Procesamiento Cuántico de Información

Ariel Bendersky[1]

[1]Departamento de Computación - FCEyN - Universidad de Buenos Aires

Clase 6

Clase 6

- Búsqueda de período.
- Factorización. Algoritmo de Shor.
- Teorema del no clonación.

Algoritmo de factorización de Shor

Definición

Dado un número $n \in \mathbb{N}$ encontrar sus factores primos.

Motivaciones

- El mejor algoritmo clásico conocido demanda recursos suprapolinomiales en el número de dígitos de n ($O(e^{(64/9+o(1))(\log n)^{1/3}(\log\log n)^{2/3}})$).
- Gran parte de la criptografía clásica (RSA) basa su seguridad en que es difícil factorizar números grandes.
- Si los factorizamos con una computadora cuántica, necesitamos una criptografía más segura (cuántica, tal vez).

Algoritmo de factorización de Shor

Definición

Dado un número $n \in \mathbb{N}$ encontrar sus factores primos.

Motivaciones

- El mejor algoritmo clásico conocido demanda recursos suprapolinomiales en el número de dígitos de n ($O(e^{(64/9+o(1))(\log n)^{1/3}(\log\log n)^{2/3}})$).
- Gran parte de la criptografía clásica (RSA) basa su seguridad en que es difícil factorizar números grandes.
- Si los factorizamos con una computadora cuántica, necesitamos una criptografía más segura (cuántica, tal vez).

Algoritmo de factorización de Shor

Definición

Dado un número $n \in \mathbb{N}$ encontrar sus factores primos.

Motivaciones

- El mejor algoritmo clásico conocido demanda recursos suprapolinomiales en el número de dígitos de n ($O(e^{(64/9+o(1))(\log n)^{1/3}(\log\log n)^{2/3}})$).
- Gran parte de la criptografía clásica (RSA) basa su seguridad en que es difícil factorizar números grandes.
- Si los factorizamos con una computadora cuántica, necesitamos una criptografía más segura (cuántica, tal vez).

Algoritmo de factorización de Shor

Definición

Dado un número $n \in \mathbb{N}$ encontrar sus factores primos.

Motivaciones

- El mejor algoritmo clásico conocido demanda recursos suprapolinomiales en el número de dígitos de n ($O(e^{(64/9+o(1))(\log n)^{1/3}(\log\log n)^{2/3}})$).
- Gran parte de la criptografía clásica (RSA) basa su seguridad en que es difícil factorizar números grandes.
- Si los factorizamos con una computadora cuántica, necesitamos una criptografía más segura (cuántica, tal vez).

El algoritmo de Shor

Pasos:

- Transformada de Fourier cuántica.
- Búsqueda de período.
- Factorización (usando búsqueda de período).

El algoritmo de Shor

Pasos:

- Transformada de Fourier cuántica.
- Búsqueda de período.
- Factorización (usando búsqueda de período).

El algoritmo de Shor

Pasos:

- Transformada de Fourier cuántica.
- Búsqueda de período.
- Factorización (usando búsqueda de período).

