QMexico Summer School 2026

QPE, Order Finding
y algoritmo de Shor

Estimación de fase, periodicidad y factorización.

Ruta conceptual

Tipo: Resumen

Estructura

Partimos de una pregunta precisa: cómo extraer una fase desconocida de un operador unitario. A partir de eso se construye QPE (Quantum Phase Estimation), después se interpreta la periodicidad modular como una fase estimable y finalmente se conecta el orden obtenido con la factorización.

Mapa de ideas

Criterio

Las fórmulas se usan para explicar por qué el algoritmo funciona. El objetivo principal es comprender cómo una periodicidad aritmética se convierte en un patrón de fase y cómo la QFT inversa transforma ese patrón en un dato medible.

Objetivos

Tipo: Resumen

Objetivos puntuales

Apuntamos a la inicialización con QPE, lectura de fases desde cadenas binarias, potencias controladas en Cirq, orden multiplicativo, fracciones continuas, condiciones de éxito de Shor y resultados probables tras una QFT inversa. Ampliamos esos elementos hasta formar una estimación de fase y factorización.

Aprendizaje

Debemos poder explicar el flujo completo: preparar registros, aplicar potencias controladas, usar QFT inversa para estimar una fase, reconstruir un racional mediante fracciones continuas, interpretar ese racional como información de orden y convertir el orden en factores no triviales.

Prerrequisitos

Tipo: Concepto

Base asumida

Se utilizarán números complejos, amplitudes, fases cuánticas, QFT, compuertas controladas y notación de registros como conocimientos previos. No se repite su introducción básica porque en este módulo se usan como herramientas ya disponibles.

Nuevo foco conceptual

La pregunta central ya no es cómo construir la QFT, sino por qué la QFT inversa permite leer una fase codificada por potencias controladas y cómo esa lectura se convierte en información aritmética útil.

El problema de estimar una fase

Tipo: Concepto

Qué problema resuelve

Dado un operador unitario U y un estado propio $|u\rangle$, queremos estimar φ tal que $U|u\rangle = e^{2\pi i\varphi}|u\rangle$. La fase no aparece como un bit escrito directamente; está codificada en la respuesta del operador sobre un estado propio.

Por qué es necesario

Muchos problemas cuánticos y aritméticos esconden información en eigenvalores. QPE transforma esa información espectral en una cadena binaria medible, lo que convierte una propiedad analítica de un operador en un dato computacional.

Eigenvalores de operadores unitarios

Tipo: Concepto

Hecho estructural

Si U es unitario, sus eigenvalores tienen módulo uno. Por tanto se escriben como $\lambda = e^{2\pi i \varphi}$ con $\varphi \in [0, 1)$.

Interpretación

La fase describe una posición angular en el círculo complejo. QPE no estima el eigenvector: asume que el registro de trabajo contiene un estado propio adecuado y extrae la fase asociada al eigenvalor.

Eigenvectores como estados estables

Tipo: Concepto

Papel dentro del algoritmo

Un estado propio no cambia de dirección bajo U; solo adquiere una fase. Esa estabilidad permite repetir potencias de U sin mezclar el registro de trabajo con otros componentes.

Significado físico

El registro de trabajo actúa como una sonda coherente. Al permanecer en la misma dirección vectorial, deja que la información relevante se acumule únicamente como fase en el registro de conteo.

Fase y eigenvalor

Tipo: Concepto

Relación formal

La fase normalizada se define por $\lambda = e^{2\pi i \varphi}$. Dos valores que difieren por un entero representan el mismo eigenvalor, por lo que se toma φ módulo uno.

Lectura computacional

El algoritmo busca aproximar φ mediante una fracción binaria. Medir m qubits de conteo produce un entero y que representa la estimación $y/2^m$.

Motivación histórica de QPE

Tipo: Concepto

Contexto

QPE se convirtió en una subrutina central porque traduce información espectral en información clásica recuperable. Aparece en simulación cuántica, estimación de energías, algoritmos de orden y análisis espectral.

Idea unificadora

La historia conceptual es la misma que en Fourier: fases acumuladas que parecen invisibles en un registro se vuelven medibles cuando se las somete a una transformada inversa adecuada.

Aplicaciones científicas de estimar fases

Tipo: Concepto

Más allá de factorización

En física, las fases de operadores de evolución contienen energías; en química cuántica, permiten estimar niveles moleculares; en aritmética, revelan periodicidad. La misma arquitectura aparece en problemas distintos porque todos comparten estructura espectral.

Implicación

QPE muestra que una computadora cuántica no solo manipula probabilidades: también convierte información de fase acumulada en resultados discretos que pueden procesarse clásicamente.

Arquitectura general de QPE

Tipo: Concepto

Dos registros

El registro de conteo almacena la estimación binaria de la fase. El registro de trabajo contiene el estado propio del operador. La separación permite que una parte acumule fase y la otra mantenga estable la referencia espectral.

