Quantum Walks For Quantum Money

Jake Doliskani, Ali Mousavi
Department of Computing and Software, McMaster University

Quantum Mechanic Postulates

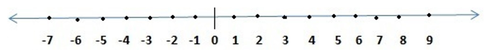
- **State Postulate**: A qubit's state can be written as
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1.$$
- **Measurement Postulate**: Measuring in the basis $\{|0\rangle, |1\rangle\}$ yields $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$.
- **Evolution Postulate**: The qubit state $|\psi(t)\rangle$ evolves according to:
$$i\hbar\frac{d}{dt}|\psi(t)\rangle = \hat{H}|\psi(t)\rangle,$$

Quantum Walks

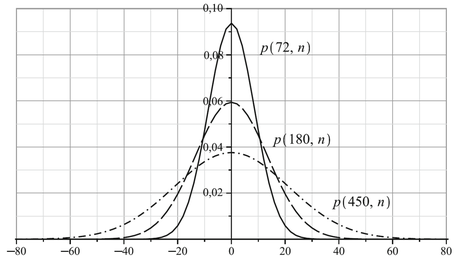
General equation:

$$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$$

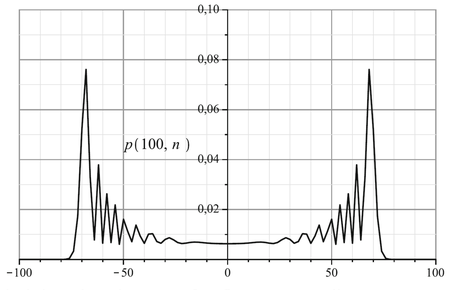
Quantum walks serve as the foundation for various quantum algorithms, providing speedups in tasks like search and graph traversal, where they outperform classical approaches.



integer axis can indeed be considered as an infinite graph



Probability distribution of a classical Random walk on integer axis

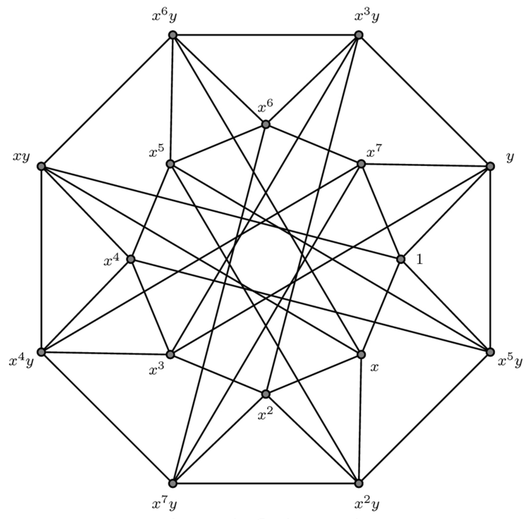


Probability distribution of a Qunatum walk on integer axis

Quantum Walk On Group Actions

- **Definition**: A group action of a group G on a set X is a way to combine each element g from G with elements x from X using an operation $*$ such that $g * x$ gives an element in X.
- **Properties**: The group action satisfies:
  Identity: The identity element e in G satisfies $e * x = x$ for all $x \in X$.
  Compatibility: For any $g, h \in G$ and $x \in X$, $(g \cdot h) * x = g * (h * x)$,
- **Importance in Cryptography**: Group actions create hard-to-reverse problems, forming the foundation for secure cryptographic protocols.

A Cayley graph is a specific example of a graph with a group action:



A sample Cayley graph

Why using Caley graphs for quantum walks?

- **Defines Movement Rules:** Cayley graphs set the structure and movement rules for quantum walks, using group elements to dictate transitions between vertices.
- **Enables Algorithm Design:** Their algebraic properties make them ideal for designing efficient quantum algorithms, like search and mixing-based algorithms.
- **Simplifies Analysis:** The group-theoretic structure aids in mathematical analysis, allowing for insights into walk behavior and performance in quantum applications.

Application: Quantum Money Verification

Quantum money is a combination of a classical value $|h\rangle$ and a quantum state $|\$\rangle$. The quantum money state is an eigenvector of the quantum walk operator. Using phase estimation, we extract the eigenvalue, which contains the money's serial number. This allows verification by checking if the extracted serial number matches the one on the money.

$$A = \sum_{k\in\mathbb{Z}_N} \lambda_k |k\rangle_F\langle k|_F$$

Where:

$$|k\rangle_F = \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}\omega_N^{ky}|y\rangle, \omega_N = e^{\frac{2\pi i}{N}}$$

is the *quantum fourier transform(QFT)*. So:

$$e^{iAt} = \sum_{k\in\mathbb{Z}_N} e^{i\lambda_k t}|k\rangle_F\langle k|_F$$

Now if we apply the continous quantum walk e^{iAt} on the *Hartly transform* $|x\rangle_H$:

$$e^{iAt}|x\rangle_H = (\sum_{k\in\mathbb{Z}_N} e^{i\lambda_k t}|k\rangle_F\langle k|_F)(\frac{1-i}{2}|x\rangle_F + \frac{1+i}{2}|-x\rangle_F)$$
$$= \frac{1-i}{2}e^{i\lambda_x t}|x\rangle_F + \frac{1+i}{2}e^{i\lambda_{-x} t}|x\rangle_F = e^{i\lambda_x t}|x\rangle_H$$

Thus, the quantum money state is the eigenvector of our quantum walk operator. Therefore, For obtaining the value h (serial number) we can perform a *phase estimation* on the quantum walk operator e^{iAt}.

References

1 Zhandry, M., 2023. Quantum money from abelian group actions. arXiv preprint arXiv:2307.12120.
2 Childs, A. M. (2009). On the relationship between continuous- and discrete-time quantum walks. arXiv preprint arXiv:0810.0312.
3 Farhi, E., Gosset, D., Hassidim, A., Lutomirski, A. and Shor, P., 2012, January. Quantum money from knots. In Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (pp. 276-289).