1 - Transformada de Fourier cuántica

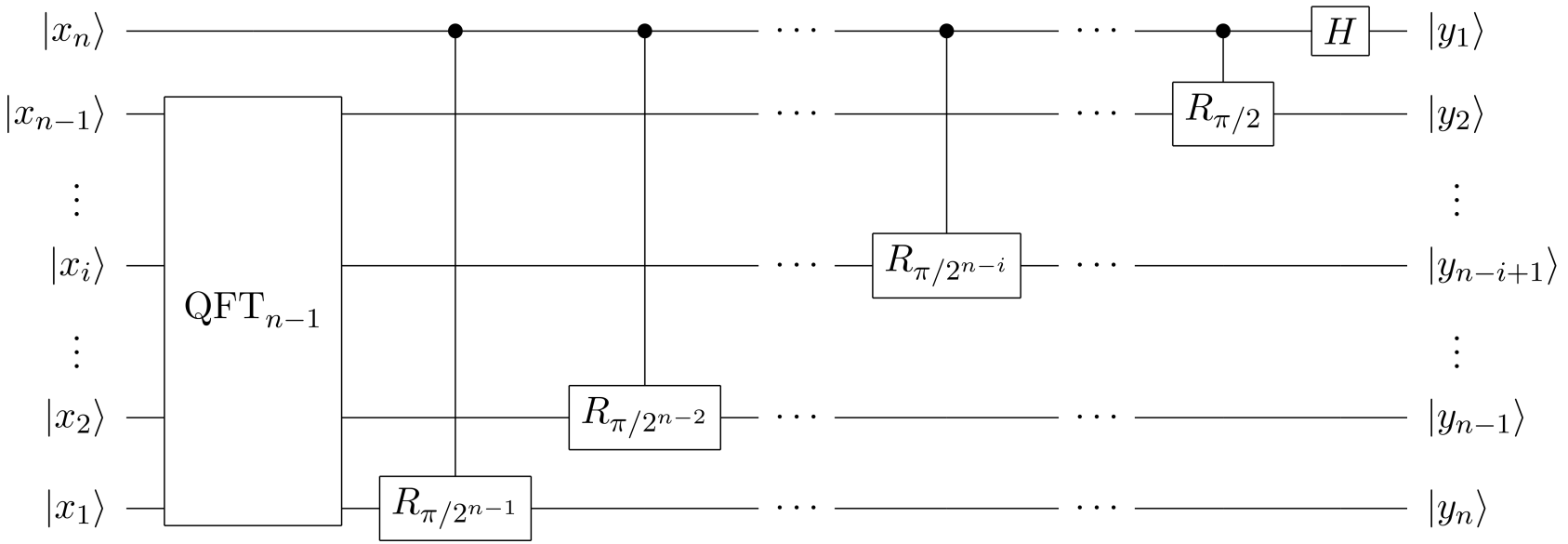
Definición

Está inspirada en la transformada de Fourier discreta. Es una transformación unitaria que actúa como:

$$|j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{2\pi ijk}{2^n}} |k\rangle$$

1 - Transformada de Fourier cuántica

$$|j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{2\pi ijk}{2^n}} |k\rangle$$



Donde $R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$. Los recursos necesarios son $O(n^2)$.

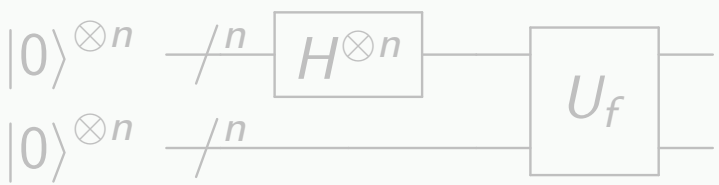
2 - Búsqueda de período

Definición

Sea $f : \{0, ..., N-1\} \to \{0, ..., N-1\}$ una función de período r (es decir, $f(x+r) = f(x)$ para todo x). Se desea encontrar el período r. No se conoce una solución clásica eficiente. Si $N = 2^n$, queremos una solución que use recursos polinomiales en n.

Primer paso

Construyo el estado $\sum_{x=0}^{N-1} |x\rangle |f(x)\rangle$ usando:



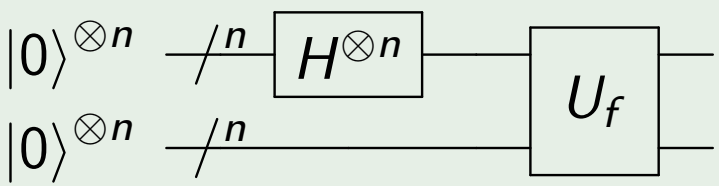
2 - Búsqueda de período

Definición

Sea $f : \{0, ..., N-1\} \to \{0, ..., N-1\}$ una función de período r (es decir, $f(x+r) = f(x)$ para todo x). Se desea encontrar el período r. No se conoce una solución clásica eficiente. Si $N = 2^n$, queremos una solución que use recursos polinomiales en n.

Primer paso

Construyo el estado $\sum_{x=0}^{N-1} |x\rangle |f(x)\rangle$ usando:



2 - Búsqueda de período

Paso innecesario

Medir el segundo registro (no importa el resultado). En el primer registro tenemos:

$$\frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle$$

Es decir, tenemos en el primer registro todos los x (cantidad A) tales que $f(x) = f(x_0)$. [a]
Queremos extraer r de aquí.

