Quantum Computing for Cryptographer

Lizheng Wang 6th July 2025
lizhengwang@sjtu.edu.cn

1 Basic Concept of Quantum Mechanics

A quantum state is described by a complex vector (column) $|\psi\rangle$ in a Hilbert space $\mathcal{H}$. This notation is known as a **ket**. The conjugate transpose of a ket is a **bra**, denoted as $\langle\psi| = (|\psi\rangle)^\dagger$.

1.1 Inner Product and its Properties

The inner product between two states $|\phi\rangle$ and $|\psi\rangle$ is written as $\langle\phi|\psi\rangle$ and results in a complex number. It has several key properties:

- **Positivity**: For any non-zero state, $\langle\psi|\psi\rangle > 0$.
- **Linearity**: $\langle\phi|(a|\psi_1\rangle + b|\psi_2\rangle) = a\langle\phi|\psi_1\rangle + b\langle\phi|\psi_2\rangle$.
- **Skew Symmetry**: $\langle\phi|\psi\rangle = (\langle\psi|\phi\rangle)^*$.

1.2 Norm and Normalization

The norm of a state is defined as $|||\psi\rangle|| = \sqrt{\langle\psi|\psi\rangle}$. For any physical quantum state, it must be normalized to 1.

$$\langle\psi|\psi\rangle = 1$$

2 State Representation and Key Theorems

In an N-dimensional Hilbert space with an orthonormal basis $\{|e_i\rangle\}_{i=1}^N$, any state $|\psi\rangle$ can be written as a linear superposition of these basis vectors:

$$|\psi\rangle = \sum_{i=1}^{N} a_i|e_i\rangle, \quad \text{where } a_i \in \mathbb{C}$$

The normalization condition implies that the complex coefficients must satisfy $\sum_{i=1}^N |a_i|^2 = 1$.

2.1 Completeness Relation

The orthonormal basis vectors satisfy the completeness relation, which states that they form a complete set spanning the space:

$$\sum_{i=1}^{N} |e_i\rangle\langle e_i| = I$$

Here, I represents the identity operator.

Proof

Let $|\psi\rangle$ be an arbitrary vector in the Hilbert space $\mathcal{H}$. Since the set $\{|e_i\rangle\}$ forms an orthonormal basis, we can express $|\psi\rangle$ as a linear combination of these basis vectors:

$$|\psi\rangle = \sum_{i=1}^{N} a_i |e_i\rangle$$

To find the coefficient a_j, we can take the inner product with $\langle e_j|$:

$$\langle e_j|\psi\rangle = \langle e_j| \sum_{i=1}^{N} a_i |e_i\rangle = \sum_{i=1}^{N} a_i \langle e_j|e_i\rangle$$

Due to the orthonormality of the basis, $\langle e_j|e_i\rangle = \delta_{ji}$ (the Kronecker delta). Thus, the sum simplifies to:

$$\langle e_j|\psi\rangle = a_j$$

Now, we substitute this expression for the coefficients back into the expansion of $|\psi\rangle$:

$$|\psi\rangle = \sum_{i=1}^{N} \langle e_i|\psi\rangle |e_i\rangle$$

By rearranging the terms (since $\langle e_i|\psi\rangle$ is a scalar), we get:

$$|\psi\rangle = \left(\sum_{i=1}^{N} |e_i\rangle\langle e_i| \right) |\psi\rangle$$

Since this equation must hold for any arbitrary vector $|\psi\rangle$, the operator in the parenthesis must be the identity operator I. Therefore, we have proven the completeness relation.

2.2 Cauchy-Schwarz Inequality

This fundamental inequality relates the inner product of two states to their individual norms. For any two states $|\psi\rangle$ and $|\phi\rangle$:

$$|\langle\psi|\phi\rangle|^2 \leq \langle\psi|\psi\rangle\langle\phi|\phi\rangle$$

This document demonstrates the current theme. Here's a sample of regular text with **bold text**, *italic text*, and `monospaced text`.

