Quantum Walks and Application to Quantum Money

Jake Doliskani* and Seyed Ali Mousavi†

Department of Computing and Software, McMaster University

*jake.doliskani@mcmaster.ca

†mousas26@mcmaster.ca

1 Introduction to Quantum Computation

Introduction

Quantum computing is a revolutionary field that combines quantum mechanics and information theory to redefine computation and information processing. In the latter part of the 20th century, scientists explored the fusion of quantum mechanics and information theory, leading to the birth of quantum information science. This field challenges the classical view of computation by introducing novel concepts like quantum bits (qubits), entanglement, and quantum superposition, which have enabled new algorithms and protocols that outpace their classical counterparts in specific tasks. Classical computers are grounded in bits, which take binary values (0 or 1). Quantum computing introduces the qubit, a fundamental unit of quantum information that can exist in a superposition of states, such as 0 and 1 simultaneously. This foundational difference enables quantum computers to process information in fundamentally new ways. Unlike technologies like DNA computing or optical computing, which describe changes in the physical substrate while retaining classical computational principles, quantum computing changes the computational paradigm itself. A quantum computer uses the principles of quantum mechanics, such as superposition and entanglement, rather than classical mechanics, to process information. In the 1980s, pioneers like Richard Feynman and David Deutsch recognized that certain quantum phenomena could not be efficiently simulated on classical computers. These insights led to the exploration of quantum Turing machines and quantum circuit models, which provided a theoretical framework for quantum computing. The discovery of quantum gates and their role in quantum algorithms formalized the field.

Early quantum algorithms demonstrated that quantum computing could solve certain problems more efficiently than classical methods. Notably, in 1994, Peter Shor introduced a polynomial-time quantum algorithm for integer factorization, which threatened classical cryptographic protocols relying on the difficulty of factoring large integers. Entanglement, a uniquely quantum phenomenon, allows particles to exhibit correlations that defy classical explanation. This property is crucial for many quantum algorithms and protocols, as it enables quantum computers to process and store information in a way that classical computers cannot. Two notable algorithms underscore the potential of quantum computing: Shor's Algorithm, which efficiently factors integers, undermining RSA encryption and other cryptographic systems based on the hardness of factoring, and Grover's Algorithm, which provides a quadratic speedup for unstructured search problems, such as searching an unsorted database. These algorithms exemplify the theoretical advantages of quantum computing over classical approaches, even though practical implementations remain challenging.

Quantum systems are fragile and susceptible to decoherence, where quantum states lose their coherence due to interactions with the environment. This makes maintaining quantum states for computation a significant challenge. Quantum error correction methods were developed to address decoherence and other quantum noise. The breakthrough work of Shor and Steane in the mid-1990s introduced error-correction codes that allowed reliable computation despite quantum noise. Building scalable quantum computers requires advances in hardware and experimental techniques. As of now, only small-scale quantum systems with a few qubits have been implemented successfully in laboratories. Quantum computing does not offer universal speedups for all problems. For example, Grover's algorithm provides only a quadratic speedup for unstructured search, and certain problems remain equally challenging for both quantum and classical computers.

Quantum key distribution protocols, like BB84 and Ekert's protocol, offer provably secure methods for communication based on the principles of quantum mechanics. Unlike classical cryptography, which relies on computational assumptions, quantum cryptography guarantees security through physical principles. The quantum perspective has provided new insights into classical

computing and inspired novel classical algorithms. It has also advanced simulation techniques for quantum systems, benefiting fields like material science and chemistry. Quantum information processing has deepened our understanding of quantum mechanics, shedding light on foundational questions about quantum measurement and entanglement. For example, experiments testing Bell's inequalities have confirmed the non-classical correlations predicted by quantum theory.

While practical quantum computing is still in its infancy, significant progress has been made. Quantum hardware companies like IBM, Google, and Rigetti have developed small-scale quantum processors capable of performing limited computations. Platforms such as Qiskit and Cirq enable researchers to experiment with quantum programming and algorithm development. Efforts to build scalable, fault-tolerant quantum computers are ongoing, alongside investigations into alternative models of quantum computation, such as topological and cluster-state quantum computing. Despite these advances, many open questions remain about the scope and ultimate power of quantum computation. While quantum computers will not replace classical ones for all tasks, they promise to revolutionize fields where their unique capabilities provide exponential speedups or new forms of computation.