[a] Asumimos que la función es no degenerada para simplificar el análisis. No puede dar el mismo resultado en valores que no cumplen ser de la forma $x_0 + jr$.

2 - Búsqueda de período

Segundo paso - Aplicar QFT

Aplicamos QFT:

$$\frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle \rightarrow \frac{1}{\sqrt{NA}} \sum_{y=0}^{N-1} e^{2\pi i x_0 y/N} \sum_{j=0}^{A-1} e^{2\pi i j r y/N} |y\rangle$$

2 - Búsqueda de período

Tercer paso - medir en la base computacional

La probabilidad de obtener cada resultado es

$$Prob(y) = \frac{A}{N} \left| \frac{1}{A} \sum_{j=0}^{A-1} e^{2\pi i j r y / N} \right|^2$$

Esta distribución favorece mucho los valores tales que $yr/N \in \mathbb{N}$. De ahí puede extraerse r escribiendo y/N como fracción irreducible y usando el denominador r' como candidato a r.

3 - Factorización de Shor

Para factorizar se usa el siguiente teorema.

Teorema

Si N es un número compuesto (no primo) de L bits y x es una solución no trivial de la ecuación $x^2 \equiv 1(\mod N)$ en el rango $1 \leq x \leq N$ que, además, no es ni $x \equiv 1(\mod N)$ ni $x \equiv N-1 \equiv -1(\mod N)$, entonces o $gcd(x-1, N)$ o $gcd(x+1, N)$ es un factor no trivial de N. Dicho factor puede encontrarse en $O(L)$ operaciones.

3 - Factorización de Shor

Los pasos del algoritmo de Shor

1. Elegir un número a al azar con $a < N$
2. Calcular $gcd(a, N)$. Si es distinto de 1, encontramos un factor, a y terminar. Si no, seguir.
3. Calcular el período r de $f(x) = a^x \bmod N$. Notemos que $a^r = a^0 = 1 \bmod N$ porque $f(r) = f(0)$, o sea que si r es par, $a^{r/2}$ cumple las hipótesis del teorema anterior.
4. Si r es impar o $a^{r/2} \equiv -1 \bmod N$, volvemos a empezar.
5. Por el teorema anterior, $gcd(a^{r/2} \pm 1, N)$ son posibles factores del número N.

¿Y la probabilidad de éxito?

3 - Factorización de Shor

Los pasos del algoritmo de Shor

1. Elegir un número a al azar con $a < N$
2. Calcular $gcd(a, N)$. Si es distinto de 1, encontramos un factor, a y terminar. Si no, seguir.
3. Calcular el período r de $f(x) = a^x \bmod N$. Notemos que $a^r = a^0 = 1 \bmod N$ porque $f(r) = f(0)$, o sea que si r es par, $a^{r/2}$ cumple las hipótesis del teorema anterior.
4. Si r es impar o $a^{r/2} \equiv -1 \bmod N$, volvemos a empezar.
5. Por el teorema anterior, $gcd(a^{r/2} \pm 1, N)$ son posibles factores del número N.

¿Y la probabilidad de éxito?

3 - Factorización de Shor

Los pasos del algoritmo de Shor

1. Elegir un número a al azar con $a < N$
2. Calcular $gcd(a, N)$. Si es distinto de 1, encontramos un factor, a y terminar. Si no, seguir.
3. Calcular el período r de $f(x) = a^x \bmod N$. Notemos que $a^r = a^0 = 1 \bmod N$ porque $f(r) = f(0)$, o sea que si r es par, $a^{r/2}$ cumple las hipótesis del teorema anterior.
4. Si r es impar o $a^{r/2} \equiv -1 \bmod N$, volvemos a empezar.
5. Por el teorema anterior, $gcd(a^{r/2} \pm 1, N)$ son posibles factores del número N.

¿Y la probabilidad de éxito?

3 - Factorización de Shor

Los pasos del algoritmo de Shor

1. Elegir un número a al azar con $a < N$
2. Calcular $gcd(a, N)$. Si es distinto de 1, encontramos un factor, a y terminar. Si no, seguir.
3. Calcular el período r de $f(x) = a^x \bmod N$. Notemos que $a^r = a^0 = 1 \bmod N$ porque $f(r) = f(0)$, o sea que si r es par, $a^{r/2}$ cumple las hipótesis del teorema anterior.
4. Si r es impar o $a^{r/2} \equiv -1 \bmod N$, volvemos a empezar.
5. Por el teorema anterior, $gcd(a^{r/2} \pm 1, N)$ son posibles factores del número N.

