BAD HONNEF LECTURE 2

"QUANTUM WALKS"

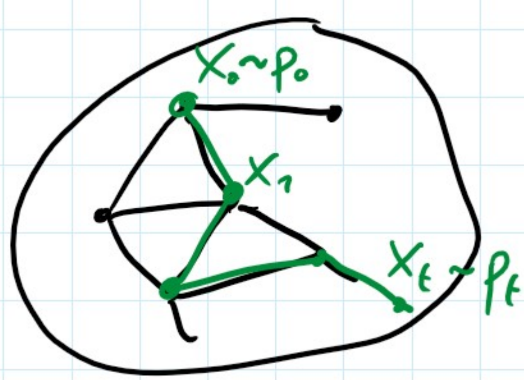
= quantum analogue of

RANDOM WALKS.

graph $G = (V, E)$ — d-regular

random walk $(X_t)_{t \geq 0}$

stochastic transition matrix P



s.t. if $X_0 \sim p_0 \in \mathbb{R}^n$ $\quad$ $\left(P_{ij} = \frac{1}{d} \text{ if } (i,j) \in E \right.$ $= 0$ o/w

then $X_t \sim p_t = P^t p_0$

If G irreducible & nonbipartite,

then $p_t \xrightarrow{t \to \infty} \pi$, $\forall p_0$

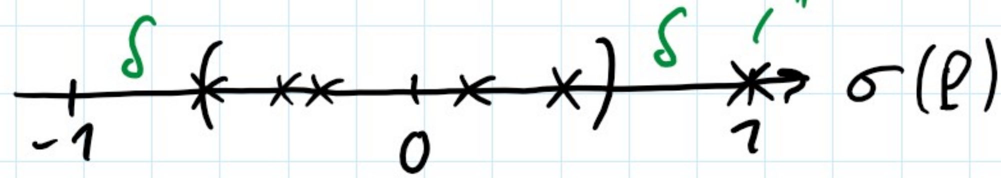
π: uniform

= "stationary distribution"

↳ convergence rate or "mixing time"

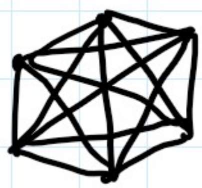
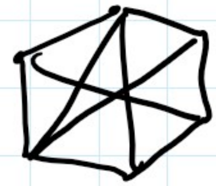
$\sim \frac{1}{\delta}$,

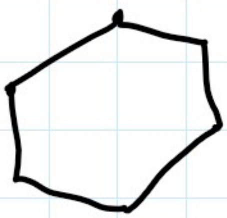
δ = "spectral gap" of P



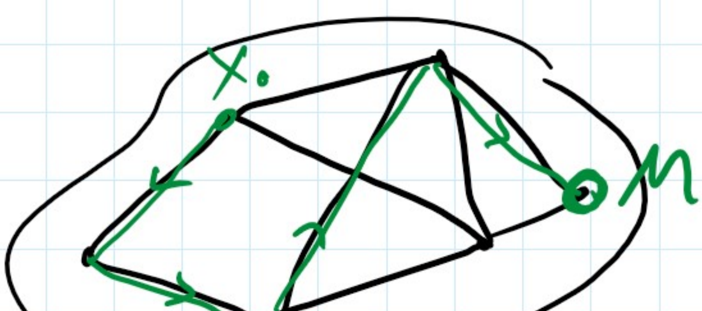
e.g., random graph

e.g., complete graph / expander : $\delta \sim 1$

 cycle : $\delta \sim 1/n^2$

dual quantity: "hitting time"



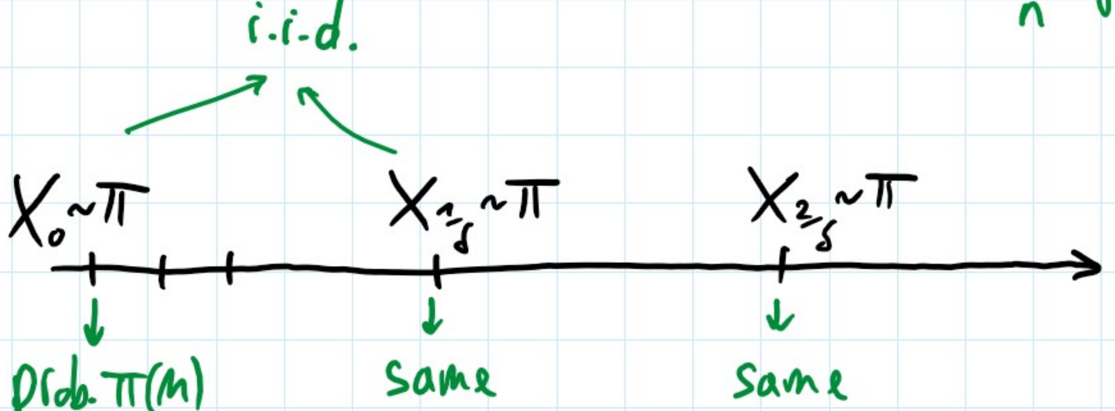
$$\tau_M = \min\{t \mid X_t \in M, X_0 \sim \pi\}$$