Quantum computing represents a profound shift in how we understand and leverage computation. By replacing classical mechanics with quantum mechanics as the foundation for processing information, quantum computing has opened new avenues for scientific discovery and technological innovation. While challenges persist, the theoretical and experimental advances made thus far underscore the transformative potential of this exciting field.

Foundations of Quantum Computation

Understanding a Qubit

A qubit (quantum bit) is the fundamental unit of quantum information, analogous to a classical bit. However, unlike a classical bit, which can only exist in one of two definite states (0 or 1), a qubit can exist in a linear combination, or superposition, of both states simultaneously. Mathematically, the state of a single qubit is represented as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

Here:

- $|0\rangle$ and $|1\rangle$ are the basis states (analogous to 0 and 1 in classical computing).
- α and β are complex numbers known as probability amplitudes.

The normalization condition $|\alpha|^2 + |\beta|^2 = 1$ ensures that the probabilities of measuring the qubit in either the $|0\rangle$ or $|1\rangle$ state sum to 1.

The qubit's unique ability to exist in a superposition of states is what gives quantum computers their immense computational potential, enabling them to process and store information in fundamentally different ways than classical computers.

Superposition

Superposition is a quantum phenomenon where a qubit exists in a combination of multiple states simultaneously. For example, a qubit in the state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{2}$$

is in an equal superposition of $|0\rangle$ and $|1\rangle$. This means that if we measure the qubit, there is an equal probability (50%) of observing it in either state.

Key properties of superposition:

- **Parallelism:** When a quantum system is in superposition, it can perform computations for all possible states simultaneously. For instance, a single qubit can encode two states ($|0\rangle$ and $|1\rangle$) at the same time, while n qubits can encode 2^n states.
- **Measurement Collapse:** When a qubit in superposition is measured, it collapses into one of its basis states, $|0\rangle$ or $|1\rangle$, with a probability given by $|\alpha|^2$ and $|\beta|^2$, respectively.

Superposition allows quantum systems to explore multiple possibilities in parallel, which is critical for quantum algorithms such as Grover's search or Shor's factoring.

Entanglement

Entanglement is a uniquely quantum phenomenon where two or more qubits become correlated in such a way that the state of one qubit is directly related to the state of the other, regardless of the physical distance between them. When qubits are entangled, the measurement of one qubit instantly determines the state of the other.

An example of an entangled state for two qubits is the Bell state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{3}$$

Here:

- $|00\rangle$ means both qubits are in the $|0\rangle$ state.
- $|11\rangle$ means both qubits are in the $|1\rangle$ state.

If one qubit is measured to be $|0\rangle$, the other qubit will instantly collapse to $|0\rangle$, and similarly for $|1\rangle$, regardless of the distance between them.

Key features of entanglement:

- **Non-Local Correlations:** Entanglement defies classical intuition, as it suggests that measurement outcomes are correlated even across vast distances, a phenomenon supported by experiments validating Bell's Theorem.
- **Applications:** Entanglement is a resource for many quantum technologies, including quantum teleportation, quantum cryptography (e.g., secure communication via the BB84 protocol), and quantum error correction.

Entanglement, along with superposition, forms the backbone of quantum computing and quantum communication, enabling capabilities that are impossible in the classical world.

Quantum Gates and Circuits

Quantum gates are the operational primitives of quantum computation. They manipulate qubits by altering their states in a manner consistent with quantum mechanics. Examples include:

- **Hadamard Gate (H)**: Creates superposition from a basis state.
- **Pauli Gates (X, Y, Z)**: Rotate qubit states around different axes.
- **CNOT Gate**: Entangles two qubits by flipping the second qubit based on the state of the first.

A sequence of quantum gates forms a *quantum circuit*, analogous to classical logic circuits but with exponentially richer possibilities due to quantum parallelism.

2 Introduction to Quantum Walks

The concept of a *quantum walk* is a quantum analog of the classical random walk and plays a significant role in quantum algorithms. There are two main types of quantum walks: *continuous-time* and *discrete-time* quantum walks, both of which exhibit behaviors that are significantly different from classical random walks.