¿Y la probabilidad de éxito?

3 - Factorización de Shor

Los pasos del algoritmo de Shor

1. Elegir un número a al azar con $a < N$
2. Calcular $gcd(a, N)$. Si es distinto de 1, encontramos un factor, a y terminar. Si no, seguir.
3. Calcular el período r de $f(x) = a^x \bmod N$. Notemos que $a^r = a^0 = 1 \bmod N$ porque $f(r) = f(0)$, o sea que si r es par, $a^{r/2}$ cumple las hipótesis del teorema anterior.
4. Si r es impar o $a^{r/2} \equiv -1 \bmod N$, volvemos a empezar.
5. Por el teorema anterior, $gcd(a^{r/2} \pm 1, N)$ son posibles factores del número N.

¿Y la probabilidad de éxito?

3 - Factorización de Shor

Los pasos del algoritmo de Shor

1. Elegir un número a al azar con $a < N$
2. Calcular $gcd(a, N)$. Si es distinto de 1, encontramos un factor, a y terminar. Si no, seguir.
3. Calcular el período r de $f(x) = a^x \bmod N$. Notemos que $a^r = a^0 = 1 \bmod N$ porque $f(r) = f(0)$, o sea que si r es par, $a^{r/2}$ cumple las hipótesis del teorema anterior.
4. Si r es impar o $a^{r/2} \equiv -1 \bmod N$, volvemos a empezar.
5. Por el teorema anterior, $gcd(a^{r/2} \pm 1, N)$ son posibles factores del número N.

¿Y la probabilidad de éxito?

3 - Factorización de Shor

Los pasos del algoritmo de Shor

1. Elegir un número a al azar con $a < N$
2. Calcular $gcd(a, N)$. Si es distinto de 1, encontramos un factor, a y terminar. Si no, seguir.
3. Calcular el período r de $f(x) = a^x \bmod N$. Notemos que $a^r = a^0 = 1 \bmod N$ porque $f(r) = f(0)$, o sea que si r es par, $a^{r/2}$ cumple las hipótesis del teorema anterior.
4. Si r es impar o $a^{r/2} \equiv -1 \bmod N$, volvemos a empezar.
5. Por el teorema anterior, $gcd(a^{r/2} \pm 1, N)$ son posibles factores del número N.

¿Y la probabilidad de éxito?

3 - Factorización de Shor

Definición

Sean x y N coprimos con $x < N$, el *orden* de x módulo N se define como el menor entero positivo r tal que $x^r = 1(\text{mod } N)$.

Teorema

Sea $N = p_1^{\alpha_1}...p_m^{\alpha_m}$ la factorización prima de un número natural compuesto impar. Sea x un entero elegido uniformemente al azar sujeto a que $1 \leq x \leq N-1$ y x coprimo con N. Sea r el orden de $f(x) = x \text{ mod } N$. Entonces

$$p(r \text{ es par y } x^{r/2} \neq -1(\text{mod}N)\ ) \geq 1 - \frac{1}{2^m}.$$

En castellano: la probabilidad de tener que volver a empezar en el slide anterior es muy baja para números con factores grandes.

3 - Factorización de Shor

Definición

Sean x y N coprimos con $x < N$, el *orden* de x módulo N se define como el menor entero positivo r tal que $x^r = 1(\text{mod } N)$.

Teorema

Sea $N = p_1^{\alpha_1}...p_m^{\alpha_m}$ la factorización prima de un número natural compuesto impar. Sea x un entero elegido uniformemente al azar sujeto a que $1 \leq x \leq N-1$ y x coprimo con N. Sea r el orden de $f(x) = x \text{ mod } N$. Entonces

$$p(r \text{ es par y } x^{r/2} \neq -1(\text{mod}N)\ ) \geq 1 - \frac{1}{2^m}.$$

En castellano: la probabilidad de tener que volver a empezar en el slide anterior es muy baja para números con factores grandes.