Flujo

El algoritmo prepara superposición en el conteo, aplica potencias controladas de U, ejecuta la QFT inversa sobre el conteo y mide una cadena binaria que aproxima la fase.

Registro de conteo

Tipo: Concepto

Función

El registro de conteo representa enteros $k = 0, \ldots, 2^m - 1$. Después de aplicar Hadamards, contiene todos esos valores con la misma amplitud, de modo que cada valor puede controlar una potencia distinta de U.

Papel conceptual

No se usa para consultar muchas respuestas clásicas en paralelo. Se usa para crear interferencia entre diferentes potencias de la misma fase.

Registro de trabajo

Tipo: Concepto

Inicialización

En QPE ideal, el segundo registro se inicializa como un eigenvector de U. En order finding se usa una variante donde el estado $|1\rangle$ puede descomponerse como superposición de eigenvectores relevantes.

Por qué importa

Si el registro de trabajo no contiene componentes propios del operador adecuado, las fases acumuladas no tendrán una interpretación simple y la medición del conteo no estimará la fase deseada.

Estado inicial de QPE

Tipo: Método

Preparación mínima

El estado ideal es $|0\rangle^{\otimes m}|u\rangle$. Tras Hadamards en el conteo se obtiene $\frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} |k\rangle|u\rangle$.

Interpretación

El registro de conteo queda preparado para explorar coherentemente todas las potencias necesarias. El registro de trabajo permanece como referencia espectral.

Potencias controladas

Tipo: Concepto

Operación central

Cada qubit del conteo controla una potencia U^{2^j}. En conjunto, esas operaciones implementan una fase dependiente del entero k almacenado en el conteo.

Por qué se usan potencias

Las potencias $1, 2, 4, \ldots$ permiten escribir la fase en base dos. El algoritmo no calcula la fase dígito por dígito de forma clásica; la hace aparecer como patrón Fourier sobre el registro de conteo.

Acumulación de fase

Tipo: Método

Transformación esencial

Si $U|u\rangle = e^{2\pi i\varphi}|u\rangle$, entonces $U^k|u\rangle = e^{2\pi ik\varphi}|u\rangle$. Después de las potencias controladas aparece $2^{-m/2}\sum_k e^{2\pi ik\varphi}|k\rangle|u\rangle$.

Lectura

La fase desconocida quedó escrita como una onda discreta sobre el registro de conteo.

Qué aporta la QFT inversa

Tipo: Concepto

Problema que resuelve

El estado del conteo contiene una frecuencia φ, pero la medición directa no lee frecuencias. La QFT inversa transforma esa onda de fase en una concentración de probabilidad alrededor del entero que mejor representa $2^m\varphi$.

Interpretación física

La QFT inversa realiza interferencia: los valores compatibles con la fase se refuerzan y los incompatibles se cancelan parcialmente.

Medición y estimador

Tipo: Método

Regla de lectura

Si el resultado medido es $y \in \{0, \ldots, 2^m - 1\}$, la estimación básica es $\widehat{\varphi} = y/2^m$.

Significado

La medición no devuelve un eigenvalor complejo. Devuelve una aproximación racional de la fase normalizada que parametriza ese eigenvalor.

Caso exacto

Tipo: Concepto

Cuándo ocurre

Si φ tiene una expansión binaria finita con a lo sumo m bits, entonces $2^m\varphi$ es un entero. En ese caso la QFT inversa concentra toda la probabilidad en la cadena correspondiente.

Implicación

Este caso muestra la versión ideal de QPE: una fase compatible con la resolución del registro se recupera exactamente en el modelo sin ruido.

Caso aproximado

Tipo: Concepto

Qué cambia

Si $2^m\varphi$ no es entero, la probabilidad se distribuye alrededor de los enteros más cercanos. La salida más frecuente sigue siendo informativa, pero ya no existe concentración perfecta.

Interpretación

La precisión depende del número de qubits de conteo. Más qubits significan una malla más fina de fracciones, aunque también requieren más recursos de circuito.

Fases como fracciones binarias

Tipo: Concepto

Representación

Una fase $\varphi \in [0, 1)$ puede escribirse como $0.\varphi_1\varphi_2\cdots$ en base dos. El registro de conteo intenta recuperar los primeros bits significativos de esa expansión.

Por qué importa

Cuando la fase tiene forma s/r, la estimación binaria debe traducirse a una fracción racional mediante posprocesamiento clásico.

Precisión y número de qubits

Tipo: Concepto

Resolución

Con m qubits se distinguen 2^m posibles resultados.
La separación entre dos estimaciones consecutivas es $1/2^m$.

Costo

Aumentar m mejora la precisión, pero incrementa el número de potencias controladas y el tamaño de la QFT inversa. QPE equilibra resolución estadística y complejidad del circuito.