2.3 Tensor Product of Hilbert Spaces

When we consider a system composed of multiple subsystems (e.g., multiple particles), the state space of the combined system is the tensor product of the individual Hilbert spaces: $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_M$. For a two-particle system with state spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, a general state $|\Psi\rangle$ can be written as:

$$|\Psi\rangle = \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} a_{ij} |e_i\rangle \otimes |f_j\rangle$$

where $\{|e_i\rangle\}$ and $\{|f_j\rangle\}$ are the bases for $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively. The normalization condition is $\sum_{i,j} |a_{ij}|^2 = 1$.

2.4 Separable and Entangled States

A state in a composite Hilbert space is called **separable** if it can be written as a tensor product of states from the individual subsystems. For a two-particle system, a separable state has the form:

$$|\Psi\rangle_{sep} = |\psi_1\rangle \otimes |\psi_2\rangle = \left(\sum_i a_i|e_i\rangle\right) \otimes \left(\sum_j b_j|f_j\rangle\right)$$

A state that cannot be written in this form is called an **entangled state** .

2.5 Multiple Qubits

A system of n qubits is described by a state in a 2^n-dimensional Hilbert space. The basis vectors are often written in a shorthand notation, for example, for a two-qubit system, $|0\rangle_1 \otimes |1\rangle_2$ is written as $|01\rangle$. The four basis vectors are $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

A famous example of a two-qubit entangled state is the **EPR (Einstein-Podolsky-Rosen) pair**, also known as a Bell state:

$$|\Psi_{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

This state is entangled because it cannot be factored into the form $(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle)$.

In contrast, a state like the following is separable, not entangled:

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

3 Quantum Measurement and Fundamental Principles

3.1 Quantum Measurement

Quantum measurements are described by observables, which are self-adjoint operators A. The possible outcomes of a measurement of A are its eigenvalues a_n.

- **Probability**: If the system is in a state $|\psi\rangle$, the probability of obtaining the eigenvalue a_n is given by $Prob(a_n) = \langle\psi|P_n|\psi\rangle$, where P_n is the projection operator onto the eigenspace of a_n.
- **State Collapse**: If the measurement result is a_n, the quantum state of the system instantaneously collapses to the new state:

$$|\psi'\rangle = \frac{P_n|\psi\rangle}{\sqrt{\langle\psi|P_n|\psi\rangle}}$$

  This collapse illustrates that the act of measurement fundamentally disturbs the original quantum state.

3.2 No-Cloning Theorem

This fundamental theorem states that it is impossible to create an identical copy of an arbitrary, unknown quantum state. In other words, there is no universal unitary operator U such that for any states $|\alpha\rangle$ and $|\beta\rangle$, $U(|\alpha 0\rangle) = |\alpha\alpha\rangle$ and $U(|\beta 0\rangle) = |\beta\beta\rangle$.

Proof

Assume such a unitary operator U exists. Let's consider a superposition state $|\gamma\rangle = \frac{1}{\sqrt{2}}(|\alpha\rangle + |\beta\rangle)$. Due to the linearity of U, applying it to $|\gamma 0\rangle$ yields:

$$U(|\gamma 0\rangle) = U\left(\frac{1}{\sqrt{2}}(|\alpha 0\rangle + |\beta 0\rangle)\right) = \frac{1}{\sqrt{2}}(U|\alpha 0\rangle + U|\beta 0\rangle) = \frac{1}{\sqrt{2}}(|\alpha\alpha\rangle + |\beta\beta\rangle)$$

However, if the cloning operation were truly universal, it should also clone the state $|\gamma\rangle$ directly:

$$U(|\gamma 0\rangle) = |\gamma\gamma\rangle = \left(\frac{1}{\sqrt{2}}(|\alpha\rangle + |\beta\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|\alpha\rangle + |\beta\rangle)\right) = \frac{1}{2}(|\alpha\alpha\rangle + |\alpha\beta\rangle + |\beta\alpha\rangle + |\beta\beta\rangle)$$

Comparing the two results, we see a contradiction:

$$\frac{1}{\sqrt{2}}(|\alpha\alpha\rangle + |\beta\beta\rangle) \neq \frac{1}{2}(|\alpha\alpha\rangle + |\alpha\beta\rangle + |\beta\alpha\rangle + |\beta\beta\rangle)$$

Therefore, our initial assumption that a universal cloning operator U exists must be false.