Continuous-Time Quantum Walks

A *continuous-time quantum walk* is defined on a graph, where the evolution of the system is governed by a differential equation similar to the Schrödinger equation:

$$i\frac{d}{dt}q(t) = Hq(t),$$

where the Hamiltonian H is an $N \times N$ Hermitian matrix, with $H_{jk} = 0$ if and only if vertices j and k are not connected. The vector $q(t) \in \mathbb{C}^N$ contains the complex amplitudes corresponding to each vertex. Notably, the state space for the quantum walk is the same as that for the corresponding classical random walk.

One important matrix associated with the graph G is the *Laplacian matrix*, defined as:

$$L_{jk} = \begin{cases} -\deg(j) & \text{if } j = k, \\ 1 & \text{if } (j,k) \in E, \\ 0 & \text{otherwise.} \end{cases}$$

The continuous-time random walk on G is then defined as the solution to the differential equation:

$$\frac{d}{dt}p_j(t) = \sum_{k \in V} L_{jk}p_k(t),$$

where $p_j(t)$ represents the probability at vertex j at time t. The solution to this equation can be expressed in closed form as:

$$p(t) = e^{Lt}p(0),$$

where L is the Laplacian matrix and $p(0)$ is the initial condition.

This equation closely resembles the Schrödinger equation, but it lacks the factor i. By adding this factor and redefining the probabilities $p_j(t)$ as quantum amplitudes $q_j(t) = \langle j|\psi(t)\rangle$ (where $\{|j\rangle : j \in V\}$ is an orthonormal basis for the Hilbert space), we obtain:

$$i\frac{d}{dt}q_j(t) = \sum_{k\in V} L_{jk}q_k(t),$$

which is the Schrödinger equation with the Laplacian of the graph as the Hamiltonian. Since the Laplacian is a Hermitian operator, these dynamics preserve normalization:

$$\frac{d}{dt}\sum_{j\in V}|q_j(t)|^2 = 0.$$

The solution to this differential equation is:

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

A continuous-time quantum walk can also be defined using any Hermitian Hamiltonian that respects the structure of G.

Differences from Classical Random Walks

The evolution of a quantum walk, governed by a Hamiltonian, dictates state transitions over time while preserving normalization. This contrasts with classical random walks, which involve probabilistic transitions. Moreover, the wave nature of quantum mechanics introduces interference effects, enabling faster exploration of graphs compared to classical methods. For instance, on one-dimensional graphs, a classical random walk progresses at a rate proportional to the square root of time, while a quantum walk progresses linearly with time due to the wave-like propagation of quantum states.

Discrete-Time Quantum Walks

Discrete-time quantum walks, though more complex to define, provide a convenient framework for certain quantum algorithms, particularly quantum search algorithms.

In the simplest classical discrete-time random walk on a graph G, at each time step, the walker moves from a given vertex to one of its neighbors with equal probability. This process is described by a $|V| \times |V|$ matrix M, where:

$$M_{jk} = \begin{cases} \frac{1}{\deg(k)} & \text{if } (j,k) \in E, \\ 0 & \text{otherwise.} \end{cases}$$

The initial probability distribution p over the vertices updates to $p' = Mp$ after one step.

For quantum walks, maintaining unitarity requires a *coin operator* C to determine the direction of the next step. A common choice for the coin operator is the Grover diffusion operator, defined as:

$$C := \sum_{j\in V}|j\rangle\langle j| \otimes (2|\partial_j\rangle\langle\partial_j| - I),$$

where:

$$|\partial_j\rangle := \frac{1}{\sqrt{\deg(j)}}\sum_{k:(j,k)\in E}|k\rangle,$$

denotes the superposition of the neighboring vertices of $|j\rangle$, and I is the identity matrix.

One step of the discrete-time quantum walk is described by the unitary operator SC, where S is the swap operator:

$$S = \sum_{(j,k)\in E} |j,k\rangle\langle k,j|.$$

Comparison of Models

The continuous-time model is simpler to define and analyze, often leading to exponential speedups under specific conditions, such as graphs with small maximum degrees. However, discrete-time quantum walks are easier to implement using quantum circuits, making them more practical in many applications. For example, while continuous-time models may struggle with certain problems like *element distinctness*, discrete-time models handle them more effectively.