Distribución de probabilidad

Tipo: Concepto

Lectura matemática

La distribución de medición tiene picos cerca de los enteros y para los cuales $y/2^m$ aproxima bien a φ. Esta distribución es una versión discreta del fenómeno de interferencia.

Lectura experimental

En simulación o hardware real, los histogramas de conteos son la forma práctica de observar si la fase fue estimada con éxito.

Ejemplo: lectura de una cadena binaria

Tipo: Ejemplo

Problema

Supongamos que el registro de conteo tiene $m = 3$ qubits y la medición más frecuente es 101_2. Queremos interpretar esa salida como estimación de fase.

Desarrollo

La cadena 101_2 representa el entero 5. Con tres qubits, la resolución es $2^3 = 8$, por lo que $\widehat{\varphi} = 5/8$.

Conclusión

El resultado es una fracción de vuelta en el círculo complejo. La fase estimada corresponde al eigenvalor $e^{2\pi i(5/8)}$.

Ejemplo: potencias controladas en Cirq

Tipo: Ejemplo

Problema

En implementaciones de QPE se requiere construir la potencia 2^i de una compuerta controlada. Esto aparece porque el qubit i del conteo representa el peso binario 2^i.

Código conceptual

En Cirq, una forma pedagógica es definir CU y luego usar `CU**(2**i)` para obtener la potencia controlada adecuada.

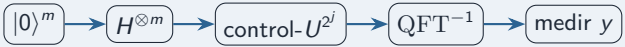
Interpretación

La línea expresa la estructura matemática de QPE, donde cada qubit controla una potencia duplicada de la unidad anterior.

Diagrama conceptual de QPE

Tipo: Resumen

Estructura



Lectura

El circuito convierte eigenfase en entero medible. La parte cuántica estima una fracción; la parte clásica interpreta esa fracción según el problema.

Qué significa una salida de QPE

Tipo: Concepto

Interpretación matemática

Una salida y indica que la fase del eigenvalor está cerca de $y/2^m$. El contenido físico no está en el bit string por sí mismo, sino en su relación con la resolución del registro de conteo.

Implicación

QPE es una interfaz: toma información espectral de un operador y la entrega como dato clásico aproximado.

Condiciones de fallo en QPE

Tipo: Concepto

Fuentes conceptuales

Puede fallar la interpretación si el estado de trabajo no es un eigenvector, si la fase requiere más precisión que la disponible, si las potencias controladas no implementan el operador correcto o si el ruido destruye coherencia.

Diagnóstico

La salida debe analizarse como distribución. Un resultado inesperado puede indicar resolución insuficiente, convención de bits o implementación incorrecta de controles.

Transición a order finding

Tipo: Concepto

Cambio de problema

Order finding pregunta por el menor entero positivo r tal que $x^r \equiv 1 \pmod{N}$. A primera vista esto es aritmética modular, no espectros cuánticos. La idea profunda es construir un operador unitario cuya fase revele esa periodicidad.

Conexión

QPE entra porque los eigenvalores del operador modular contienen fracciones s/r. Estimar fases se convierte en estimar una razón ligada al orden.

Congruencias modulares

Tipo: Concepto

Definición operativa

Dos enteros son congruentes módulo N si tienen el mismo residuo al dividir por N. En order finding se estudia la secuencia $1, x, x^2, x^3, \ldots$ reducida módulo N.

Por qué importa

La secuencia no crece indefinidamente: al trabajar módulo N, eventualmente repite. El primer retorno a 1 define el orden multiplicativo.

Orden multiplicativo

Tipo: Concepto

Definición formal

Si $\gcd(x, N) = 1$, el orden de x módulo N es $r = \min\{t > 0 : x^t \equiv 1 \pmod{N}\}$.

Interpretación

El orden mide la longitud del ciclo generado por multiplicar repetidamente por x en el grupo de unidades módulo N.

Funciones periódicas y orden

Tipo: Concepto

Periodicidad

La función $f(a) = x^a$ mód N cumple $f(a+r) = f(a)$ cuando r es el orden. Por tanto, encontrar el orden equivale a encontrar el período de esta función modular.

Implicación cuántica

La QFT y QPE son útiles porque las transformadas de Fourier están diseñadas para revelar periodicidad.

Operador modular U_x

Tipo: Concepto

Definición conceptual

El operador relevante actúa como $U_x|y\rangle = |xy \text{ mód } N\rangle$ cuando x y N son coprimos.

Por qué es unitario

Multiplicar por x módulo N permuta los residuos coprimos con N. Una permutación de estados base define una operación reversible, y por tanto puede representarse unitariamente.

Eigenvalores de U_x

Tipo: Concepto

Estructura

Los eigenvalores de U_x tienen forma $e^{2\pi i s/r}$ para enteros s asociados a los modos del ciclo de longitud r.