4 Quantum Key Distribution

Quantum Key Distribution (QKD) allows two parties, typically called Alice and Bob, to produce a shared secret random key known only to them, using the principles of quantum mechanics. The security of the protocol is based on the fact that any attempt by an eavesdropper (Eve) to learn information about the key will disturb the quantum system and be detected. The BB84 protocol[1] is one of the first and most famous QKD protocols.

4.1 The Four States and Two Bases

The BB84 protocol uses four quantum states, which are grouped into two mutually unbiased bases:

- **Rectilinear Basis (Z-basis)**: Used to encode bits as $|0\rangle$ and $|1\rangle$.
- **Diagonal Basis (X-basis)**: Used to encode bits as $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

The key idea is that if you measure a state from one basis using the other basis, the outcome is completely random. For example, measuring $|+\rangle$ in the Z-basis gives $|0\rangle$ or $|1\rangle$ with 50% probability each.

4.2 Protocol Steps

1. **Alice's Transmission**: Alice wants to send a string of random bits to Bob. For each bit, she randomly chooses one of the two bases (Z or X) to encode it. She then sends the corresponding quantum state (a qubit) to Bob through a quantum channel.
2. **Bob's Measurement**: For each qubit he receives, Bob also randomly and independently chooses one of the two bases (Z or X) to perform a measurement. He records his measurement outcome.

3. **Basis Reconciliation (Sifting)**: After all qubits have been sent and measured, Bob communicates with Alice over a public classical channel (e.g., a phone call). They announce the sequence of bases they used for each qubit, but not their bit values. They discard all the results where they used different bases. On average, they will agree on the basis 50% of the time. The remaining sequence of bits is called the *sifted key*.
4. **Eavesdropping Detection**: Alice and Bob publicly compare a random subset of their sifted keys. If the bits match, they can be confident no one was listening. If there are discrepancies, they assume an eavesdropper (Eve) was present and abort the protocol.

4.3 Security Against Eavesdropping

Suppose Eve tries to intercept the qubits, measure them, and then resend them to Bob (a measure-and-resend attack). Since Eve does not know which basis Alice used for any given qubit, she must guess.

- On average, Eve will guess the correct basis 50% of the time. In these cases, she learns the bit value and wouldn't interfere with the correct state , introducing no error.
- For the other 50% of the qubits, Eve will guess the wrong basis. Her measurement will collapse the state into a random outcome. Then even if Bob measures in the correct (original) basis, there is a 50% chance he will get the wrong bit value.

Therefore, Eve's presence introduces an error rate of approximately 25% ($50\% \times 50\%$) in the sifted key. When Alice and Bob compare their subset of keys, they will easily detect this high error rate and know that their communication has been compromised.

Note

What will happen if Eve just measure one qubit? She will be discovered with a $50\% * 50\% * 50\% * 50\% = 6.25\%$ probability. (Sifting $\wedge$ measure in wrong basis $\wedge$ get wrong bit value $\wedge$ random subset)

5 Quantum Computation

Quantum computation leverages quantum-mechanical phenomena such as superposition and entanglement to perform calculations.

5.1 Quantum Circuit

Quantum algorithms are implemented using quantum circuits, which are analogous to classical logic circuits. A quantum circuit consists of a sequence of quantum gates applied to a set of qubits.