3 - Factorización de Shor

Ejemplo paso a paso

Supongamos $N = 33$.

1. Elijo a al azar, por ejemplo $a = 5$.
2. Calcular $gcd(a, N)$: $gcd(5, 33) = 1$. Sigo adelante.
3. Calcular el período r de $f(x) = 5^x \bmod 33$. Nos da $r = 10$ (esto lo hice en mi computadora cuántica).
4. Si r es impar o $a^{r/2} \equiv -1 \bmod N$, volvemos a empezar. r es par y $5^5 \equiv 23 \bmod 33$, entonces sigo.
5. Por el teorema anterior, $gcd(5^5 \pm 1, 33)$ son posibles factores del número 33. Esos son $gcd(3126, 33) = 3$ y $gcd(3124, 33) = 11$. Bingo.

3 - Factorización de Shor

Ejemplo paso a paso

Supongamos $N = 33$.

1. Elijo a al azar, por ejemplo $a = 5$.
2. Calcular $gcd(a, N)$: $gcd(5, 33) = 1$. Sigo adelante.
3. Calcular el período r de $f(x) = 5^x \bmod 33$. Nos da $r = 10$ (esto lo hice en mi computadora cuántica).
4. Si r es impar o $a^{r/2} \equiv -1 \bmod N$, volvemos a empezar. r es par y $5^5 \equiv 23 \bmod 33$, entonces sigo.
5. Por el teorema anterior, $gcd(5^5 \pm 1, 33)$ son posibles factores del número 33. Esos son $gcd(3126, 33) = 3$ y $gcd(3124, 33) = 11$. Bingo.

3 - Factorización de Shor

Ejemplo paso a paso

Supongamos $N = 33$.

1. Elijo a al azar, por ejemplo $a = 5$.
2. Calcular $gcd(a, N)$: $gcd(5, 33) = 1$. Sigo adelante.
3. Calcular el período r de $f(x) = 5^x \bmod 33$. Nos da $r = 10$ (esto lo hice en mi computadora cuántica).
4. Si r es impar o $a^{r/2} \equiv -1 \bmod N$, volvemos a empezar. r es par y $5^5 \equiv 23 \bmod 33$, entonces sigo.
5. Por el teorema anterior, $gcd(5^5 \pm 1, 33)$ son posibles factores del número 33. Esos son $gcd(3126, 33) = 3$ y $gcd(3124, 33) = 11$. Bingo.

3 - Factorización de Shor

Ejemplo paso a paso

Supongamos $N = 33$.

1. Elijo a al azar, por ejemplo $a = 5$.
2. Calcular $gcd(a, N)$: $gcd(5, 33) = 1$. Sigo adelante.
3. Calcular el período r de $f(x) = 5^x \bmod 33$. Nos da $r = 10$ (esto lo hice en mi computadora cuántica).
4. Si r es impar o $a^{r/2} \equiv -1 \bmod N$, volvemos a empezar. r es par y $5^5 \equiv 23 \bmod 33$, entonces sigo.
5. Por el teorema anterior, $gcd(5^5 \pm 1, 33)$ son posibles factores del número 33. Esos son $gcd(3126, 33) = 3$ y $gcd(3124, 33) = 11$. Bingo.

3 - Factorización de Shor

Ejemplo paso a paso

Supongamos $N = 33$.

1. Elijo a al azar, por ejemplo $a = 5$.
2. Calcular $gcd(a, N)$: $gcd(5, 33) = 1$. Sigo adelante.
3. Calcular el período r de $f(x) = 5^x \bmod 33$. Nos da $r = 10$ (esto lo hice en mi computadora cuántica).
4. Si r es impar o $a^{r/2} \equiv -1 \bmod N$, volvemos a empezar. r es par y $5^5 \equiv 23 \bmod 33$, entonces sigo.
5. Por el teorema anterior, $gcd(5^5 \pm 1, 33)$ son posibles factores del número 33. Esos son $gcd(3126, 33) = 3$ y $gcd(3124, 33) = 11$. Bingo.

Complejidad de Shor

Podemos factorizar usando $O(n^2)$ compuertas (para la QFT) más el oráculo de la exponenciación modular.
En total la complejidad es $O(n^2 \log n \log\log n)$, donde los últimos dos términos son del oráculo.
Factorización es polinomial en una computadora cuántica con probabilidad de éxito alta. La mejor solución clásica conocida requiere recursos que crecen más rápido que cualquier polinomio.