$$\boxed{HT_m = \mathbb{E}[\tau_m]}$$

e.g., complete graph: $HT_m \in O\left(\frac{n}{|M|}\right)$

LEMMA: $$\boxed{HT_m \in O\left(\frac{1}{\delta}\,\frac{1}{\pi(M)}\right)}$$

$\frac{|M|}{n}$ for regular graph



$$\text{"COST"} = S + \frac{n}{|M|}\left(C + \frac{1}{\delta}U\right)$$

$|M|$

setup:
sample $X_0 \sim \pi$

checking:
is $x \in M$?

update:
1 RW step

QUANTUM WALK SEARCH:

= Grover search with quantum walks

→ recall Grover:

initial state

$$|\pi\rangle = \frac{1}{\sqrt{n}} \sum |x\rangle$$

Grover iteration

$$(2\Pi_M - \mathbb{1})(2|\pi\rangle\langle\pi| - \mathbb{1})$$

reflect around marked states

reflect around initial state

Finds marked element after $O\left(\sqrt{\frac{n}{|M|}}\right)$ iterations

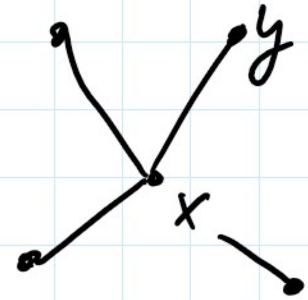
$$\mathrm{COST} = S + \sqrt{\frac{n}{|M|}}\left(\overbrace{C + R_\pi}^{\text{cost per iteration}}\right)$$

"setup" $|\pi\rangle$

"setup" $|\pi\rangle$

use quantum walks

QUANTUM WALKS



recall RW:

$$p_0 = e_x \longrightarrow P p_0 = \frac{1}{d} \sum_{y \sim x} e_y$$

QW: many definitions!

here, block encoding of RW operator P.

$\hookrightarrow$ define

0

- "row oracle" V for P:

$$|\psi_0\rangle = |0\rangle|x\rangle \longrightarrow V|\psi_0\rangle = \frac{1}{\sqrt{d}}\sum_{y\sim x}\underbrace{|y\rangle}_{\text{next}}\underbrace{|x\rangle}_{\text{current}}$$

- "SWAP" operator:

$$|x\rangle|y\rangle \longrightarrow \mathrm{SWAP}|x\rangle|y\rangle = |y\rangle|x\rangle$$

Then (see exercises Tuesday)

$$V^\dagger S V = \begin{bmatrix} P & \cdot \\ \cdot & \cdot \end{bmatrix}.$$

(and $(V^\dagger S V)^2 = \mathbb{1}$)

Hence

$$\left(\begin{bmatrix} \mathbb{1} & \\ & \mathbb{1} \end{bmatrix} V^\dagger S V\right)^k = \begin{bmatrix} T_k(P) & \cdot \\ & \end{bmatrix}.$$

$$\underbrace{\left(\begin{bmatrix}\mathbb{1} & \\ & -\mathbb{1}\end{bmatrix} V^\dagger S V\right)}_{W} = \begin{bmatrix} T_k(I) & \\ \cdot & \cdot \end{bmatrix}.$$