Note

A fundamental requirement of quantum mechanics is that the evolution of a closed quantum system must be a **unitary transformation**. This is a direct consequence of the Schrödinger equation ($i\hbar\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle$), which ensures that the total probability (i.e., the norm of the state vector) is conserved over time. Therefore, every quantum gate must be represented by a unitary matrix U, satisfying the condition $U^\dagger U = UU^\dagger = I$. This unitarity implies that

every quantum operation is **reversible**. Given the output of a gate, one can always determine its input by applying the inverse operation, $U^\dagger$. This contrasts with many classical gates, such as the AND gate, which are irreversible because they lose information (e.g., given the output 0, you cannot know if the inputs were 00, 01, or 10).

Some fundamental gates include:

- **Hadamard Gate (H)**: Creates superpositions. $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$. When applied to an n-qubit register (denoted $H^{\otimes n}$), it transforms a computational basis state $|x\rangle$ into a superposition of all 2^n basis states, with specific phase relationships:

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle$$

  Here, $x \cdot y = x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_ny_n$ is the bitwise dot product. This phase relationship is crucial for quantum interference, as seen in algorithms like Simon's and Shor's.

- **Pauli-X Gate (NOT Gate)**: Flips the qubit state. $X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$.

- **Controlled-NOT Gate (CNOT)**: A two-qubit gate that flips the target qubit if and only if the control qubit is $|1\rangle$. It is essential for creating entanglement.

Example Circuit: Creating a Bell State. A circuit to create the EPR pair (a Bell state) $|\Psi_{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ from the initial state $|00\rangle$ is as follows:

1. Apply a Hadamard gate to the first qubit. The state becomes $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle+|10\rangle)$.
2. Apply a CNOT gate, with the first qubit as the control and the second qubit as the target. The $|10\rangle$ component becomes $|11\rangle$, resulting in the final entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

5.2 Quantum Parallelism

Theorem

It's possible to construct reversible quantum gates for any arbitrary classically computable function f

$$U_f|x, 0\rangle \rightarrow |x, f(\mathrm{x})\rangle$$

The core power of quantum computing comes from quantum parallelism. By preparing an n-qubit register in a uniform superposition of all 2^n possible states, a quantum computer can perform a single operation on all these states simultaneously. For a function $f(x)$, a unitary operator U_f can be constructed such that:

$$U_f\left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x, 0\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x, f(x)\rangle$$

This single operation computes $f(x)$ for all possible values of x. The challenge then lies in designing algorithms that can extract useful information from this final superposition.

5.3 Simon's Algorithm: A Precursor to Shor's

Problem

Imagine a black-box function $f : \{0,1\}^n \to \{0,1\}^n$ with a promise: there exists a unique, non-zero "hidden period" string $s \in \{0,1\}^n$ such that for any two inputs x_1, x_2, we have $f(x_1) = f(x_2)$ if and only if $x_2 = x_1 \oplus s$. The goal is to find this hidden period s.

Simon's algorithm was one of the first to demonstrate an exponential speedup over any classical algorithm for a specific problem. While the problem it solves is somewhat contrived, its core technique of using quantum interference to find a hidden property (a period) was a direct inspiration for Shor's algorithm.

1. **Initialization**: Start with two n-qubit registers, both initialized to $|0\rangle^{\otimes n}$.

$$|0\rangle^{\otimes n}|0\rangle^{\otimes n}$$

2. **Superposition**: Apply $H^{\otimes n}$ to the first register to create a uniform superposition of all 2^n possible inputs.

$$\left(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle\right)|0\rangle^{\otimes n}$$

3. **Oracle Query**: Apply the quantum oracle U_f which computes $f(x)$ into the second register. This entangles the two registers.

