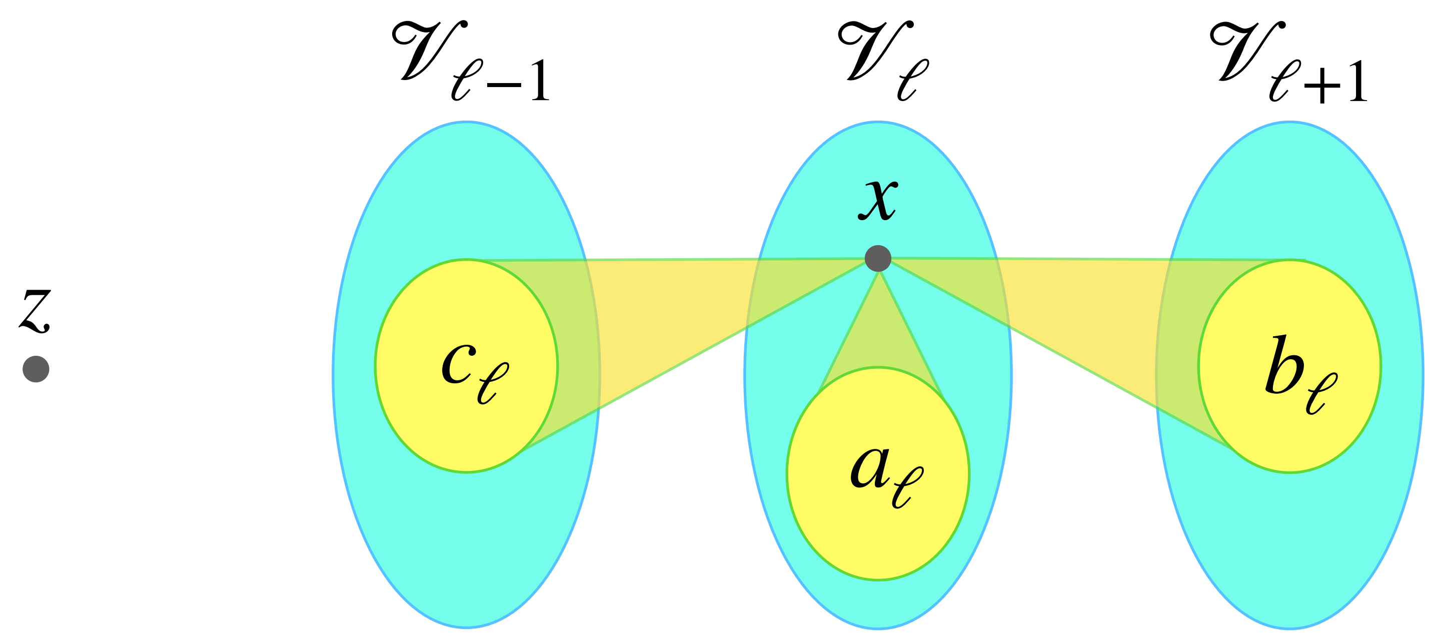
Some previous work

- complete graphs (Childs–Goldstone, 2004) ⟵ DRG
- hypercubes (Childs–Goldstone, 2004) ⟵ DRG
- Cartesian powers of cycles (Childs–Goldstone, 2004)
- strongly regular graphs (Janmark–Meyer–Wong, 2014) ⟵ DRG
- Johnson graphs with diameter 3 (Wong, 2016) ⟵ DRG
- Erdős–Renyi graphs (Chakraborty–Novo–Ambainis–Omar, 2016)

Johnson graphs

- $n, r \in \mathbb{N} \ \ (1 \leqslant r \leqslant n/2)$
- $\mathscr{V}$: the set of r-subsets of $\{1,2,\ldots,n\} \implies N = \binom{n}{r}$
- $x \sim y \overset{\text{def}}{\iff} |x \cap y| = r-1 \quad (x, y \in \mathscr{V})$
- $G = J(n,r)$

- $\mathscr{V}_\ell = \left\{x \in \mathscr{V} : |x \cap z| = r - \ell\right\} \quad (0 \leqslant \ell \leqslant r)$



$a_\ell = \ell(n-2\ell)$

$b_\ell = (r-\ell)(n-r-\ell)$

$c_\ell = \ell^2$

Search on Johnson graphs

- $H = \gamma L - |z\rangle\langle z|$
- $U(t) = e^{-iHt}$
- $|\psi(t)\rangle = U(t)|\psi(0)\rangle$

Fix r and let $n \to \infty$!!