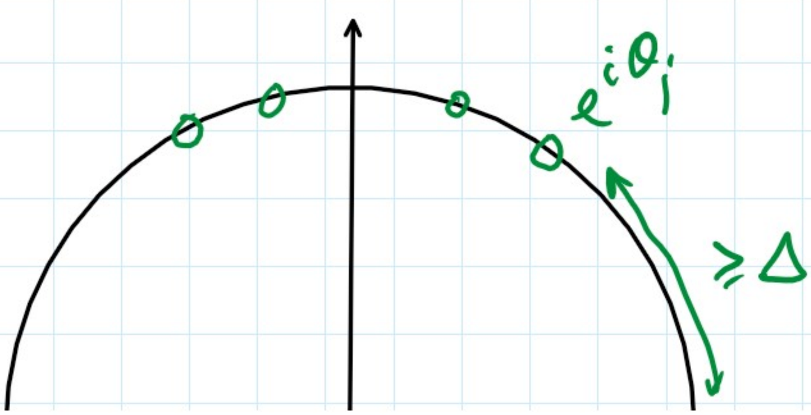
$\parallel$

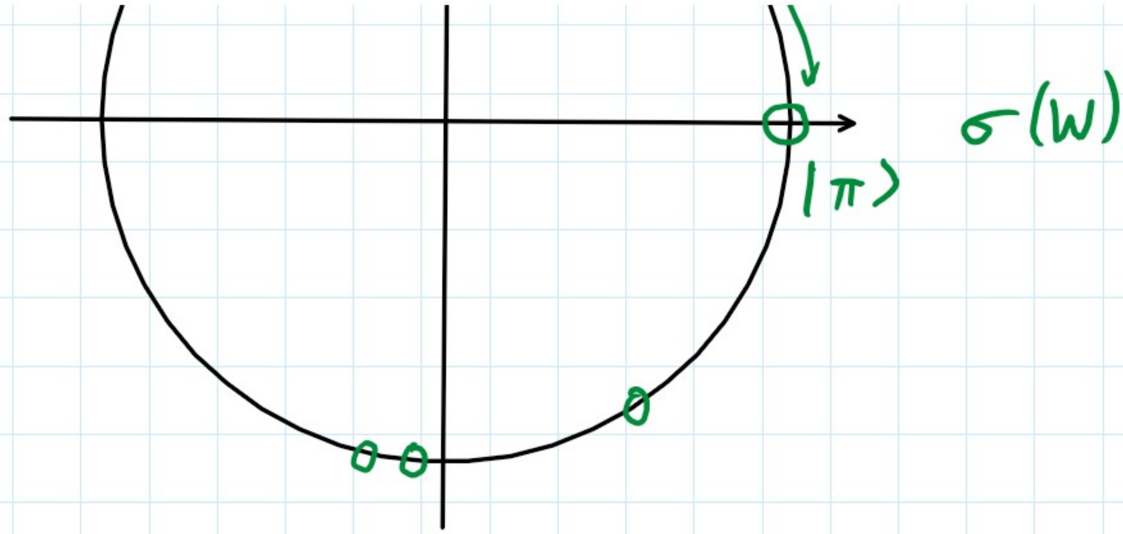
Szegedy's QW operator

= first block encoding
(also in Watrous '98)

$$\boxed{\text{Exercise: } W|0\rangle|\pi\rangle = |0\rangle|\pi\rangle.}$$

$\hookrightarrow$ $|0\rangle|\pi\rangle$ is <u>stationary</u> of QW.





! can use W to reflect around $|\pi\rangle$:

for any $|\psi\rangle \in \mathbb{C}^n$, decompose

$$|0\rangle|\psi\rangle = \alpha_0 |0\rangle|\pi\rangle + \sum_{j=1}^{n-1} \alpha_j |v_j\rangle$$

with $W|v_j\rangle = e^{i\theta_j}|v_j\rangle$, $\theta_j \geq \Delta > 0$

↳ quantum phase estimation QPE_{Δ}:
(alt.: via LCU)

$|0\rangle|\psi\rangle|0\rangle$

>0

$$|0\rangle|\psi\rangle|0\rangle$$

$$\xrightarrow{QPE_\Delta} \alpha_0|0\rangle|\pi\rangle|0\rangle + \sum \alpha_j |v_j\rangle|\tilde{\theta}_j\rangle$$

$$\xrightarrow{2\mathbb{1}\otimes\mathbb{1}\otimes|0\rangle\langle 0| - \mathbb{1}} \alpha_0|0\rangle|\pi\rangle|0\rangle - \sum \alpha_j |v_j\rangle|\tilde{\theta}_j\rangle$$

$$\xrightarrow{QPE_\Delta^{-1}} \alpha_0|0\rangle|\pi\rangle|0\rangle - \sum \alpha_j |v_j\rangle|0\rangle$$

$$= \left(\alpha_0|0\rangle|\pi\rangle - \sum \alpha_j |v_j\rangle\right)|0\rangle$$