Consecuencia

Si QPE estima una fase de U_x, lo que entrega no es directamente r, sino una aproximación a alguna fracción s/r.

Por qué se puede iniciar en $|1>$

Tipo: Concepto

Problema aparente

QPE ideal requiere un eigenvector, pero en order finding no preparamos explícitamente los eigenvectores de U_x.

Resolución conceptual

El estado $|1\rangle$ puede expresarse como superposición de eigenvectores del ciclo. Al ejecutar QPE, la medición selecciona coherentemente una de las fases s/r.

Modular exponentiation

Tipo: Concepto

Qué implementa

La exponenciación modular controlada aplica transformaciones equivalentes a multiplicar por x^{2^j} módulo N condicionadas por los bits del registro de conteo.

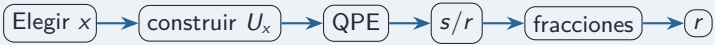
Papel computacional

Es el bloque caro de Shor. La ventaja conceptual de QPE solo se vuelve un algoritmo útil si estas potencias modulares se implementan reversiblemente con costo polinomial.

Flujo de order finding

Tipo: Resumen

Proceso



Lectura

La parte cuántica produce una aproximación de fase; la parte clásica reconstruye el período mediante aritmética racional.

Ejemplo: orden de 4 módulo 81

Tipo: Ejemplo

Problema

Determinar el menor r tal que $4^r \equiv 1 \pmod{81}$.

Desarrollo

Calculando potencias modulares se obtiene una secuencia que eventualmente regresa a 1. El primer retorno define el orden y puede verificarse con una rutina clásica para instancias pequeñas.

Interpretación

El procedimiento clásico verifica el resultado en una instancia pequeña. En Shor, la meta es obtener ese período eficientemente mediante QPE cuando los tamaños son grandes.

Visualización de periodicidad

Tipo: Concepto

Patrón

La secuencia x^a mód N se repite con período r. Si se grafica el residuo contra a, el periodo aparece como repetición de valores; si se transforma, aparece como concentración espectral.

Conexión con QFT

La QFT inversa que aparece en QPE es el mecanismo que traduce una periodicidad de fase en picos de medición.

Qué se mide en order finding

Tipo: Concepto

Salida real

El primer registro no devuelve r directamente. Devuelve un entero y que aproxima $2^m(s/r)$ para algún s.

Implicación

El algoritmo necesita posprocesamiento. Sin fracciones continuas, el resultado cuántico es solo una aproximación binaria; con fracciones continuas puede convertirse en un candidato a periodo.

Por qué entran fracciones continuas

Tipo: Concepto

Problema que resuelven

Dada una aproximación numérica a s/r, queremos reconstruir la fracción con denominador razonable que probablemente produjo esa aproximación.

Ventaja matemática

Las fracciones continuas generan convergentes que son las mejores aproximaciones racionales en un sentido preciso. Por eso son la herramienta natural para pasar de $y/2^m$ a un candidato para r.

Convergentes

Tipo: Método

Definición

Una fracción continua $[a_0, a_1, \ldots, a_n]$ produce una sucesión de racionales llamados convergentes. Cada convergente aproxima mejor al número original con denominadores crecientes.

Lectura algorítmica

En order finding se prueban denominadores de convergentes hasta encontrar un r que satisfaga $x^r \equiv 1$ (mód N).

Ejemplo: $[1, 4, 2, 1]$

Tipo: Ejemplo

Problema

Obtener convergentes de una fracción continua corta.

Desarrollo

Los primeros convergentes son 1, 5/4, 11/9 y luego el convergente completo.
Cada uno representa una aproximación racional candidata.

Interpretación

No todo convergente será el período correcto en un problema de orden.
Cada candidato debe validarse con la congruencia modular.

Recuperar r desde s/r

Tipo: Método

Procedimiento

A partir de $y/2^m$, se calculan convergentes. Para cada denominador candidato q, se verifica si $x^q \equiv 1$ (mód N). El primer candidato válido puede tomarse como orden.

Criterio

La reconstrucción es una etapa clásica esencial. QPE da una aproximación; el algoritmo aritmético decide si el denominador candidato realmente explica la periodicidad.

Cuando s y r no son coprimos

Tipo: Concepto

Problema

Si la fase estimada es s/r y s comparte factores con r, la fracción reducida tendrá un denominador menor que r.

Consecuencia

El candidato puede no ser el orden completo. En ese caso se repite el procedimiento o se prueban múltiplos del denominador hasta verificar la congruencia.

Posprocesamiento clásico

Tipo: Concepto

Papel

Después de QPE, todo el algoritmo depende de aritmética clásica: fracciones continuas, validación modular, cálculo de máximos comunes divisores y verificación de factores.