- $|\psi(0)\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathcal{V}} |x\rangle \in \mathcal{H}_{\mathcal{V}}$: the **uniform superposition**

(T.–Sabri–Portugal, '22)

Theorem. We can choose appropriate $\gamma = \gamma(n, r) > 0$ s.t.

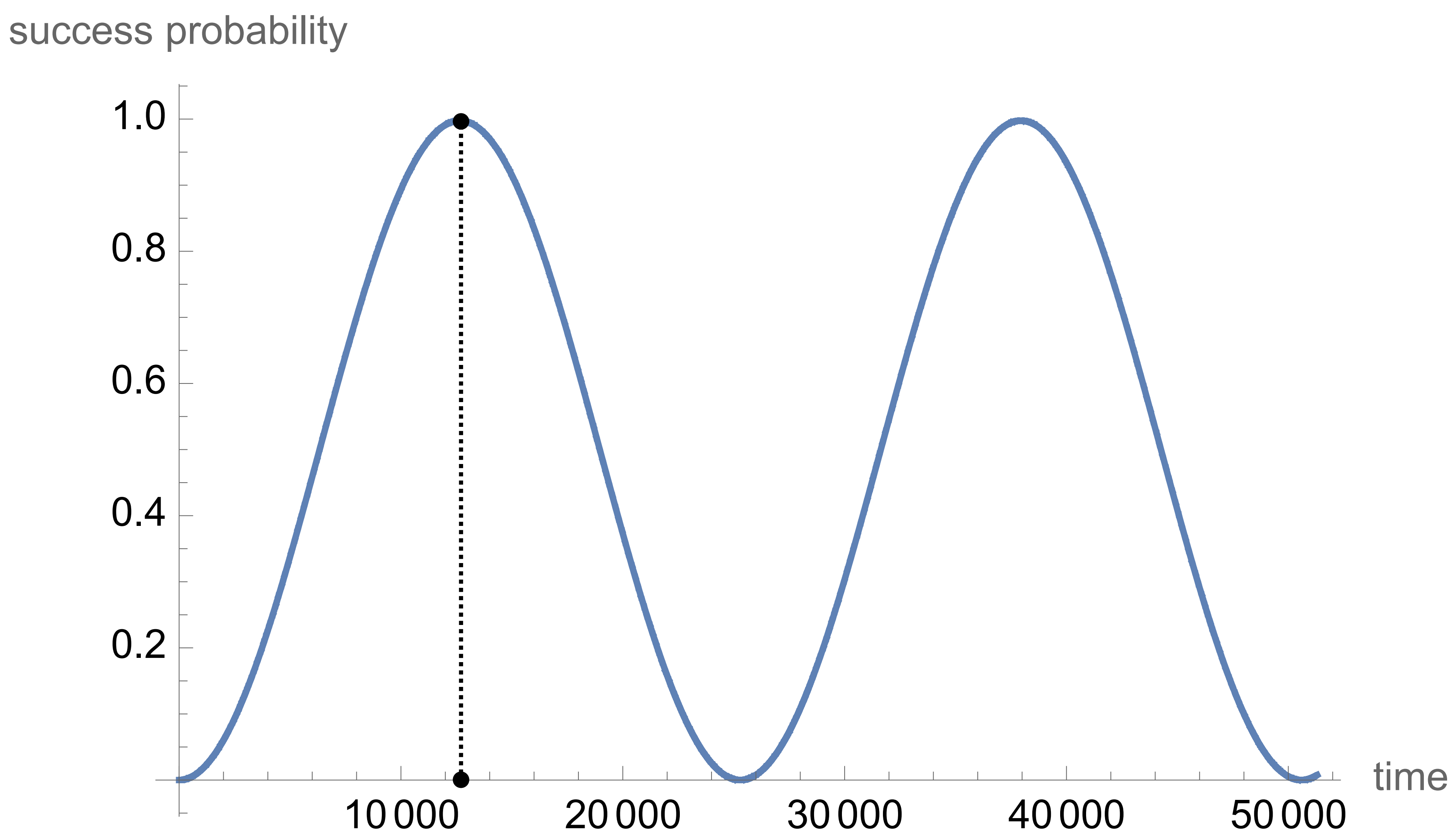
$$|\langle z|\psi(t_{\mathrm{opt}})\rangle|^2 = 1 + o(1) \quad (n \to \infty),$$

where

$$t_{\mathrm{opt}} = \frac{\pi n^{r/2}}{2\sqrt{r!}} \approx \frac{\pi\sqrt{N}}{2}.$$