3 Group Actions

Group actions provide a framework for understanding how groups interact with sets, formalizing the concept of applying transformations systematically. They capture the symmetries and structure-preserving transformations of objects, making them fundamental in mathematics and its applications. Group actions describe transformations through a set of rules that ensure consistency and compatibility with the underlying group operations. This concept is pivotal in cryptography, where the symmetries and operations of groups underpin many secure systems.

In cryptography, group actions are critical to protocols like Elliptic Curve Cryptography (ECC), which relies on the difficulty of reversing group-based operations to ensure security. Isogeny-based cryptography, a post-quantum cryptographic candidate, uses group actions on elliptic curves to create complex mathematical problems resistant to quantum attacks. Similarly, lattice-based and code-based cryptography use group actions to study transformations in structures that form the basis for secure communication systems. Non-abelian group actions are being explored for their potential to create quantum-resistant algorithms.

In quantum computing, group actions are central to quantum walks, a quantum equivalent of classical random walks. Quantum walks leverage group actions to describe the evolution of quantum states and exploit the symmetries of these states for tasks like search, optimization, and cryptographic protocol design. This makes them valuable in constructing secure quantum algorithms and protocols, particularly in quantum key distribution and graph-based cryptography. Overall, group actions bridge abstract mathematical theory with practical applications in classical and quantum cryptography.

Definition of Group Action

Group actions form a bridge between group theory and other mathematical structures, offering a systematic way to study symmetry, transformations, and invariants. Let us delve deeper into their properties, classifications, and applications.

Formal Definition

A **group action** of a group G on a set X is a map $\cdot : G \times X \to X$ that satisfies:

1. **Identity Property**:
$$e \cdot x = x \quad \text{for all } x \in X,$$
where e is the identity element of G.

2. **Compatibility (Associativity)**:
$$(gh) \cdot x = g \cdot (h \cdot x) \quad \text{for all } g, h \in G,\ x \in X.$$

Alternatively, the group action can be viewed as a homomorphism $\phi : G \to \mathrm{Sym}(X)$, where $\mathrm{Sym}(X)$ is the group of all permutations of X.

Types of Group Actions

1. **Faithful Action**: The action is faithful if $g \cdot x = x$ for all $x \in X$ implies $g = e$. Equivalently, the homomorphism ϕ is injective.

2. **Transitive Action**: The action is transitive if, for any $x, y \in X$, there exists $g \in G$ such that $g \cdot x = y$. In this case, X consists of a single orbit.

3. **Free Action**: The action is free if $g \cdot x = x$ implies $g = e$ for all $x \in X$.

4. **Regular Action**: The action is both transitive and free, meaning there is exactly one $g \in G$ for each pair (x, y) such that $g \cdot x = y$.

5. **Effective Action**: The action is effective if the only group element acting as the identity on X is e.

Key Concepts in Group Actions

1. **Orbits**: For $x \in X$, the **orbit** of x is:
$$\mathrm{Orb}(x) = \{g \cdot x \mid g \in G\}.$$
Orbits partition the set X, and each orbit is a subset where the action appears "connected."

2. **Stabilizer Subgroup**: The **stabilizer** of $x \in X$ is:
$$\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}.$$
It is a subgroup of G and describes the symmetries that leave x unchanged.

3. **Orbit-Stabilizer Theorem**: This theorem links the size of an orbit and its stabilizer:
$$|G| = |\mathrm{Orb}(x)| \cdot |\mathrm{Stab}_G(x)|.$$

4. **Fixed Points**: A point $x \in X$ is a **fixed point** if $g \cdot x = x$ for all $g \in G$. The set of fixed points is:
$$\mathrm{Fix}(G) = \{x \in X \mid g \cdot x = x,\ \forall g \in G\}.$$

5. **Invariant Subsets**: A subset $Y \subseteq X$ is **invariant** under the action if $g \cdot y \in Y$ for all $g \in G$ and $y \in Y$.

Equivalence Relations Induced by Group Actions

The orbits of a group action define an equivalence relation on X, where $x \sim y$ if there exists $g \in G$ such that $g \cdot x = y$.

- **Equivalence Classes**: The orbits of the action.
- **Quotient Set**: The set of orbits, denoted X/G.