Complejidad de Shor

Podemos factorizar usando $O(n^2)$ compuertas (para la QFT) más el oráculo de la exponenciación modular.
En total la complejidad es $O(n^2 \log n \log\log n)$, donde los últimos dos términos son del oráculo.
Factorización es polinomial en una computadora cuántica con probabilidad de éxito alta. La mejor solución clásica conocida requiere recursos que crecen más rápido que cualquier polinomio.

El Teorema de No-Clonación

Teorema No-Cloning

Idea básica

¿Podríamos crear una copia exacta de un estado cuántico *arbitrario y desconocido*?

¿Por qué nos interesaría?

- Hacer backups de estados cuánticos.
- Implementar corrección de errores "clásica" (basada en redundancia).
- Espiar una comunicación cuántica (haciendo una copia de los qubits transmitidos).

El Teorema

Es imposible construir una máquina cuántica universal que copie perfectamente un estado cuántico arbitrario y desconocido.

Teorema No-Cloning

Idea básica

¿Podríamos crear una copia exacta de un estado cuántico *arbitrario y desconocido*?

¿Por qué nos interesaría?

- Hacer backups de estados cuánticos.
- Implementar corrección de errores "clásica" (basada en redundancia).
- Espiar una comunicación cuántica (haciendo una copia de los qubits transmitidos).

El Teorema

Es imposible construir una máquina cuántica universal que copie perfectamente un estado cuántico arbitrario y desconocido.

Teorema No-Cloning

Idea básica

¿Podríamos crear una copia exacta de un estado cuántico *arbitrario y desconocido*?

¿Por qué nos interesaría?

- Hacer backups de estados cuánticos.
- Implementar corrección de errores "clásica" (basada en redundancia).
- Espiar una comunicación cuántica (haciendo una copia de los qubits transmitidos).

El Teorema

Es imposible construir una máquina cuántica universal que copie perfectamente un estado cuántico arbitrario y desconocido.

Teorema No-Cloning

Idea básica

¿Podríamos crear una copia exacta de un estado cuántico *arbitrario y desconocido*?

¿Por qué nos interesaría?

- Hacer backups de estados cuánticos.
- Implementar corrección de errores "clásica" (basada en redundancia).
- Espiar una comunicación cuántica (haciendo una copia de los qubits transmitidos).

El Teorema

Es imposible construir una máquina cuántica universal que copie perfectamente un estado cuántico arbitrario y desconocido.

Teorema No-Cloning

Idea básica

¿Podríamos crear una copia exacta de un estado cuántico *arbitrario y desconocido*?

¿Por qué nos interesaría?

- Hacer backups de estados cuánticos.
- Implementar corrección de errores "clásica" (basada en redundancia).
- Espiar una comunicación cuántica (haciendo una copia de los qubits transmitidos).

El Teorema

Es imposible construir una máquina cuántica universal que copie perfectamente un estado cuántico arbitrario y desconocido.

Teorema No-Cloning

Declaración Formal

No existe un operador unitario U_{clone} y un estado "vacío" (o de "memoria") $|s\rangle$ tal que para *cualquier* estado cuántico de entrada $|\psi\rangle$, el operador U_{clone} realice la siguiente transformación:

$$U_{clone}(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

- $|\psi\rangle$ es un estado en un espacio de Hilbert $\mathcal{H}$.
- $|s\rangle$ es un estado fijo y conocido en un espacio de Hilbert $\mathcal{H}_s$.
- La salida $|\psi\rangle \otimes |\psi\rangle$ estaría en $\mathcal{H} \otimes \mathcal{H}$.