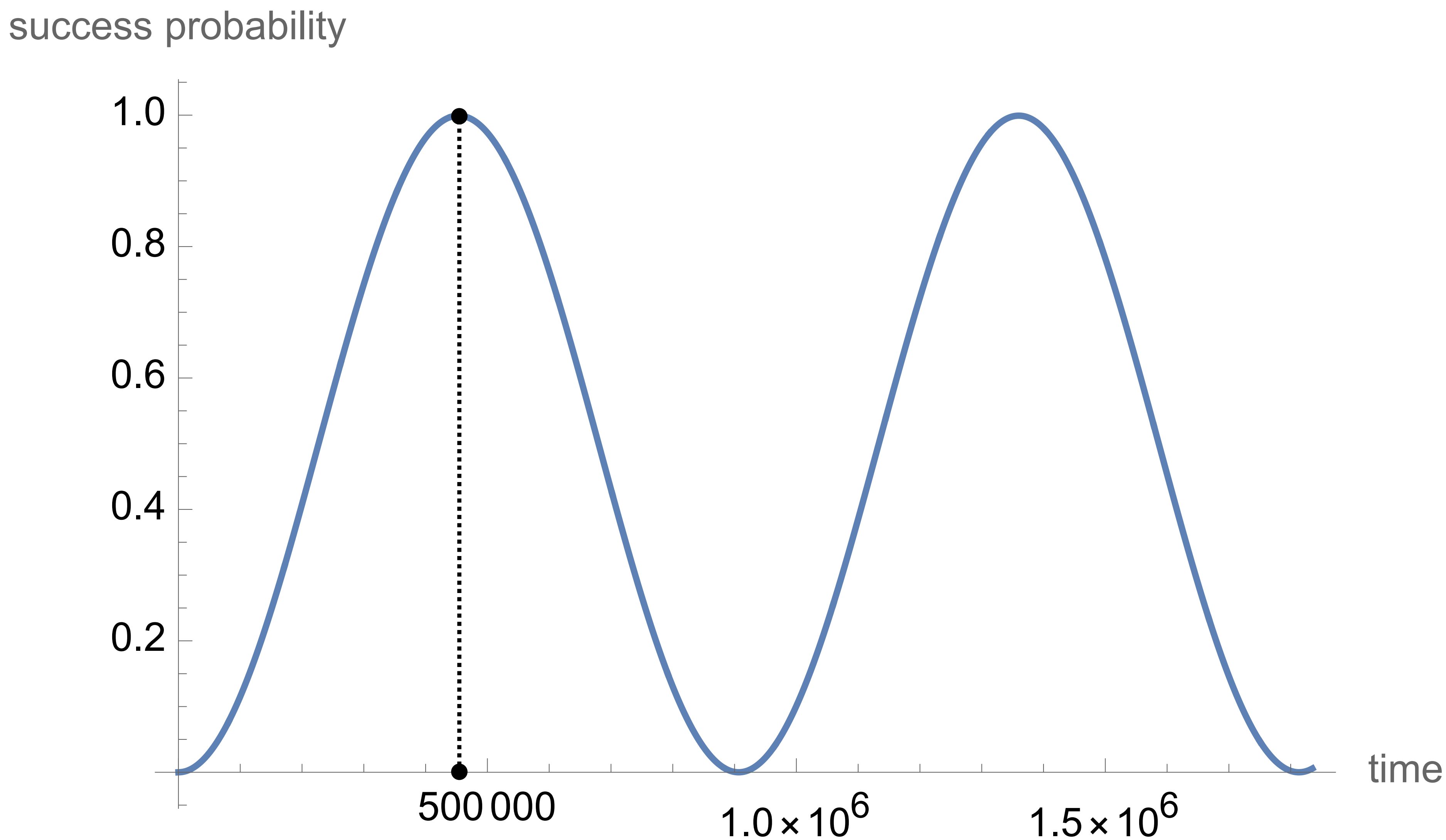
Example $(r = 4, n = 200)$.