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle$$

4. **First Measurement**: Measure the second register. Suppose the outcome is some value z_0. The state of the first register collapses to an equal superposition of the two inputs that could have produced this output: some unknown x_0 and $x_0 \oplus s$.

$$\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus s\rangle)$$

5. **Second Hadamard Transform**: Apply $H^{\otimes n}$ again to this collapsed first register. This is the key interference step. The state becomes:

$$\begin{aligned}
H^{\otimes n}\left(\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus s\rangle)\right) &= \frac{1}{\sqrt{2^{n+1}}}\sum_{y\in\{0,1\}^n}[(-1)^{x_0\cdot y} + (-1)^{(x_0\oplus s)\cdot y}]|y\rangle \\
&= \frac{1}{\sqrt{2^{n+1}}}\sum_{y\in\{0,1\}^n}[(-1)^{x_0\cdot y} + (-1)^{(x_0\cdot y)\oplus(s\cdot y)}]|y\rangle \\
&= \frac{1}{\sqrt{2^{n+1}}}\sum_{y\in\{0,1\}^n}[(-1)^{x_0\cdot y} + (-1)^{(x_0\cdot y)}(-1)^{(s\cdot y)}]|y\rangle \\
&= \frac{1}{\sqrt{2^{n+1}}}\sum_{y\in\{0,1\}^n}[(-1)^{x_0\cdot y}(1 + (-1)^{s\cdot y})]|y\rangle
\end{aligned}$$

The term in the square brackets, $[(-1)^{x_0 \cdot y}(1 + (-1)^{s \cdot y})]$, is non-zero only if $s \cdot y = 0 \pmod 2$. For all other values of y, destructive interference causes the amplitude to be zero.

6. **Second Measurement**: Measure the first register. The outcome will be a random string y that is guaranteed to satisfy the condition $y \cdot s = 0$.

7. **Classical Post-processing**: Repeat the quantum steps about n times to obtain $n - 1$ linearly independent equations of the form $y_i \cdot s = 0$. Use a classical algorithm (like Gaussian elimination) to solve this system of linear equations for the unknown hidden period s.

Simon's algorithm finds s in polynomial time, demonstrating a clear exponential advantage over classical methods and paving the way for more practical algorithms.

5.4 Shor's Algorithm

Problem

Period-finding problem: Given a periodic function $f(x)$ such that $f(x) = f(x + r)$, find the period r. $f(x)$ can be efficiently computed from x, $N/2 < r < N$ for some N.

Shor's algorithm[2] is a quantum algorithm for period-finding problem, with profound implications for cryptography. It can factor a large number N in polynomial time, posing a threat to classical cryptosystems like RSA.

The algorithm proceeds as follows:

1. **Initialization**: We start with two n qubits "registers", an input register X and an output register Y. Let N be the number we are interested in (e.g., for factorization). We choose n such that $2^n \approx N^2$. The registers are initialized to the state $|0\rangle|0\rangle$.

2. **Superposition**: Apply a Hadamard gate to each qubit in the input register X. This creates a uniform superposition of all possible input values from 0 to $w - 1$, where $w = 2^n$.

$$\frac{1}{\sqrt{w}} \sum_{x=0}^{w-1} |x\rangle|0\rangle$$

3. **Function Evaluation (Oracle)**: Apply a unitary operator U_f that computes the function $f(x)$ and stores the result in the output register Y.

$$U_f(|x\rangle|0\rangle) = |x\rangle|f(x)\rangle$$

Applying this to our superposition gives:

$$\frac{1}{\sqrt{w}} \sum_{x=0}^{w-1} |x\rangle|f(x)\rangle$$

Due to entanglement, the state is now a superposition of pairs $(x, f(x))$.

4. **Measure Output Register**: Measure the output register Y. The measurement will yield some value u. Due to the principles of quantum measurement, the state collapses. The output register is now fixed at $|u\rangle$, and crucially, the input register X collapses into a superposition of

only those values of x for which $f(x) = u$.

$$\frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |d_u + jr\rangle |u\rangle$$

Here, d_u is the smallest input that gives the output u, r is the period, and $M \approx w/r$ is the number of times this value u appears.