Quantum walks from Group Actions

The spectral decomposition of the adjacency matrix of a Cayley graph generated by a general group action G provides insights into the structure and properties of the graph. This decomposition leverages the symmetries of the group G and representation theory to analyze the eigenvalues and eigenvectors of the adjacency matrix.

Let G be a finite group, and let X be a set on which G acts via a group action $G \times X \to X$. A Cayley graph can be constructed based on this action, where the vertices are the elements of the set X, and For each $g \in G$ and $x \in X$, there is an edge between x and $g * x$, where $g * x$ is the action of g on x.

If the generating set $S \subset G$ is symmetric (i.e., $s \in S \implies s^{-1} \in S$), then the Cayley graph is undirected. Otherwise, it may be directed.

The adjacency matrix A of the Cayley graph is a matrix that encodes the edges of the graph:

$$A_{x,y} = \begin{cases} 1, & \text{if there exists } g \in G \text{ such that } y = g * x, \\ 0, & \text{otherwise.} \end{cases}$$

The adjacency matrix is symmetric if the group action preserves symmetry, which happens if G is acting via an involution, i.e., if for every generator $g \in G$, its inverse is also a generator. It also inherits the symmetries of the group action. That is, the group G acts on the vertices of the graph, and the adjacency matrix commutes with the action of the group. This means that the adjacency matrix A is highly structured, and its eigenvalues can be computed using the representation theory of the group G.

The eigenvalues of the adjacency matrix correspond to the eigenvalues of these blocks $\rho(A)$, and the multiplicities of the eigenvalues are related to the dimensions of the corresponding irreducible representations.

The spectral decomposition of the adjacency matrix A can be written as:

$$A = \sum_i \lambda_i v_i v_i^\top,$$

where:

- λ_i are the eigenvalues, - v_i are the corresponding eigenvectors (which lie in the spaces corresponding to the irreducible representations), - $v_i v_i^\top$ is the outer product of the eigenvector v_i with itself.

The eigenvectors v_i are related to the characters of the group G. Specifically, the characters of irreducible representations of G help determine the eigenvalues of A. If χ_ρ denotes the character of the irreducible representation ρ, then the eigenvalues are given by:

$$\lambda_\rho = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) A(g),$$

where $A(g)$ is the action of g as represented in the adjacency matrix.

4 Quantum Money

Introduction to Quantum Money

Quantum money is a revolutionary concept in cryptography that uses quantum mechanics to create a form of currency that is provably secure against forgery. Originally introduced by physicist Stephen Wiesner in the 1970s, quantum money represents one of the earliest proposed applications of quantum information science. By encoding information into quantum states, quantum money exploits the fundamental principles of quantum mechanics to provide security features unattainable by classical systems.

How Quantum Money Works

At its core, quantum money relies on two key principles of quantum mechanics: the *no-cloning theorem* and the *observer effect*.

Encoding Information in Quantum States

- Each quantum bill contains a unique quantum state, such as a set of qubits encoded in superposition.
- These states are generated and stored by the issuing authority (e.g., a central bank) using a secret algorithm.

Verification Process

- The issuing authority also generates a verification protocol, allowing a legitimate quantum bill to be authenticated.
- When a user presents a quantum bill for verification, the authority measures the encoded quantum states using the pre-determined protocol.
- If the measured states align with the expected values, the bill is deemed valid.

Unforgeability

- Due to the *no-cloning theorem*, it is impossible to copy an unknown quantum state without altering it.
- Any attempt to measure or duplicate the quantum state results in a disturbance detectable during verification.

Key Principles Underpinning Quantum Money

1. **No-Cloning Theorem:** The no-cloning theorem states that an unknown quantum state cannot be perfectly copied. This makes quantum money inherently secure, as counterfeiters cannot reproduce the quantum states encoded in legitimate currency.

2. **Measurement Disturbance:** Observing or measuring a quantum state generally alters it. This ensures that any unauthorized attempt to inspect the quantum money will render it invalid, as the encoded states will no longer match their original form.

3. **Randomness and Superposition:** Quantum money utilizes superposition to encode information. For example, a single qubit in superposition may represent both 0 and 1 simultaneously until measured. The randomness of these states makes predicting or reproducing them without knowledge of the original encoding impossible.

4. **Entanglement (Optional Feature):** Some implementations of quantum money involve quantum entanglement, where pairs of quantum states are interconnected. Changes to one entangled state directly affect its pair, adding another layer of security against forgery.