- $$t_{\text{opt}} = \frac{\pi n^{r/2}}{2\sqrt{r!}} \approx 12{,}825.5$$



Example ($r = 5, n = 400$).

- $t_{\text{opt}} = \dfrac{\pi n^{r/2}}{2\sqrt{r!}} \approx 458{,}859$



Comments

$$\frac{\epsilon^2}{3} + \frac{7\epsilon^4}{6} + O(\epsilon^6)$$

- $\gamma = \gamma(n, r)$ is given as a function of $\epsilon = 1/\sqrt{n}$ as follows:

$$r = 3: \quad \frac{\epsilon^2(1-3\epsilon^2)(2+\epsilon^2+16\epsilon^4-52\epsilon^6+24\epsilon^8)}{6(1-\epsilon^2)^2(1-2\epsilon^2)^2}$$

$$r = 4: \quad \frac{\epsilon^2(1-4\epsilon^2)(3-11\epsilon^2+33\epsilon^4+47\epsilon^6-660\epsilon^8+1116\epsilon^{10}-432\epsilon^{12})}{12(1-\epsilon^2)^2(1-2\epsilon^2)^2(1-3\epsilon^2)^2}$$

$$r = 5: \quad \frac{\epsilon^2(1-5\epsilon^2)(12-117\epsilon^2+532\epsilon^4-1107\epsilon^6+2508\epsilon^8-22588\epsilon^{10}+80448\epsilon^{12}-99648\epsilon^{14}+34560\epsilon^{16})}{60(1-\epsilon^2)^2(1-2\epsilon^2)^2(1-3\epsilon^2)^2(1-4\epsilon^2)^2}$$

- Wong (2016) used $\gamma = \dfrac{\epsilon^2}{3} + \dfrac{7\epsilon^4}{6}$ in his algorithm for $J(n,3)$.

Set-up (discrete-time)

- $G = (\mathscr{V}, \mathscr{E})$: a finite simple graph, where $|\mathscr{V}| = N$
- $\mathscr{A} = \left\{ a = (x, y) : x, y \in \mathscr{V}, x \sim y \right\}$ arc set

  head

  tail
- $\mathscr{H}_{\mathscr{A}} = \mathrm{span}\{ |a\rangle : a \in \mathscr{A} \}$, where $\langle a | b \rangle = \delta_{a,b}$
- S : the **shift operator** on $\mathscr{H}_{\mathscr{A}}$

