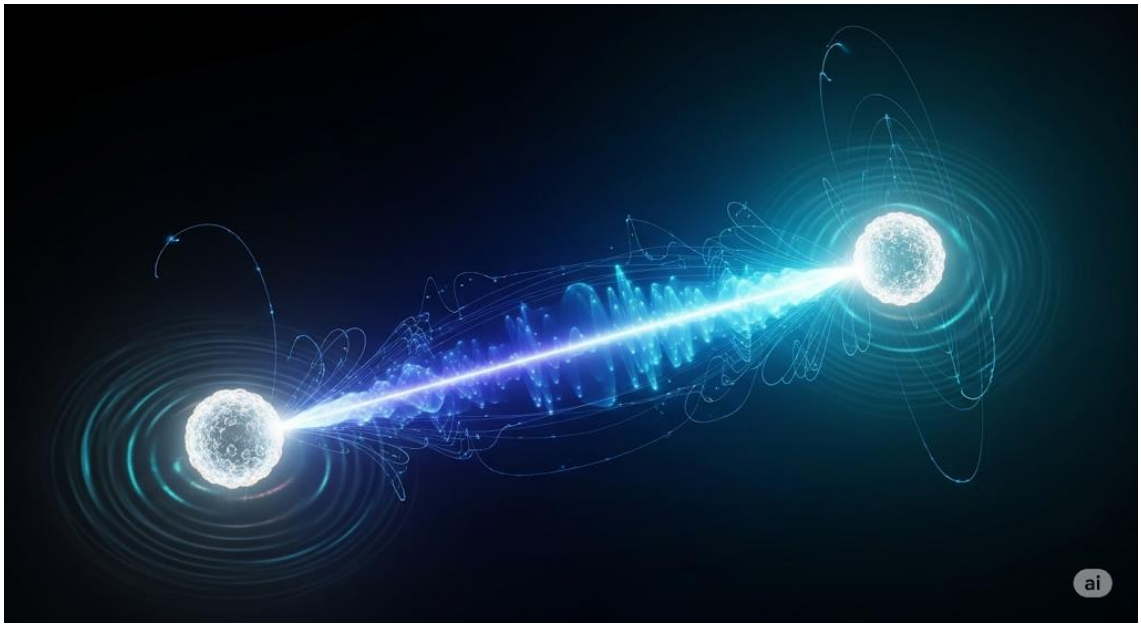
Seniors ICAI

ACTUALIDAD CIENTIFICA

Capítulo II - Fundamentos del Poder Cuántico



1. Introducción: El Cúbit es la Unidad de la Información Cuántica

El cúbit es el análogo cuántico del bit clásico. Si el bit es el "átomo" de la información en la computación digital, el cúbit es su contraparte en el universo cuántico.

El cúbit, por otro lado, se materializa a través de sistemas cuánticos que también poseen dos estados base, representados con la notación |0> y |1>. Algunas implementaciones físicas incluyen:

- **Iones con espín:** Partículas que se comportan como pequeñas peonzas magnéticas, cuyo campo magnético puede apuntar "hacia arriba" (|0>) o "hacia abajo" (|1>).
- **Microcircuitos superconductores:** Circuitos diminutos donde una corriente eléctrica puede girar en un sentido (|0>) o en el contrario (|1>).

La computación cuántica emerge no como una simple mejora incremental, sino como un "salto abismal" hacia un paradigma de cálculo completamente nuevo y radicalmente más potente.

Este salto se debe a que la computación cuántica opera bajo un conjunto de reglas completamente diferente: las de la física cuántica. A diferencia del mundo macroscópico,

ACTUALIDAD CIENTIFICA

Capítulo II - Fundamentos del Poder Cuántico

predecible y determinista, el reino cuántico está gobernado por la probabilidad y fenómenos contraintuitivos.

Dos de estos fenómenos, la **superposición** y el **entrelazamiento**, son la fuente del extraordinario poder de los ordenadores cuánticos. Son posibles gracias a la naturaleza de la unidad fundamental de información cuántica: el **cúbit**.

Los cúbits pueden aprovechar las extrañas leyes de la física cuántica para existir en un estado adicional: una superposición de ambos estados base a la vez, representado como |0> + |1>.

La verdadera potencia del cúbit no reside en su capacidad de ser |0> o |1>, sino en su asombrosa habilidad de ser ambos simultáneamente.