Mensaje central

Shor no es un circuito aislado. Es una arquitectura híbrida donde la parte cuántica revela periodicidad y la parte clásica convierte esa periodicidad en factores.

Transición a Shor

Tipo: Concepto

Cambio de escala

Order finding es la subrutina que hace posible la factorización. Shor muestra que, si podemos encontrar órdenes eficientemente, entonces podemos factorizar enteros compuestos con alta probabilidad.

Idea central

La factorización se reduce a encontrar una periodicidad modular. QPE proporciona el mecanismo para extraer esa periodicidad.

Problema de factorización

Tipo: Concepto

Enunciado

Dado un entero compuesto N, queremos encontrar factores no triviales p, q tales que $N = pq$ o una descomposición no trivial de N.

Motivación criptográfica

La dificultad práctica de factorizar enteros grandes sostiene esquemas criptográficos clásicos ampliamente usados. Shor es importante porque ofrece un algoritmo cuántico polinomial bajo el modelo ideal de computación tolerante a fallos.

Reducción de factorización a orden

Tipo: Concepto

Idea matemática

Se elige x coprimo con N y se encuentra su orden r. Si r es par y $x^{r/2} \not\equiv -1 \pmod{N}$, entonces $\gcd(x^{r/2}-1, N)$ y $\gcd(x^{r/2}+1, N)$ pueden revelar factores no triviales.

Interpretación

El orden produce una diferencia de cuadrados: $x^r - 1 = (x^{r/2}-1)(x^{r/2}+1)$. La aritmética modular transforma esa identidad en un método de factorización.

Selección de x

Tipo: Método

Procedimiento

Se elige un entero aleatorio $1 < x < N$. Si $\gcd(x, N) > 1$, ya se encontró un factor. Si $\gcd(x, N) = 1$, se ejecuta order finding para obtener el orden de x módulo N.

Por qué hay azar

No todos los valores de x conducen a éxito. Shor es probabilístico por la selección de x y por el resultado de la estimación de fase.

Atajo por máximo común divisor

Tipo: Concepto

Caso favorable

Si el valor elegido x ya comparte un factor no trivial con N, el cálculo clásico de $\gcd(x, N)$ resuelve el problema sin entrar a la parte cuántica.

Implicación

La parte cuántica no sustituye toda la aritmética clásica. Actúa cuando el candidato x es coprimo con N y la dificultad está en obtener su orden.

Por qué se requiere r par

Tipo: Concepto

Razón algebraica

La factorización usa $x^r - 1 = (x^{r/2} - 1)(x^{r/2} + 1)$. Si r es impar, $r/2$ no es entero y esta descomposición no produce los dos términos requeridos.

Consecuencia

Cuando el orden hallado no es par, se elige un nuevo x y se repite. Esto no contradice la eficiencia: la probabilidad de éxito es suficientemente alta al repetir un número moderado de veces.

Evitar el caso trivial -1

Tipo: Concepto

Condición

Aunque r sea par, puede ocurrir que $x^{r/2} \equiv -1 \pmod{N}$. Entonces $x^{r/2}+1 \equiv 0 \pmod{N}$ y los máximos comunes divisores no entregan factores no triviales.

Interpretación

El algoritmo necesita que la diferencia de cuadrados produzca información modular útil. Si cae en el caso trivial, se repite con otro x.

Casos exitosos

Tipo: Resumen

Criterios

Un intento tiene éxito si x es coprimo con N, QPE y fracciones continuas producen el orden correcto o un múltiplo suficiente, r es par y $x^{r/2} \not\equiv -1 \pmod{N}$.

Resultado

Bajo esas condiciones, $\gcd(x^{r/2}-1, N)$ y $\gcd(x^{r/2}+1, N)$ producen factores no triviales con alta probabilidad.

Casos fallidos

Tipo: Resumen

Tipos de fallo

Puede fallar la estimación por precisión insuficiente, la fracción reducida puede no revelar r, el orden puede ser impar o el valor $x^{r/2}$ puede dar el caso trivial -1 módulo N.

Lectura

Estos fallos no invalidan el algoritmo. Definen un proceso probabilístico donde se repite con nuevos parámetros hasta obtener un intento exitoso.

Flujo completo de Shor

Tipo: Resumen

Diagrama

Interpretación

La QFT aparece dentro de QPE, y QPE aparece dentro de order finding. Shor hereda su potencia de esta cadena de reducciones.

Por qué QFT aparece dentro de Shor

Tipo: Concepto

Respuesta conceptual

La periodicidad modular genera fases con estructura racional. La QFT inversa es el instrumento que transforma esa estructura periódica en picos medibles asociados a múltiplos de $2^m/r$.

Implicación

La QFT no se usa como adorno matemático. Es el mecanismo que convierte periodicidad oculta en una distribución de medición interpretable.