5. **Quantum Fourier Transform (QFT)**: Discard the output register and apply the Quantum Fourier Transform to the input register X. The QFT is a quantum analogue of the classical discrete Fourier transform.

$$U_{QFT}|x\rangle = \frac{1}{\sqrt{w}} \sum_{k=0}^{w-1} e^{i2\pi kx/w} |k\rangle$$

Applying the QFT to our periodic superposition state transforms it into a new superposition where the amplitudes are sharply peaked at integer multiples of w/r.

6. **Measure Input Register**: Measure the input register X. The measurement outcome will, with high probability, be a value v that is close to an integer multiple of w/r.

$$v \approx \frac{\lambda w}{r} \quad \text{for some unknown integer } \lambda$$

7. **Classical Post-processing**: From the measured value v, we now have the equation $\frac{v}{w} \approx \frac{\lambda}{r}$. We can use the continued fractions algorithm to find the irreducible fraction $\frac{\lambda'}{r'}$ that best approximates $\frac{v}{w}$. The denominator r' is a very good candidate for the period r. If it is not, the algorithm can be repeated. The probability of success is arbitrarily close to 1 with a few repetitions.

5.4.1 Application 1: Integer Factorization

Shor's algorithm's most famous application is factoring a large integer N.

- **The Function**: We choose a random number $a < N$ (if $\gcd(a, N) \neq 1$, we have found a factor already). We then define the function $f(x) = a^x \pmod N$. The goal is to find the period r of this function, which is the smallest positive integer such that $a^r \equiv 1 \pmod N$.
- **Finding Factors**: Once the period-finding subroutine returns r, we check if r is even. If it is, we have $a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \pmod N$. This means N must divide $(a^{r/2} - 1)(a^{r/2} + 1)$.
- **The Result**: As long as $a^{r/2} \not\equiv \pm 1 \pmod N$ (which is highly likely for a random a), then $\gcd(a^{r/2} - 1, N)$ and $\gcd(a^{r/2} + 1, N)$ will be non-trivial factors of N.

Example: To factor $N = 15$. Let's pick $a = 7$. We need to find the period of $f(x) = 7^x \pmod{15}$. $7^1 \equiv 7$, $7^2 \equiv 4$, $7^3 \equiv 13$, $7^4 \equiv 1$. The period is $r = 4$. Since $r = 4$ is even, we compute $\gcd(7^{4/2} - 1, 15) = \gcd(48, 15) = 3$ and $\gcd(7^{4/2} + 1, 15) = \gcd(50, 15) = 5$. We have successfully found the factors 3 and 5.

5.4.2 Application 2: Discrete Logarithm Problem

Shor's algorithm can also be adapted to solve the discrete logarithm problem, which is another hard problem underlying many cryptosystems.

- **The Problem**: Given a prime p, a generator g, and a value y, find the integer x such that $g^x \equiv y \pmod{p}$.
- **The Function**: To solve this, we define a function of two variables: $f(a,b) = g^a y^{-b} \pmod{p}$. This function is periodic. We are looking for a pair (a,b) such that $g^a y^{-b} \equiv 1 \pmod{p}$. Substituting $y \equiv g^x$, we get $g^a (g^x)^{-b} \equiv g^{a-xb} \equiv 1 \pmod{p}$. This means $a - xb$ must be a multiple of the order of the group.
- **The Solution**: By using a 2D version of the Quantum Fourier Transform, Shor's algorithm can find the period of this function $f(a,b)$. This period gives us a relationship between a and b which allows us to solve for the unknown x. The core mechanism remains the same: transforming a problem into a period-finding problem that can be solved efficiently on a quantum computer.

5.5 Grover's Search Algorithm

Problem

Searching Problem: find the input x_0 for a function $P(x)$ such that $P(x_0) = 1$ and $P(x) = 0$ for all other x.

Grover's algorithm[3] provides a quadratic speedup for searching an unstructured database. For a database with N items, a classical search takes on average $O(N)$ queries. Grover's algorithm can find the unique marked item in approximately $O(\sqrt{N})$ queries.