Demostración por contradicción

- Supongamos que existe tal unitario U_{clone}.
- Consideremos dos estados no ortogonales $|\psi\rangle$ y $|\phi\rangle$ en $\mathcal{H}$.
- Aplicamos U_{clone} a cada uno:

$$U_{\text{clone}}(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle\,, \quad U_{\text{clone}}(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle\,.$$

Conservación del producto interno

Dado que U_{clone} es unitario,

$$(\langle\psi| \otimes \langle s|)\,(|\phi\rangle \otimes |s\rangle) = (\langle\psi| \otimes \langle\psi|)\,(|\phi\rangle \otimes |\phi\rangle)$$

Calculamos ambos lados:

$$\langle\psi \mid \phi\rangle\,\langle s \mid s\rangle = \big(\langle\psi \mid \phi\rangle\big)\big(\langle\psi \mid \phi\rangle\big) = \big(\langle\psi \mid \phi\rangle\big)^2.$$

Como $|s\rangle$ está normalizado, $\langle s \mid s\rangle = 1$, luego

$$\langle\psi \mid \phi\rangle = \big(\langle\psi \mid \phi\rangle\big)^2.$$

Contradicción y conclusión

La ecuación

$$x = x^2, \quad x = \langle \psi \mid \phi \rangle,$$

sólo tiene soluciones reales $x = 0$ ó $x = 1$.

- $x = 1$ implica $|\psi\rangle = |\phi\rangle$ (estados idénticos).
- $x = 0$ implica $|\psi\rangle$ y $|\phi\rangle$ ortogonales.

Esto muestra que *no* se puede clonar simultáneamente dos estados arbitrarios (no ortogonales). Por tanto, no existe un clonador unitario universal. □

Implicaciones del Teorema No-Cloning (I)

Este teorema fundamental tiene profundas consecuencias en el manejo de información cuántica:

- **Corrección de Errores Cuánticos:** No podemos usar técnicas clásicas de redundancia simple (copiar el bit) para proteger la información cuántica de errores. Necesitamos códigos de corrección de errores cuánticos más sofisticados que no clonan, sino que distribuyen la información de otra manera.
- **Comunicación Cuántica y Criptografía:** Un espía no puede interceptar un qubit en tránsito, copiarlo, enviar el original y quedarse con la copia sin perturbar el estado original. Intentar copiarlo (o medirlo para "clonar" el resultado) inevitablemente introduce un cambio detectable en el estado original. ¡Esta es la base de la seguridad en protocolos de criptografía cuántica como BB84!

Implicaciones del Teorema No-Cloning (I)

Este teorema fundamental tiene profundas consecuencias en el manejo de información cuántica:

- **Corrección de Errores Cuánticos:** No podemos usar técnicas clásicas de redundancia simple (copiar el bit) para proteger la información cuántica de errores. Necesitamos códigos de corrección de errores cuánticos más sofisticados que no clonan, sino que distribuyen la información de otra manera.
- **Comunicación Cuántica y Criptografía:** Un espía no puede interceptar un qubit en tránsito, copiarlo, enviar el original y quedarse con la copia sin perturbar el estado original. Intentar copiarlo (o medirlo para "clonar" el resultado) inevitablemente introduce un cambio detectable en el estado original. ¡Esta es la base de la seguridad en protocolos de criptografía cuántica como BB84!

Implicaciones del Teorema No-Cloning (II)

Otras consecuencias importantes incluyen:

- **Medición:** La medición cuántica no es una clonación. Colapsa el estado a un autoestado, "clonando" la información sobre *ese* autoestado específico mientras destruye la información sobre la superposición original. Una medición es irreversible.
- **Distinción de Estados:** Si no puedes clonar estados no ortogonales, tampoco puedes distinguirlos perfectamente con una sola medición. Distinguir un estado cuántico arbitrario de otro requiere múltiples copias (si fueran clonables) o mediciones probabilísticas.

Implicaciones del Teorema No-Cloning (II)

Otras consecuencias importantes incluyen:

- **Medición:** La medición cuántica no es una clonación. Colapsa el estado a un autoestado, "clonando" la información sobre *ese* autoestado específico mientras destruye la información sobre la superposición original. Una medición es irreversible.
- **Distinción de Estados:** Si no puedes clonar estados no ortogonales, tampoco puedes distinguirlos perfectamente con una sola medición. Distinguir un estado cuántico arbitrario de otro requiere múltiples copias (si fueran clonables) o mediciones probabilísticas.

Vimos hoy

- Búsqueda de período.
- Algoritmo de Shor.
- Teorema de no clonado.

La que viene

- Teleportación.
- Estados mixtos.
- Operadores de Pauli generalizados.
- Canales.