  opposite arc of a

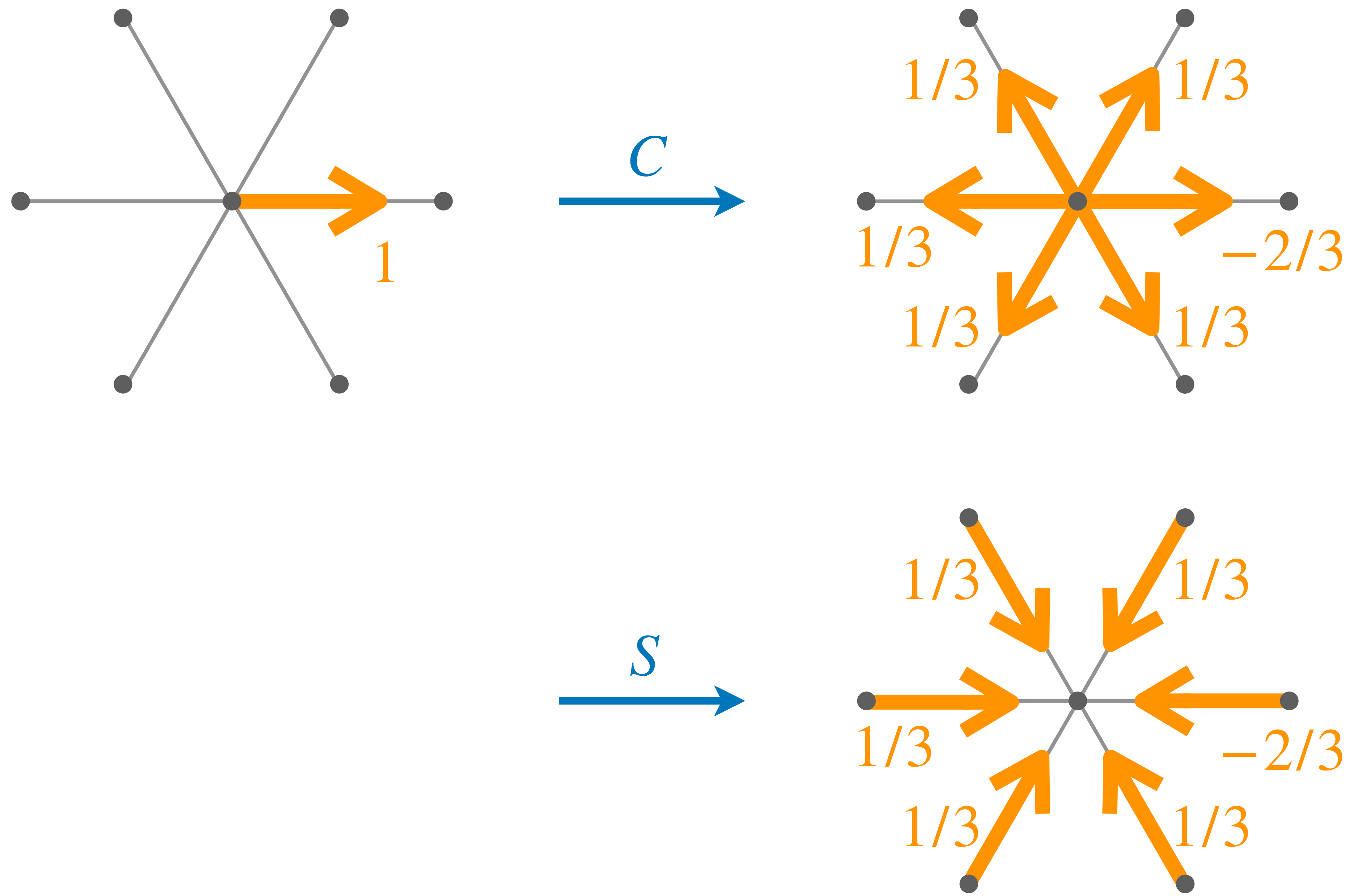
$$S|a\rangle = |\bar{a}\rangle$$

- C : the **Grover coin operator** on $\mathscr{H}_{\mathscr{A}}$

$$C|a\rangle = \frac{2}{\deg(\mathrm{tail}(a))} \sum_{\mathrm{tail}(b)=\mathrm{tail}(a)} |b\rangle - |a\rangle$$

Set-up (discrete-time)

- $U = SC$: the **evolution operator** on $\mathscr{H}_{\mathscr{A}}$



Set-up (discrete-time)

$U = SC$

unit vector

- $|\psi(0)\rangle \in \mathscr{H}_{\mathscr{A}}$: the initial state
- $|\psi(t)\rangle = U^t|\psi(0)\rangle$: the state at time $t \in \mathbb{N}$
- $\sum_{\substack{\mathrm{tail}(a)=x \\ \text{or} \\ \mathrm{head}(a)=x}} |\langle a|\psi(t)\rangle|^2$: the probability of finding x at time t

marked vertex

- R : the **oracle** for z on $\mathscr{H}_{\mathscr{A}}$:

$$R|a\rangle = \begin{cases} -|a\rangle & \text{if } \mathrm{tail}(a) = z, \\ |a\rangle & \text{otherwise}, \end{cases} \qquad (a \in \mathscr{A}).$$

- $U' = UR$: the **modified evolution operator** on $\mathscr{H}_{\mathscr{A}}$

Some previous work

- complete graphs (Grover, 1996) ⟵ DRG
- hypercubes (Shenvi–Kempe–Whaley, 2003) ⟵ DRG
- finite two-dimensional lattices (Tulsi, 2008)
- Johnson graphs with diameter 3 (Xue–Ruan–Liu, 2019) ⟵ DRG

Search on Johnson graphs

- $U = SC$
- $U' = UR$

Fix r and let $n \to \infty$!!