1. **Initialization**: Prepare an n-qubit register in a uniform superposition of all possible states. This is done by applying a Hadamard gate to each qubit, starting from the $|0...0\rangle$ state.

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

   In this state, every possible item has the same small amplitude, $\frac{1}{\sqrt{N}}$.

2. **The Grover Iteration (Amplitude Amplification)**: The core of the algorithm is to repeatedly apply an operation called the Grover operator, G. This operator cleverly increases the amplitude of the marked state while decreasing the amplitudes of all other states. The Grover operator consists of two steps:

   - **a) The Oracle (U_P)**: The oracle is a black-box operation that recognizes the solution. Its goal is to apply a phase shift of -1 to the marked item x_0, effectively "marking" it. This is achieved through a clever trick called *phase kickback*.

     Instead of directly computing $P(x)$, we use an auxiliary qubit (ancilla) prepared in the state $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The standard oracle operation is defined as $U_P(|x\rangle|q\rangle) = |x\rangle|q \oplus P(x)\rangle$. Let's see what happens when we apply this to our main register $|x\rangle$ and the ancilla $|-\rangle$:

$$U_P(|x\rangle|-\rangle) = |x\rangle \otimes U_P[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)] = |x\rangle \otimes \frac{1}{\sqrt{2}}(|P(x)\rangle - |1 \oplus P(x)\rangle)$$

     Now we consider two cases:

- If x is not the solution, $P(x) = 0$. The expression becomes $|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |x\rangle|-\rangle$. The state is unchanged.
- If x is the solution ($x = x_0$), $P(x) = 1$. The expression becomes $|x\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = -|x\rangle|-\rangle$.

In summary, the ancilla state $|-\rangle$ remains unchanged, but its phase is "kicked back" to the main register. The overall transformation is exactly what we need:

$$U_P(|x\rangle) = (-1)^{P(x)}|x\rangle$$

After this step, the amplitude of the marked state is negative, while all others remain positive.

- **b) Inversion About the Average (Diffusion Operator D)**: This operation reflects every amplitude about the average amplitude of all states. The transformation is given by:

$$\sum_{i=0}^{N-1} a_i|x_i\rangle \longrightarrow \sum_{i=0}^{N-1}(2A - a_i)|x_i\rangle \quad \text{where } A = \frac{1}{N}\sum_i a_i$$

Since the marked state's amplitude was made negative by the oracle, its distance from the average is large. This reflection dramatically increases its amplitude, while the amplitudes of all other states (which were slightly above the average) are decreased.

The full Grover operator is $G = DU_P$.

3. **Repetition and Measurement**: The Grover iteration is repeated a specific number of times. The optimal number of iterations is approximately:

$$\text{Iterations} \approx \frac{\pi}{4}\sqrt{N} = \frac{\pi}{4}\sqrt{2^n}$$

After this many iterations, the amplitude of the marked state $|x_0\rangle$ is very close to 1. A final measurement of the register will then yield the correct answer x_0 with a very high probability (failure rate of $\approx 2^{-n}$). Repeating the process more or fewer times will decrease the probability of success.

6 Acknowledge

This note were compiled as part of the Quantum Information Summer Camp at Xidian University, based on lectures by Prof. Keqin Feng and Prof. Shaoming Fei. Special thanks to Zhouyu Quan for discussion.

7 References

[1] Charles H Bennett and Gilles Brassard. 'Quantum cryptography: Public key distribution and coin tossing'. In: *Theoretical computer science* 560 (2014), pp. 7–11.

[2] Peter W Shor. 'Algorithms for quantum computation: discrete logarithms and factoring'. In: *Proceedings 35th annual symposium on foundations of computer science*. Ieee. 1994, pp. 124–134.

[3] Lov K Grover. ‘A fast quantum mechanical algorithm for database search’. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. 1996, pp. 212–219.