Complejidad computacional

Tipo: Concepto

Mensaje central

El algoritmo de Shor ofrece un procedimiento cuántico de tiempo polinomial para factorización en el modelo ideal. La mejora no es una aceleración cuadrática simple; cambia la clase de complejidad conocida para el problema bajo el modelo cuántico.

Matiz

No se ha probado que ningún algoritmo clásico pueda factorizar en tiempo polinomial. La afirmación correcta compara contra los mejores métodos clásicos conocidos y contra la evidencia de dificultad usada en criptografía.

Lo que Shor no afirma

Tipo: Concepto

Aclaración

Shor no demuestra imposibilidad clásica. Tampoco resuelve la factorización práctica de números criptográficos en hardware ruidoso actual sin corrección de errores.

Valor real

Su importancia es teórica y arquitectónica: muestra que la periodicidad cuánticamente accesible puede romper una barrera central de la computación clásica conocida.

Ventaja y condiciones

Tipo: Concepto

Ventaja

La ventaja principal está en encontrar el orden eficientemente. Una vez que el orden está disponible, el resto de la factorización usa aritmética clásica eficiente.

Condiciones

La implementación completa requiere modular exponentiation reversible, suficientes qubits de conteo, QFT inversa, medición confiable y corrección de errores para escalas criptográficas.

Costo de modular exponentiation

Tipo: Concepto

Recurso dominante

La exponenciación modular reversible consume gran parte de los recursos. Construirla requiere aritmética reversible: sumadores, multiplicadores modulares, registros auxiliares y descomputación.

Interpretación práctica

Aunque QPE sea conceptualmente elegante, el costo real de Shor vive en implementar $U_x^{2^j}$ de forma reversible y escalable.

Escalabilidad y hardware

Tipo: Concepto

Situación conceptual

El algoritmo ideal es polinomial, pero las implementaciones físicas requieren baja tasa de error, muchos qubits lógicos y circuitos profundos.

Implicación

La teoría justifica la amenaza criptográfica a largo plazo. La ejecución práctica a gran escala depende de avances en corrección de errores y arquitecturas tolerantes a fallos.

Corrección de errores: nivel necesario

Tipo: Concepto

Alcance

No se desarrolla teoría de corrección de errores en este módulo. Solo se identifica su papel: mantener coherencia durante circuitos largos y permitir puertas lógicas confiables.

Conexión

Shor es un ejemplo donde la diferencia entre algoritmo ideal y ejecución física es central. Comprender esa diferencia evita confundir una demostración matemática con una implementación inmediata.

QPE en Qiskit: estructura manual

Tipo: Método

Código conceptual

El esqueleto contiene tres bloques: Hadamards sobre el conteo, potencias controladas de U y QFT inversa antes de medir. En Qiskit esto se expresa con un circuito de m qubits de conteo y un registro de trabajo.

Interpretación

El código debe expresar la arquitectura, no ocultarla. Primero se crea interferencia entre potencias, luego se decodifica con QFT inversa.

QPE en Cirq: potencias controladas

Tipo: Método

Código conceptual

Para una compuerta controlada CU, la potencia del qubit i puede expresarse como `CU**(2**i)`. Esta sintaxis representa directamente el peso binario 2^i del registro de conteo.

Lectura

El exponente duplicado por 2^i es la implementación directa de la fase acumulada por el bit i del registro de conteo.

Construcción de la QFT inversa

Tipo: Método

Bloques

La QFT inversa se implementa invirtiendo el circuito de QFT: SWAPs según convención, compuertas controladas de fase con signo opuesto y Hadamards en orden inverso.

Papel

No introduce nueva información. Reorganiza amplitudes para que la fase acumulada aparezca como una etiqueta binaria medible.

Potencias controladas en Qiskit

Tipo: Método

Patrón

En Qiskit se puede construir una compuerta base, elevarla a potencias o repetir bloques controlados, y componerlos condicionados por qubits del registro de conteo.

Precaución

La convención de orden de bits afecta cómo se interpreta la cadena medida. La fórmula $y/2^m$ requiere saber qué bit representa el peso más significativo.

Potencias controladas en Cirq

Tipo: Método

Patrón

Cirq permite expresar compuertas elevadas a exponentes y luego aplicarlas sobre qubits específicos. En ejemplos de fase pura, ‘CZPowGate‘ permite modelar un eigenvalor con fase controlada.

Interpretación

Estos ejemplos son pedagógicos: muestran el mecanismo de QPE sin construir aún una exponenciación modular completa.

Ejemplo QPE con compuerta de fase

Tipo: Ejemplo

Problema

Queremos estimar una fase conocida en un circuito pequeño para verificar la mecánica de QPE.

Procedimiento

Se usa un operador diagonal cuyo eigenvector es computacional. Las potencias controladas escriben $e^{2\pi i k\varphi}$ sobre el conteo y la QFT inversa debe concentrar la medición cerca de $2^m\varphi$.