- $$|\psi(0)\rangle = \frac{1}{\sqrt{|\mathscr{A}|}} \sum_{a \in \mathscr{A}} |a\rangle \in \mathscr{H}_{\mathscr{A}}$$

(T.–Sabri–Portugal, '22)

Theorem. We have

$$\sum_{\substack{\mathrm{tail}(a) = z \\ \text{or} \\ \mathrm{head}(a) = z}} |\langle a | \psi(t_{\mathrm{opt}})\rangle|^2 = 1 + o(1) \quad (n \to \infty),$$

where

$$t_{\mathrm{opt}} = \left\lfloor \frac{\pi n^{r/2}}{2\sqrt{2r!}} \right\rfloor \approx \frac{\pi \sqrt{N}}{2\sqrt{2}}.$$

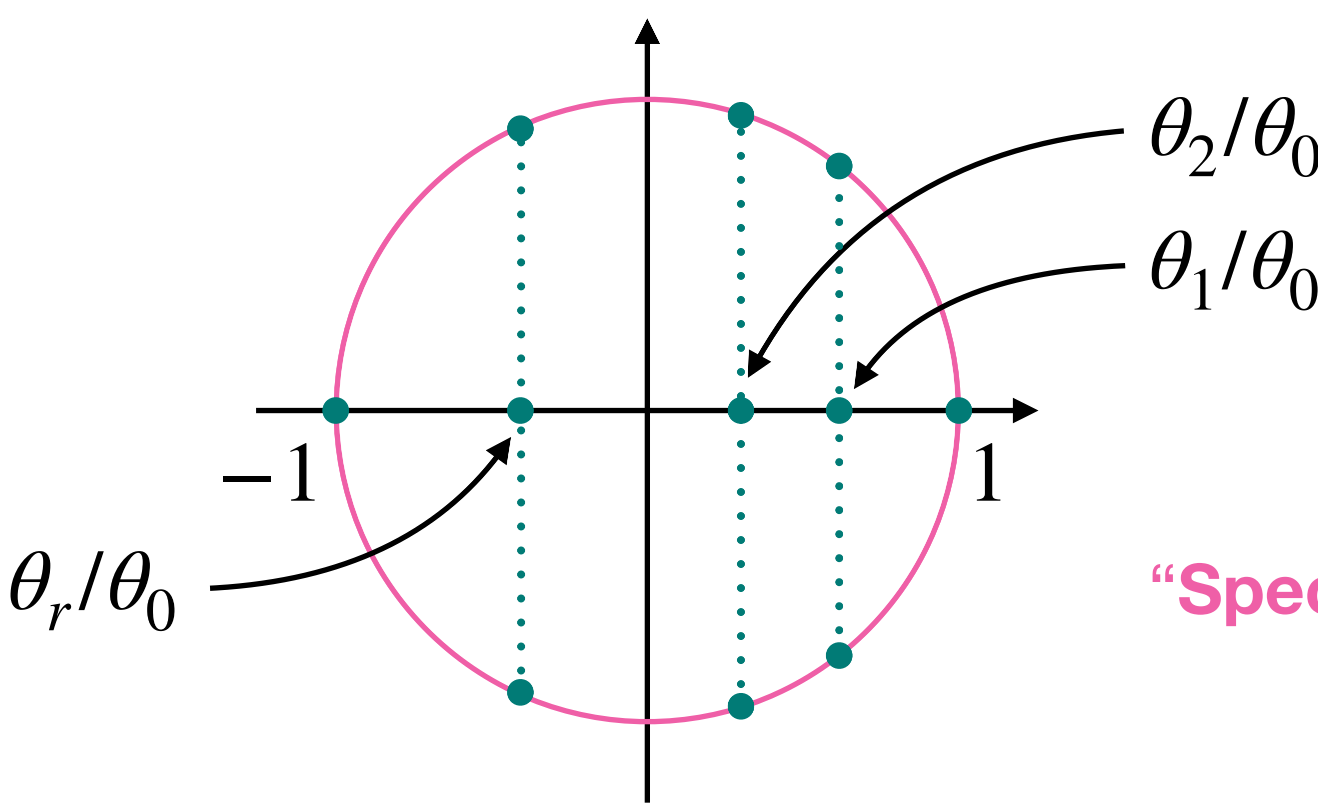
Comments

- $J(n, r)$ has $r+1$ $\underbrace{\text{distinct eigenvalues}}^{\text{adjacency}}$ $\theta_0 > \theta_1 > \cdots > \theta_r$:

$$\theta_\ell = (r-\ell)(n-r-\ell) - \ell \quad (0 \leqslant \ell \leqslant r).$$