2. El Poder Exponencial de la Superposición

La superposición es la base de la ventaja exponencial de la computación cuántica. Este fenómeno, exclusivo del mundo subatómico, permite que un cúbit explore una vasta cantidad de valores al mismo tiempo, otorgando a los ordenadores cuánticos un paralelismo masivo inherente.

Formalmente, un estado de superposición se describe como una combinación lineal de los estados básicos:

|Ψ> = a|0> + b|1>

Donde los coeficientes a y b son amplitudes de probabilidad (que pueden ser números complejos).

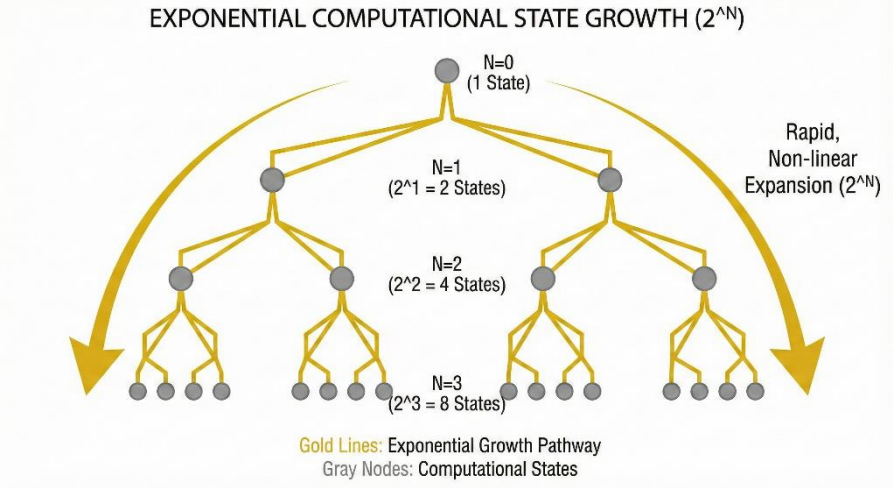
Al medir el cúbit, la probabilidad de obtener el resultado |0> o |1> se obtiene elevando al cuadrado la "magnitud" o "peso" de cada amplitud (matemáticamente, $|a|^2$ y $|b|^2$).

Esta capacidad conduce a un crecimiento exponencial del espacio de estados computacionales. Si un ordenador cuántico dispone de N cúbits, el número de superposiciones posibles es de **2^N**.

- Con **2 cúbits**, el sistema puede estar en $2^2 = 4$ superposiciones a la vez (00, 01, 10, 11).
- Con **3 cúbits**, el sistema puede manejar $2^3 = 8$ superposiciones simultáneamente.

ACTUALIDAD CIENTIFICA

Capítulo II - Fundamentos del Poder Cuántico



Este crecimiento es explosivo. Un sistema hipotético de tan solo **300 cúbits** podría manejar $\mathbf{2^{300}}$ superposiciones, una cifra tan vasta que es comparable al número de átomos en el universo conocido.

Esto permite al ordenador cuántico desarrollar 2^N procesos de cálculo de forma simultánea, una hazaña inalcanzable para cualquier superordenador clásico.

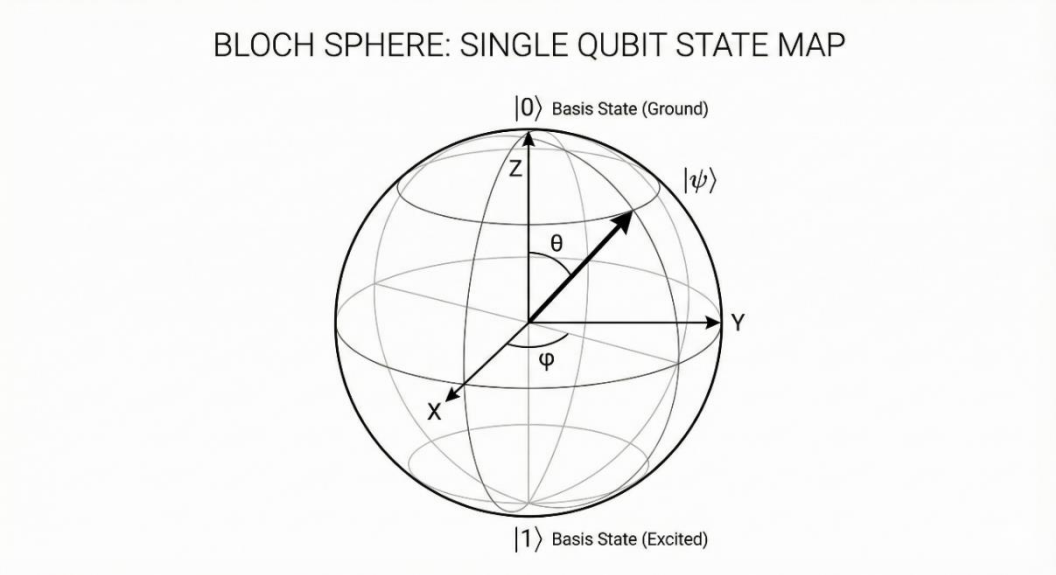
Para facilitar la comprensión de este concepto, los físicos utilizan la **esfera de Bloch**.

