The element distinctness problem revisited

Hajime Tanaka

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

August 21, 2023

Recent topics on generalized orthogonal polynomials and their applications

ICIAM 2023 TOKYO

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:

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

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

$$\text{adjacency}: (S,T) \sim (S',T') \iff S = S' \text{ or } T = T'$$

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

The goal

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

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

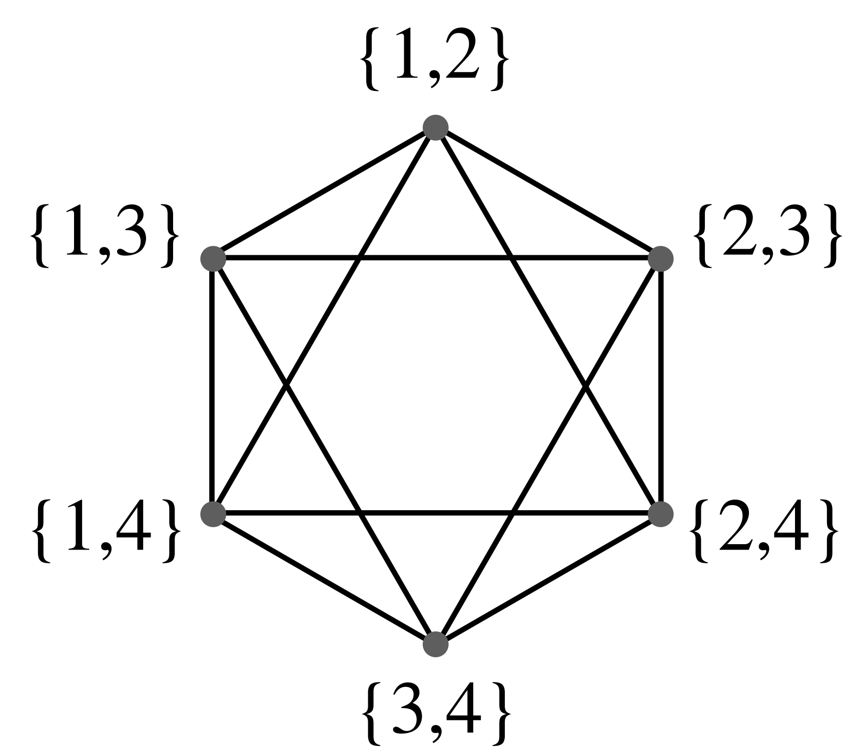
- We use the **Johnson graph** $J(n, r)$:

vertex set : $\{S : S \subset \{1,2,\ldots,n\},\ |S| = r\}$

adjacency : $S \sim S' \iff |S \cap S'| = r - 1$

distance-regular

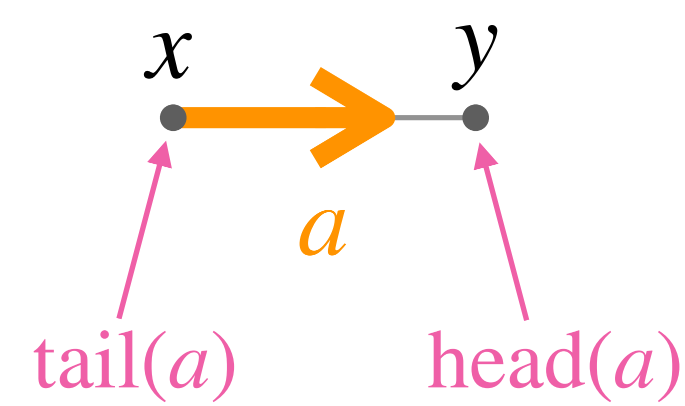
$n = 4, r = 2:$



The Grover quantum walk on a graph

- Γ : a finite simple graph with vertex set V
- D : the set of **arcs** (or directed edges) in Γ:

$$D = \{a = (x, y) : x, y \in V,\ x \sim y\}$$



- For $a = (x, y) \in D$, let

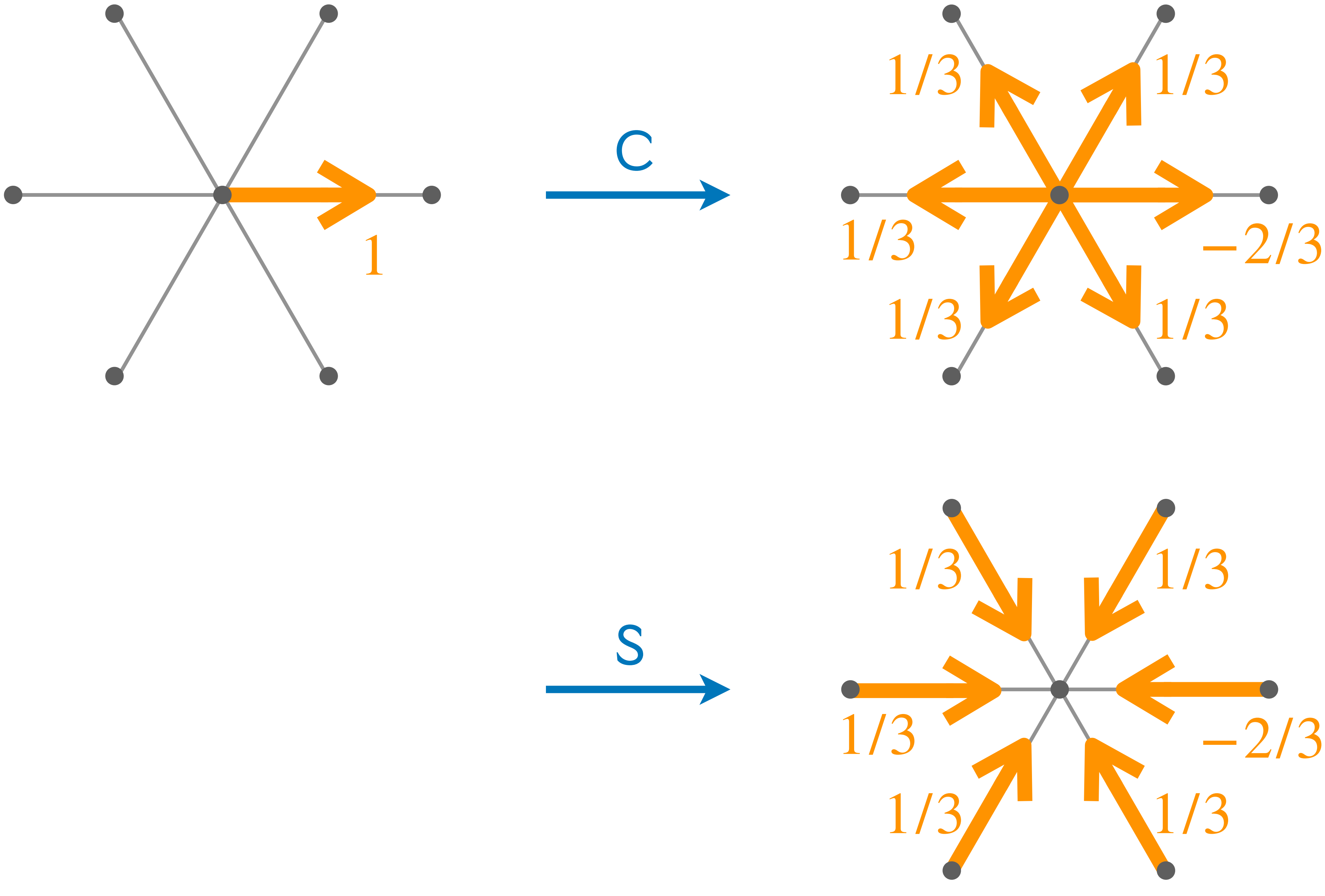
$$\mathrm{tail}(a) = x,\ \ \mathrm{head}(a) = y,\ \ \bar{a} = (y, x).$$

- $\mathscr{H}_D = \mathrm{span}\{\,|\,a\rangle : a \in D\}$, where $\langle a\,|\,b\rangle = \delta_{a,b}$
- S : the **shift operator** on $\mathscr{H}_D$: $\mathsf{S}\,|\,a\rangle = |\,\bar{a}\rangle$
- C : the **Grover coin operator** on $\mathscr{H}_D$:

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

The Grover quantum walk on a graph

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



Our algorithm

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

- Let $\Gamma = J(n, r)$.
- R : an **oracle** on $\mathscr{H}_D$:

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

- $|\sigma\rangle = |D|^{-1/2} \sum_{a \in D} |a\rangle$: the initial state
- $|\tau\rangle = (\mathrm{U}^{t_2}\mathrm{R})^{t_1}|\sigma\rangle$, where $t_1 = \left\lfloor \frac{\pi\sqrt{r}}{4} \right\rfloor$, $t_2 = 2\left\lfloor \frac{\pi\sqrt{r}}{2\sqrt{2k}} \right\rfloor + 1$
- $p_{\mathrm{succ}} = \sum_{\substack{a \in D \\ K \subset \mathrm{tail}(a), \mathrm{head}(a)}} |\langle a|\tau\rangle|^2$: the success probability

Theorem. We have $p_{\mathrm{succ}} = 1 + o(1)\ \ (n \to \infty)$.

How orthogonal polynomials play a role

Terwilliger ('01)

- A pair $A, A^* \in \mathrm{End}_{\mathbb{C}}(\mathbb{C}^{d+1})$ is a **Leonard pair** if:

  ① There is an ordered eigenbasis of A for which A^* is irreducible tridiagonal.

  ② There is an ordered eigenbasis of A^* for which A is irreducible tridiagonal.

nonzero superdiagonal/subdiagonal entries

Fact. Leonard pairs characterize the terminating branch of the **Askey scheme** consisting of q-Racah, q-Hahn, dual q-Hahn, q-Krawtchouk, dual q-Krawtchouk, quantum q-Krawtchouk, affine q-Krawtchouk, Racah, Hahn, dual Hahn, Krawtchouk, and Bannai/Ito polynomials.

How orthogonal polynomials play a role

- Recall $J(n,r)$ with $V = \{S : S \subset \{1,2,\ldots,n\}, |S| = r\}$.
- Consider $\mathscr{H}_V = \mathrm{span}\{\,|S\rangle : S \in V\}$.
- Fix $S \in V$ and set $$|v_i\rangle = \sum_{\substack{S' \in V \\ |S \cap S'| = i}} |S'\rangle \quad (i = 0,1,\ldots,r).$$

Theorem (Terwilliger, '91)**.** The linear span of the $|v_i\rangle$ affords a Leonard pair, one of whose operators is the adjacency operator.

- Recall the k-collision $K = \{i_1, i_2, \ldots, i_k\}$.
- Set $$|u_i\rangle = \sum_{\substack{S' \in V \\ |K \cap S'| = i}} |S'\rangle \quad (i = 0,1,\ldots,k).$$

Theorem (T., '11)**.** The linear span of the $|u_i\rangle$ affords $\cdots$.

An orthogonality for dual Hahn polynomials

- Recall the **dual Hahn polynomials**:

$$R_i(\lambda(j);\gamma,\delta,N) = {}_3F_2\left(\begin{matrix} -i, -j, j+\gamma+\delta+1 \\ \gamma+1, -N \end{matrix} \middle| 1\right)$$

for $i = 0,1,\ldots,N$, where $\lambda(j) = j(j+\gamma+\delta+1)$.

Fact. The polynomials associated with the $|v_i\rangle$ are the dual Hahn polynomials with $N = r$, $\gamma = r - n - 1$, $\delta = -r-1$.

Theorem (T., '09, '11)**.** The polynomials associated with the $|u_i\rangle$ are the dual Hahn polynomials with $N = k$ and the same γ, δ:

$$\sum_{j=0}^{k} \frac{(2j+\gamma+\delta+1)(\gamma+1)_j(-k)_j k!}{(-1)^j(j+\gamma+\delta+1)_{k+1}(\delta+1)_j j!} R_i(\lambda(j);r)R_\ell(\lambda(j);k) = 0$$

if $i < \ell$ or $i > \ell + r - k$.