- The eigenvalues of U are $\pm 1, \mathrm{e}^{\pm i\omega_1}, \ldots, \mathrm{e}^{\pm i\omega_r}$, where

$$\omega_\ell = \arccos\left(\frac{\theta_\ell}{\theta_0}\right) \quad (1 \leqslant \ell \leqslant r).$$



"Spectral Mapping Theorem"

The element k-distinctness problem

Given a sequence of data of length n

$$a_1, a_2, a_3, \ldots, a_{i_1}, \ldots, a_{i_2}, \ldots\ldots, a_{i_k}, \ldots, a_n,$$

find if it contains k identical entries!

a k**-collision**

- Classically, we need $\Omega(n)$ queries.
- Ambainis ('07) found a quantum-walk-based algorithm with $O(n^{k/(k+1)})$ queries. ← optimal when $k = 2$
- Belovs ('12) improved this to $O(n^{1-2^{k-2}/(2^k-1)})$.

Ambainis' algorithm

- The main part of Ambainis' algorithm handles the following case:

Assumption. The sequence $a_1, a_2, \ldots, a_n$ contains precisely one k-collision, denoted $K = \{i_1, i_2, \ldots, i_k\}$.

- Ambainis considered the following graph:

$r = \lfloor n^{k/(k+1)} \rfloor$

$$\text{vertex set}: \left\{ (x, y) : \begin{array}{c} x, y \subset \{1,2,\ldots,n\},\ x \subset y \\ |x| = r,\ |y| = r+1 \end{array} \right\}$$

$$\text{adjacency}: (x, y) \sim (x', y') \iff x = x' \text{ or } y = y'$$

- Ambainis used a **staggered quantum walk** on this graph to find a vertex (x, y) such that $K \subset x$.

Our algorithm

Rebuild the main part of Ambainis' algorithm using a better graph and a simpler quantum walk!

- We use the Johnson graph $J(n, r)$ and the Grover quantum walk on it.

$r = \lfloor n^{k/(k+1)} \rfloor$ $U = SC$

- $|\psi(0)\rangle = \dfrac{1}{\sqrt{|\mathscr{A}|}} \sum_{a \in \mathscr{A}} |a\rangle \in \mathscr{H}_{\mathscr{A}}$

- R : the **oracle** on $\mathscr{H}_{\mathscr{A}}$:

$$R|a\rangle = \begin{cases} -|a\rangle & \text{if } K \subset \mathrm{tail}(a), \mathrm{head}(a), \\ |a\rangle & \text{otherwise}, \end{cases} \qquad (a \in \mathscr{A}).$$

Our algorithm

$s \in \mathbb{N}$: fixed

- $U' = U^s R$: the **modified evolution operator** on $\mathscr{H}_{\mathscr{A}}$
- $|\psi(t)\rangle = (U')^t |\psi(0)\rangle$: the state at time $t \in \mathbb{N}$
- $\displaystyle\sum_{\substack{K \subset \mathrm{tail}(a) \\ \text{or} \\ K \subset \mathrm{head}(a)}} |\langle a | \psi(t)\rangle|^2$: the probability of finding K at time t

$=: p_{\mathrm{succ}}(t)$

Theorem. $p_{\mathrm{succ}}(t_{\mathrm{opt}}) = 1 + o(1) \ (n \to \infty)$ when $s = s_{\mathrm{opt}}$, where

$$s_{\mathrm{opt}} = 2\left\lfloor \frac{\pi}{2\arccos\left(\theta_k/\theta_0\right)} \right\rfloor + 1, \quad t_{\mathrm{opt}} = \left\lfloor \frac{\pi n^{k/2}}{4 r^{k/2}} \right\rfloor.$$

Remark. $\displaystyle s_{\mathrm{opt}} t_{\mathrm{opt}} \approx \frac{\pi^2 n^{k/(k+1)}}{4\sqrt{2k}}.$ ← related to # of queries !!