Conclusión

El ejemplo separa la dificultad de estimar fases de la dificultad aritmética de Shor.

Simulación clásica de order finding

Tipo: Método

Propósito

Antes de ejecutar circuitos, conviene verificar periodos con código clásico en instancias pequeñas. Esto ayuda a interpretar resultados de QPE y a validar candidatos obtenidos por fracciones continuas.

Ejemplo

Para $x = 4$ y $N = 81$, una rutina clásica puede multiplicar residuos hasta encontrar el primer retorno a 1. Ese valor es el orden que la parte cuántica debería recuperar indirectamente.

Fracciones continuas en Python

Tipo: Método

Objetivo

Implementar convergentes permite convertir una medición y en candidatos de denominador. El código del notebook muestra cada paso, no solo el resultado final.

Lectura

Esta etapa es determinista. Su éxito depende de que la aproximación cuántica sea suficientemente cercana a una fracción y de que se valide el denominador contra la congruencia modular.

Ejemplo conceptual: Shor para $N = 15$

Tipo: Ejemplo

Problema

Usar un entero pequeño para explicar la reducción sin ocultarla detrás de detalles de hardware.

Desarrollo

Si se elige $x = 2$, el orden módulo 15 es $r = 4$ porque $2^4 \equiv 1 \pmod{15}$. Como r es par, se calculan $\gcd(2^2 - 1, 15) = 3$ y $\gcd(2^2 + 1, 15) = 5$.

Conclusión

El orden convierte una periodicidad modular en factores concretos.

Picos de alta probabilidad

Tipo: Concepto

Interpretación

Cuando el periodo es r, las mediciones del registro de conteo tienden a concentrarse cerca de múltiplos de $2^m/r$. Por eso ciertos enteros aparecen como resultados probables.

Ejemplo

Si $2^m = 512$ y la estructura genera picos separados de forma regular, resultados como 85 pueden interpretarse como indicadores de una fracción cercana a un múltiplo de $1/r$.

Ejercicio: fase exacta

Tipo: Ejercicio

Enunciado

Con $m = 4$ qubits de conteo y fase exacta $\varphi = 3/16$, determine el resultado ideal de QPE.

Desarrollo

Se calcula $2^m\varphi = 16 \cdot 3/16 = 3$. El entero 3 se representa como 0011_2 si se usan cuatro bits.

Interpretación

La compatibilidad exacta entre fase y resolución produce concentración de probabilidad en una sola cadena.

Ejercicio: orden modular

Tipo: Ejercicio

Enunciado

Determine conceptualmente el orden de $x = 2$ módulo 15.

Desarrollo

Se verifican potencias: $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 16 \equiv 1$ (mód 15). Por tanto $r = 4$.

Interpretación

El resultado será útil para factorizar porque es par y produce una diferencia de cuadrados no trivial.

Ejercicio: convergente

Tipo: Ejercicio

Enunciado

Si una medición produce $y = 85$ con $m = 9$, use la interpretación $y/2^m$ como aproximación racional.

Desarrollo

La fracción inicial es $85/512$. El trabajo de fracciones continuas busca denominadores pequeños que aproximen esa razón y puedan validarse como candidatos de periodo.

Interpretación

La medición no entrega directamente el periodo. Entrega una pista racional que debe convertirse en denominador verificable.

Ejercicio: condición de éxito

Tipo: Ejercicio

Enunciado

Suponga que order finding devuelve un periodo impar. ¿Qué decisión toma el algoritmo de factorización?

Desarrollo

El paso de factorización requiere $r/2$ entero. Si r es impar, no se puede formar la diferencia de cuadrados requerida.

Interpretación

Se elige otro valor de x y se repite. El algoritmo es probabilístico, no una receta determinista de un solo intento.

Comparación: QPE, order finding y Shor

Tipo: Resumen

Roles

QPE estima fases de operadores unitarios. Order finding diseña un operador cuyas fases contienen razones s/r. Shor usa el orden r para convertir periodicidad modular en factores.

Conexión

Cada nivel traduce el resultado del nivel anterior a un nuevo lenguaje: fase, racional, periodo, factor.

Mapa completo de dependencias

Tipo: Resumen

Secuencia

Lectura

El poder del módulo está en encadenar traducciones bien justificadas. Ninguna etapa por sí sola explica Shor; el algoritmo completo surge de su composición.

Preguntas conceptuales

Tipo: Concepto

Por qué funciona

Porque las potencias controladas convierten eigenfases en una onda sobre el registro de conteo y la QFT inversa lee la frecuencia de esa onda.

Qué significa físicamente

La medición es consecuencia de interferencia entre caminos que acumularon diferentes múltiplos de la misma fase.