En esta representación visual, los polos de la esfera representan los estados definidos |0> (polo norte) y |1> (polo sur).

Cada uno de los infinitos puntos sobre la superficie de la esfera corresponde a una posible superposición ponderada de un cúbit, mapeando visualmente el vasto espacio de estados que esta única unidad de información puede habitar.

ACTUALIDAD CIENTIFICA

Capítulo II - Fundamentos del Poder Cuántico



Si la superposición otorga a los cúbits un vasto espacio para realizar cálculos, el entrelazamiento es el fenómeno que les permite interactuar y correlacionarse de maneras complejas y profundas dentro de ese espacio.

3. Entrelazamiento: Una Conexión "Instantánea"

El entrelazamiento es el segundo pilar del poder cuántico. Se trata de una correlación profunda y no local entre dos o más cúbits, una propiedad misteriosa sin equivalente en el mundo clásico. Este fenómeno se puede ilustrar con el experimento de polarización de fotones, presentado en 1935 por Einstein, Podolsky y Rosen y conocido como el experimento EPR.

Si una fuente emite dos fotones simultáneamente de tal manera que queden entrelazados y se envían en direcciones opuestas, ocurre algo extraordinario. Al medir la polarización de cada fotón con detectores separados (incluso a cientos de kilómetros de distancia), si uno resulta tener polarización horizontal, se sabe con certeza absoluta que el otro tendrá polarización vertical, y viceversa.

Esto plantea una pregunta fundamental: **"¿Cómo sabe un fotón de qué manera se ha polarizado el otro para hacerlo él al contrario?"**. La respuesta es que, en cierto sentido, no son dos partículas independientes, sino un único sistema cuántico correlacionado.

ACTUALIDAD CIENTIFICA

Capítulo II - Fundamentos del Poder Cuántico

La implicación clave del entrelazamiento es que al medir el estado de un cúbit, se conoce instantáneamente el estado de su par entrelazado. Esta propiedad ofrece enormes ventajas, por ejemplo, en comunicaciones seguras. Si un fotón entrelazado es parte de un mensaje, su par puede delatar si el mensaje ha sido interceptado, ya que cualquier medición externa perturbaría el sistema.

La superposición y el entrelazamiento no son meras curiosidades teóricas; son las herramientas que se manipulan mediante circuitos cuánticos para resolver problemas complejos.

4. Circuitos Cuánticos: La Lógica del Cálculo

Para aplicar los principios de superposición y entrelazamiento a la resolución de problemas, los físicos e ingenieros diseñan **circuitos lógicos cuánticos**.

De forma análoga a la computación clásica, estos circuitos utilizan una serie de **puertas cuánticas** que manipulan el estado de los cúbits para ejecutar un algoritmo. Para el usuario, una puerta es como una "caja negra" con una entrada y una salida, que transforma el estado de los cúbits que la atraviesan.

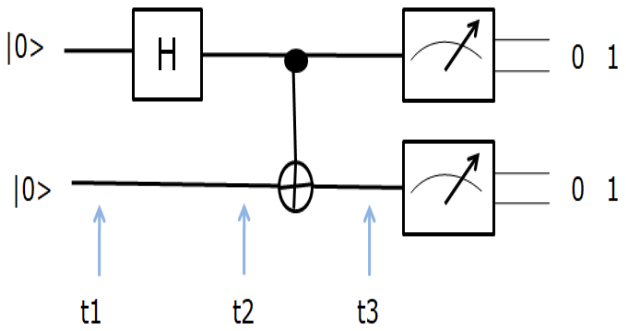
Algunas de las puertas fundamentales son:

- **Puerta X (NOT):** Invierte el estado de un cúbit, transformando |0> en |1> y viceversa.
- **Puerta de Hadamard (H):** Es una de las puertas más importantes, ya que crea superposición. Por ejemplo, transforma un cúbit en estado |0> al estado de superposición equiprobable |+>, que es una combinación de |0> y |1>.
- **Puerta CNOT (Controlada-NO):** Es una puerta de dos cúbits. Un "cúbit de control" determina si el estado del segundo "cúbit objetivo" se invierte. Si el cúbit de control es |1>, el objetivo se invierte; si es |0>, el objetivo no cambia.