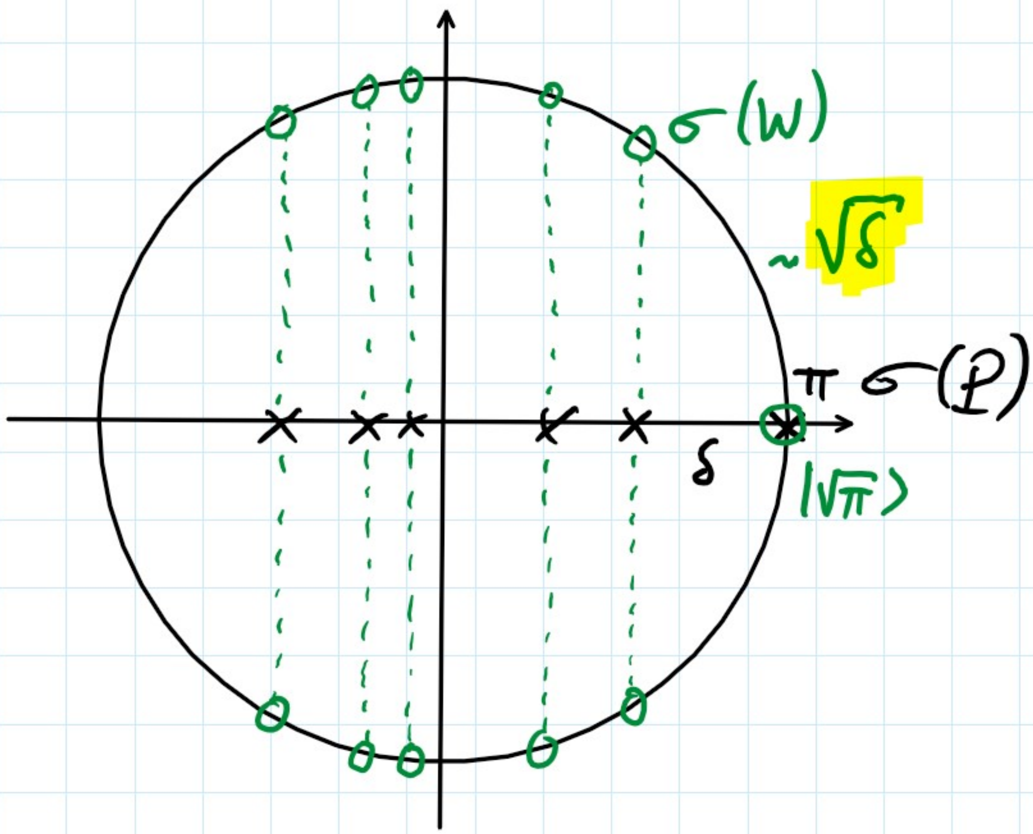
$$= \left(R_\pi |0\rangle|\psi\rangle\right)|0\rangle$$

$$\mathrm{COST}(QPE_\Delta) = 1/\Delta \text{ calls to } W$$
$$= 1/\Delta \text{ QW steps}$$

? QW gap ?

? QW gap ?

Szegedy's spectral lemma:



$$\lambda_j = \cos(\theta_j) \in \sigma(P) \rightsquigarrow e^{\pm i\theta_j} \in \sigma(W)$$

$$1-\delta \simeq \cos(\sqrt{\delta}) \rightsquigarrow e^{\pm i\sqrt{\delta}}$$

so $\boxed{\Delta \geq \sqrt{\delta}}$

and $R_\pi \sim \frac{1}{\sqrt{\delta}}$ QW steps.

↳ TOTAL COST QW SEARCH:

$$\boxed{S + \sqrt{\frac{n}{|M|}}\left(C + \frac{1}{\sqrt{\delta}}U\right)}$$

↔ RW search: $S + \frac{n}{|M|}\left(C + \frac{1}{\delta}U\right)$.

Applications:

* element distinctness, [Ambainis '04]

  collision finding / q. birthday paradox

* triangle finding, (verifying) matrix products

* quantum property testing

Quantum walks more generally:

* Markov chain Monte Carlo,

  Gibbs sampling

* backtracking algorithms

Extra: QW mixing

RW: $p_0 = e_x \longrightarrow p_t = P^t e_x$

$\approx \pi$ if $t \sim 1/\delta$

basis for MCMC.

$\boxed{\text{? mixing with QWs in } 1/\sqrt{\delta}\text{ ?}}$

! obstruction: cannot prepare $|\pi\rangle$ in $\mathrm{poly}(1/\delta)$

unlikely: implies $SZK \subseteq BQP$

GI, lattice problems

("stronger" than sampling from π

Recent approach:

we saw $W^t = \begin{bmatrix} T_t(P) & \cdot \\ \cdot & \cdot \end{bmatrix}$

? understand QW mixing

via Chebyshev polynomials ?

EXTRA:

ELEMENT DISTINCTNESS

$$\begin{cases} \text{array } x_1, x_2, \ldots, x_N \in \mathbb{Z} \\ ?\ \exists \text{ collision } (x_i = x_j) \text{ or all distinct} \end{cases}$$

Classically: $\Omega(N)$ queries

Quantum: $\tilde{O}(N^{3/4})$ with Grover

$\tilde{O}(N^{2/3})$ with QWs

↳ optimal!

QW algorithm: $Y \subseteq [N]$, $|Y| = k$ $\{x_i \mid i \in Y\}$

QW algorithm:

$Y \subseteq [N], |Y| = k$ $\{x_i \mid i \in Y\}$

graph nodes: $n = \binom{N}{k}$ pairs $y = (Y, x_Y)$,

y "marked" if x_Y contains collision

s.t.
- if all x_i's distinct: $|M|/n = 0$
- if ≥ 1 collision: $|M|/n$