Qué pasaría si cambia una condición

Si falta precisión, si el periodo es impar o si el candidato de fracción continua no valida la congruencia, el intento debe repetirse o la estimación debe refinarse.

Limitaciones y realidad actual

Tipo: Concepto

Limitaciones prácticas

El circuito completo para números grandes requiere muchos qubits lógicos y circuitos profundos. La parte dominante es la aritmética modular reversible, no la QFT por sí sola.

Estado conceptual

El algoritmo define una ventaja asintótica en un modelo ideal. La realización física a escala criptográfica depende de progreso en corrección de errores, fabricación, control y compilación de circuitos.

Criterios de implementación

Tipo: Resumen

Verificación

Una implementación pedagógica debe comprobar: convención de bits del conteo, signo de la QFT inversa, potencias controladas correctas, elección de x, validación de convergentes y cálculo de gcd.

Uso del notebook

El notebook acompaña la presentación con histogramas, diagramas, fracciones continuas y circuitos en Qiskit/Cirq para que el estudiante pueda experimentar sin perder la estructura conceptual.

Fórmulas esenciales del módulo

Tipo: Resumen

QPE

$U|u\rangle = e^{2\pi i\varphi}|u\rangle$, y una medición y estima $\varphi \approx y/2^m$.

Order finding

$r = \text{mín}\{t > 0 : x^t \equiv 1 \pmod{N}\}$, y QPE produce aproximaciones a s/r.

Shor

Si r es par y $x^{r/2} \not\equiv -1 \pmod{N}$, entonces $\gcd(x^{r/2} \pm 1, N)$ puede revelar factores no triviales.

Cierre conceptual

Tipo: Resumen

Síntesis

QPE convierte fase en número. Order finding convierte número en periodo. Shor convierte periodo en factores. La QFT inversa es el puente que permite pasar de interferencia cuántica a información aritmética.

Proyección

En cursos posteriores, esta arquitectura servirá como referencia para distinguir entre una subrutina cuántica profunda, su posprocesamiento clásico y las condiciones físicas necesarias para ejecutarla a escala.

Distribución exacta de QPE

Tipo: Concepto

Por qué aparece un pico

Cuando la fase es exactamente representable con m bits, todos los términos de la suma de Fourier se alinean para un único entero y. Esa alineación produce probabilidad uno en la medición ideal.

Qué significa para el algoritmo

El caso exacto no es solo un cálculo conveniente: revela el mecanismo puro de QPE antes de introducir errores de aproximación, ruido o fases con expansión binaria infinita.

Distribución aproximada de QPE

Tipo: Concepto

Forma cualitativa

Cuando la fase cae entre dos puntos de la malla $y/2^m$, la probabilidad se reparte con un lóbulo principal alrededor de los enteros más cercanos y lóbulos laterales de menor peso.

Interpretación

La medición más frecuente sigue conteniendo información útil, pero el profesor debe enfatizar que QPE produce estimación probabilística cuando la fase no encaja exactamente en la resolución disponible.

Ejemplo: de fase a racional candidato

Tipo: Ejemplo

Problema

Suponga que QPE devuelve repetidamente un entero cercano a $2^m \cdot 3/7$. El resultado crudo es una fracción con denominador 2^m, pero el patrón sugiere un racional más simple.

Desarrollo

El posprocesamiento compara convergentes y valida denominadores mediante la congruencia modular. El candidato 7 no se acepta por apariencia decimal, sino porque explica la periodicidad de la función modular.

Conclusión

La estimación cuántica y la validación clásica forman una sola cadena lógica.

Order finding no mide el orden directamente

Tipo: Concepto

Aclaración necesaria

El primer registro mide información de fase. El orden aparece después de reconstruir un denominador racional y verificarlo contra la operación modular.

Implicación pedagógica

Esta distinción evita una confusión frecuente: el algoritmo no imprime r como variable interna; produce evidencia espectral a partir de la cual r se infiere.

Ejemplo: intento fallido en Shor

Tipo: Ejemplo

Problema

Un intento puede devolver un orden impar o un caso en el que $x^{r/2} \equiv -1 \pmod{N}$.

Desarrollo

En ambos casos, los máximos comunes divisores no generan factores no triviales. La respuesta correcta no es forzar la salida, sino repetir con otro x o mejorar la estimación.

Conclusión

El carácter probabilístico de Shor reside en intentos que se validan aritméticamente, no en aceptar cualquier salida del circuito.

Visualizaciones que acompañan el módulo

Tipo: Resumen

Notebook

El notebook incluye diagramas de QPE, fases binarias, periodicidad modular, fracciones continuas paso a paso, histogramas de medición, circuitos Qiskit y circuitos Cirq.

Propósito

Estas visualizaciones convierten la cadena fase-racional-periodo-factor en objetos observables: curvas, picos, circuitos y validaciones numéricas reproducibles.