Para entender cómo funcionan, analicemos un circuito simple de dos cúbits como el siguiente

ACTUALIDAD CIENTIFICA

Capítulo II - Fundamentos del Poder Cuántico



Estado Inicial (t_1): El sistema comienza con ambos cúbits en el estado |00>.

Aplicación de la Puerta H: Se aplica una puerta Hadamard al primer cúbit. Esto lo pone en superposición. Debido a este principio, ya no podemos hablar de los cúbits por separado, sino que debemos describir el **estado global del sistema**. El estado del sistema pasa a ser $(|0\rangle_1 + |1\rangle_1)|0\rangle_2$. Expandiendo los términos, esto es equivalente a $|0\rangle_1|0\rangle_2 + |1\rangle_1|0\rangle_2$.

Aplicación de la Puerta CNOT (t_2): La puerta CNOT utiliza el primer cúbit como control y el segundo como objetivo. Actúa sobre cada parte de la superposición:

- En la primera parte del estado ($|0\rangle_1|0\rangle_2$), el control es 0, por lo que el objetivo $|0\rangle_2$ no cambia.
- En la segunda parte ($|1\rangle_1|0\rangle_2$), el control es 1, por lo que el objetivo $|0\rangle_2$ se invierte a $|1\rangle_2$. El estado final entrelazado es $|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2$.

Medición (t_3): Al medir este estado global, el sistema "colapsa" a una de las dos posibilidades: se obtendrá 00 o 11, ambas con la misma probabilidad. Es imposible obtener 01 o 10.

La capacidad de construir circuitos lógicos es fundamental. Un hito clave es poder construir un circuito para la **suma**.

Dado que todas las funciones matemáticas pueden desarrollarse en series de Taylor (que se basan en sumas y productos), dominar la suma es el primer paso hacia la computación general.

Estos circuitos son la base de los algoritmos que demuestran la superioridad cuántica.

ACTUALIDAD CIENTIFICA

Capítulo II - Fundamentos del Poder Cuántico

5. El Potencial Demostrado: Algoritmos de Shor y Grover

Los fundamentos teóricos de superposición, entrelazamiento y puertas cuánticas cobran vida en los **algoritmos cuánticos**, que son la demostración más impactante de su potencial.

Los algoritmos de Shor y Grover son los ejemplos paradigmáticos que prueban una superioridad computacional inequívoca sobre sus contrapartes clásicas para problemas específicos.

El Algoritmo de Shor: Una Amenaza a la Criptografía Moderna

El algoritmo de Peter Shor resuelve el problema de la **factorización de números grandes** en sus factores primos.

Para un ordenador clásico, esta tarea es exponencialmente difícil; el tiempo de cálculo crece de forma desmesurada con el número de cifras (ej. a^N).

La seguridad de la criptografía actual, como el sistema RSA que protege nuestras transacciones bancarias y comunicaciones, se basa precisamente en esta dificultad.

Un ordenador cuántico ejecutando el algoritmo de Shor reduce este problema a un tiempo polinómico (ej. $(\log N)^3$), lo que supone una reducción de tiempo abismal.

Podría factorizar en segundos números que a un superordenador clásico le llevaría miles de años, volviendo obsoleta gran parte de la infraestructura de ciberseguridad mundial.

El Algoritmo de Grover: Una Búsqueda Revolucionaria

El algoritmo de Lov Grover aborda otro problema fundamental: la **búsqueda en una base de datos desordenada** de N elementos.

Pensemos en el problema inverso a una guía telefónica: dado un número de teléfono, encontrar a su propietario. Un ordenador clásico tendría, en el peor de los casos, que revisar los N registros uno por uno.

El algoritmo de Grover aprovecha la superposición para reducir drásticamente el número de intentos a aproximadamente la **raíz cuadrada de N ($\sqrt{N}$)**.