Benefits of Quantum Money

- **Unforgeable:** Classical currency, both physical and digital, can be counterfeited with enough effort and resources. Quantum money, however, is fundamentally unforgeable due to the laws of quantum physics.

- **Decentralized Verification:** In some theoretical models, quantum money can be verified without contacting the issuing authority, enabling decentralized systems for authentication.

- **Enhanced Privacy:** The unique encoding of each quantum bill could allow for privacy-preserving transactions, as the details of the transaction need not be linked to the bill's verification.

Challenges and Open Questions

1. **Practical Implementation:** Generating and maintaining stable quantum states in real-world conditions is technically challenging. Quantum systems are highly sensitive to environmental noise, requiring robust error-correction mechanisms.

2. **Scalability:** For quantum money to replace traditional systems, it must scale to accommodate billions of users and transactions.

3. **Theft and Security:** While quantum money cannot be forged, it can still be stolen, much like traditional physical or digital assets. Developing secure storage and transfer mechanisms is a priority.

4. **Centralized vs. Decentralized Systems:** Most current proposals involve a centralized authority for issuing and verifying quantum money. However, decentralized quantum money systems (akin to blockchain technology) are an area of active research.

Applications Beyond Money

The principles underlying quantum money have broader applications, such as:

- **Quantum Tokens:** Used in secure communication or access control.

- **Quantum Cryptography:** Building secure voting systems or decentralized platforms.

- **Quantum Key Distribution (QKD):** While distinct from quantum money, QKD relies on similar quantum principles to ensure the security of communication channels.

Conclusion

Quantum money represents a paradigm shift in secure transactions, leveraging the foundational principles of quantum mechanics to create currency that is inherently secure against forgery. While still a theoretical concept, advances in quantum technology and cryptography are rapidly bringing us closer to practical implementations. If realized, quantum money could redefine financial systems, offering unparalleled security and efficiency in the digital age.

5 Applicaions

Quantum Hartley Transform (QHT)

The **Quantum Hartley Transform (QHT)** is a linear unitary transform that operates on quantum states. It transforms the basis states $|x\rangle$ as follows:

$$|x\rangle \xrightarrow{\text{QHT}} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \text{cas}\left(\frac{2\pi xk}{N}\right) |k\rangle$$

where:

- x and k are integers in $\{0, 1, \ldots, N-1\}$,
- $\text{cas}(x) = \cos(x) + \sin(x)$,
- N is the dimension of the transform, typically 2^n for n-qubit systems.

For a quantum state $|\psi\rangle$ in an N-dimensional Hilbert space, represented as:

$$|\psi\rangle = \sum_{x=0}^{N-1} \psi_x |x\rangle,$$

the QHT transforms the state into:

$$|\psi'\rangle = \text{QHT}|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \left(\sum_{x=0}^{N-1} \psi_x \, \text{cas}\left(\frac{2\pi xk}{N}\right) \right) |k\rangle.$$

Properties of the QHT

1. **Unitary Transformation**: The QHT matrix U_{QHT} is unitary:

   $$U_{\text{QHT}} U_{\text{QHT}}^{\dagger} = I,$$

   preserving quantum state normalization.

2. **Symmetry**: The QHT is symmetric because $\text{cas}(x) = \text{cas}(-x)$.

3. **Efficient Implementation**: Like the Quantum Fourier Transform (QFT), the QHT can be implemented with $O(\log^2 N)$ gates for $N = 2^n$.

Comparison with the Quantum Fourier Transform (QFT)

The QFT and QHT differ in their transformation kernels:

- **QFT**:
$$|x\rangle \xrightarrow{\text{QFT}} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i x k/N} |k\rangle.$$
- **QHT**:
$$|x\rangle \xrightarrow{\text{QHT}} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \left[\cos\left(\frac{2\pi x k}{N}\right) + \sin\left(\frac{2\pi x k}{N}\right) \right] |k\rangle.$$

Applications of the QHT

- **Signal Processing**: Analysis of real-valued signals in quantum systems.
- **Quantum Algorithms**: Used in problems where real and symmetric basis representations simplify computations.
- **Data Compression**: Efficient representation of signals with high symmetry.

References