Para una base de datos con un millón de elementos, un ordenador clásico podría necesitar hasta un millón de intentos, mientras que uno cuántico con el algoritmo de Grover solo necesitaría unos mil.

ACTUALIDAD CIENTIFICA

Capítulo II - Fundamentos del Poder Cuántico

Estos algoritmos son la prueba tangible de que, al aprovechar directamente la superposición y el entrelazamiento, los ordenadores cuánticos pueden resolver ciertos problemas de una manera fundamentalmente más eficiente. Sin embargo, aprovechar este poder no está exento de enormes desafíos prácticos.

6. Conclusión: Los Retos Fundamentales del Poder Cuántico

A pesar del inmenso potencial teórico y de las pruebas de concepto que ofrecen algoritmos como los de Shor y Grover, la computación cuántica se enfrenta a obstáculos fundamentales que deben superarse para materializar su promesa. Lejos de ser máquinas perfectas, los sistemas cuánticos son increíblemente frágiles y complejos de manejar.

Los dos principales desafíos son:

Lectura de Resultados (El Colapso de la Función de Onda):

La superposición permite realizar un número elevadísimo de cálculos simultáneos. Sin embargo, en el momento en que intentamos "leer" el resultado, el acto de la medición fuerza al sistema a colapsar a un único estado clásico (0 o 1), perdiendo toda la riqueza de la información cuántica que coexistía en la superposición.

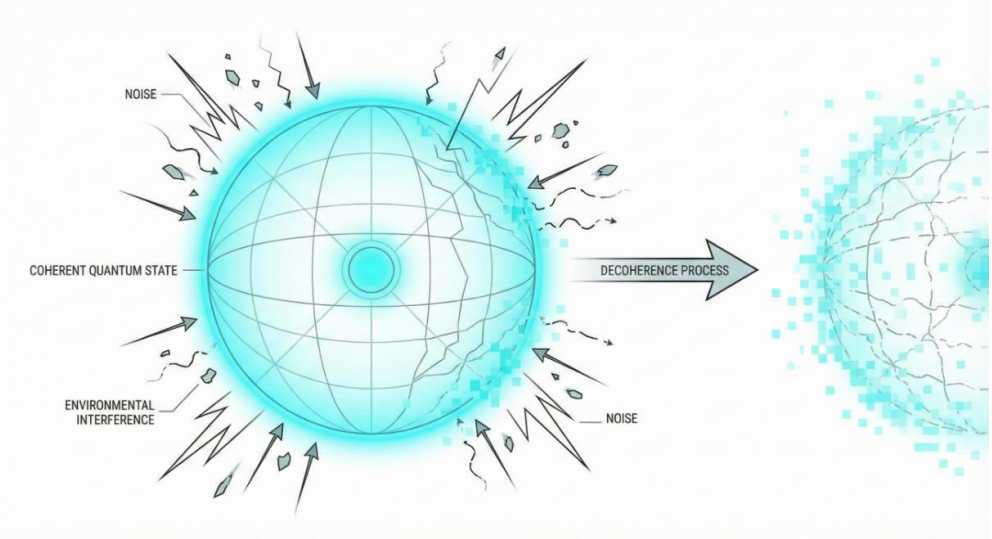
El diseño de algoritmos es, en gran medida, un arte para extraer una respuesta útil antes de que este colapso destruya la ventaja cuántica.

Decoherencia:

Los estados cuánticos como la superposición y el entrelazamiento son extremadamente delicados. La interacción con el entorno (vibraciones, campos electromagnéticos, cambios de temperatura) puede destruir la coherencia del sistema, un proceso llamado decoherencia.

ACTUALIDAD CIENTIFICA

Capítulo II - Fundamentos del Poder Cuántico



Como afirma el físico Michio Kaku, **"la más mínima vibración o ruido puede perturbar la delicada danza de los átomos"**.

Para evitarlo, los procesadores cuánticos deben operar en condiciones de aislamiento extremo y a temperaturas cercanas al cero absoluto (-273 °C).

Superar estos retos mediante el desarrollo de cúbits más estables y, sobre todo, mediante técnicas avanzadas de **corrección de errores cuánticos**, es la clave para desbloquear plenamente la revolución prometida por la computación cuántica y construir máquinas tolerantes a fallos capaces de resolver problemas del mundo real.

Autores:

Enrique Reina Reina

Guillermo García Gila

Javier Pérez Sousa

Todos Seniors ICAI