Tipo: Resumen

Deutsch–Jozsa
y Bernstein–Vazirani

Oráculos, phase kickback e interferencia

Notas académicas para exposición en vivo: explicación conceptual desarrollada, matemática mínima en el cuerpo principal y derivaciones completas en material complementario.

La pregunta computacional

Tipo: Concepto

Problema que se quiere resolver

El punto de partida no es calcular una tabla de verdad, sino decidir una propiedad global de una función booleana desconocida. Para una función $f : \{0,1\}^n \to \{0,1\}$, la pregunta relevante puede depender de la forma completa de f, aunque el acceso disponible sea solamente a través de un oráculo. Esta tensión entre información local y propiedad global es la razón de ser de los algoritmos oraculares.

Limitación del enfoque clásico

Una consulta clásica entrega un único valor $f(x)$. Ese dato puede ser correcto y, al mismo tiempo, insuficiente para distinguir estructuras globales diferentes. En el peor caso, muchas funciones incompatibles con conclusiones distintas siguen siendo compatibles con las pocas respuestas observadas.

Idea cuántica

La estrategia cuántica no consiste en leer todos los valores. Consiste en preparar caminos coherentes, hacer que el oráculo escriba información como fases relativas y después usar interferencia para que la propiedad global aparezca como una salida medible.

Historia conceptual de los algoritmos oraculares

Tipo: Concepto

Por qué fueron importantes

Deutsch–Jozsa y Bernstein–Vazirani fueron diseñados para aislar una pregunta precisa: qué tipo de información puede extraer una computadora cuántica de una caja negra con menos consultas que una computadora clásica. Su valor histórico no está en que resuelvan directamente una aplicación industrial, sino en que exhiben, en un entorno matemáticamente controlado, cómo la coherencia y la interferencia modifican la noción de acceso a la información.

Implicación para la computación cuántica

Ambos algoritmos muestran que una consulta cuántica puede transportar una estructura global, siempre que el problema tenga una promesa adecuada. Deutsch–Jozsa decide una categoría extrema; Bernstein–Vazirani recupera una máscara lineal. En ambos casos, el oráculo no se usa como una subrutina clásica, sino como un dispositivo que transforma valores de función en geometría de fases.

Mapa mental del mecanismo

Tipo: Resumen

Lectura académica del diagrama

La secuencia resume una idea central de los algoritmos de consulta: la ventaja no proviene de observar trayectorias paralelas, sino de organizar amplitudes complejas para que unas alternativas se cancelen y otras se refuercen. La medición final es informativa porque el circuito completo fue diseñado para concentrar probabilidad en etiquetas asociadas con la estructura de f.

Uso durante el análisis

Cada bloque del diagrama responde a una necesidad concreta. La preparación crea caminos comparables; el oráculo introduce dependencia respecto de f; la interferencia convierte fase en probabilidad; la medición extrae una conclusión que debe interpretarse de acuerdo con la promesa del problema.

Modelo de consulta

Tipo: Concepto

Qué problema resuelve

El modelo de consulta permite estudiar cuántas veces se necesita acceder a una función desconocida para decidir una propiedad. Al abstraer el costo interno de implementar el oráculo, se concentra la atención en una pregunta informacional: cuánta información útil puede extraerse por cada acceso.

Por qué fue necesario introducirlo

Sin este modelo, comparar un algoritmo clásico y uno cuántico puede mezclar factores secundarios: lenguaje de programación, simulador, descomposición de compuertas o arquitectura física. La complejidad por consulta separa el acto de preguntar a la caja negra del procesamiento posterior de la respuesta.

Implicación

Deutsch–Jozsa y Bernstein–Vazirani deben leerse como resultados sobre información extraíble por acceso. La ventaja aparece porque una consulta cuántica puede escribir una familia completa de fases coherentes, mientras que una consulta clásica devuelve un valor puntual.

Propiedad global frente a valor local

Tipo: Concepto

Distinción esencial

Una pregunta local pide el valor $f(x)$ para una entrada concreta. Una pregunta global pide una propiedad de la función completa: si todos los valores son iguales, si la mitad son cero y la mitad uno, o qué máscara lineal determina una paridad. La segunda familia de preguntas no puede reducirse, en general, a una sola observación clásica.

Papel dentro del algoritmo

El circuito cuántico se diseña para que la propiedad global tenga una firma de interferencia. En lugar de almacenar una lista de valores, el oráculo transforma la función en un patrón de signos. El último cambio de base convierte ese patrón en una etiqueta medible.

Conclusión conceptual

La salida del algoritmo no debe interpretarse como un valor particular de la función, sino como una lectura comprimida de una estructura global. Esta interpretación es indispensable para evitar la falsa idea de que la superposición permite leer todos los datos simultáneamente.

La superposición no es una lista de respuestas

Tipo: Concepto

Problema conceptual que resuelve

La superposición permite que varios estados base participen coherentemente en una evolución, pero no convierte un registro cuántico en una memoria clásica de la cual puedan extraerse todas las entradas una por una. Al medir, se obtiene una sola cadena, de modo que la utilidad debe producirse antes de la medición.

Por qué es fundamental

Si la superposición solo ofreciera una lista oculta de respuestas, la medición destruiría casi toda la información. La clave es distinta: el oráculo modifica amplitudes relativas y esas modificaciones pueden interferir. El algoritmo tiene éxito cuando las amplitudes se organizan para que el resultado medido represente una propiedad de la función.

$$\text{fase relativa} \longrightarrow \text{interferencia} \longrightarrow \text{salida informativa}$$

Registros de n qubits

Tipo: Concepto

Definición formal mínima

Una cadena binaria $x = x_1 x_2 \cdots x_n \in \{0,1\}^n$ etiqueta un estado base de n qubits:

$$|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle .$$

Esta notación permite tratar de manera uniforme las 2^n entradas posibles de una función booleana.

Papel dentro del algoritmo

El registro de entrada no es un contenedor pasivo. Es el espacio donde se construye el patrón de fases que representa a f. El oráculo debe preservar la etiqueta x porque esa etiqueta identifica el camino sobre el cual se escribe el signo correspondiente.

Implicación

La notación de registros hace posible expresar el algoritmo sin enumerar manualmente todos los estados. También deja claro que el crecimiento exponencial del espacio de estados solo es útil si las amplitudes se hacen interferir de forma estructurada.

Dimensión y espacio de posibilidades

Tipo: Concepto

Hecho estructural

Con n qubits hay 2^n etiquetas base y el espacio de estados puro se representa en un espacio complejo de dimensión 2^n:

$$\mathcal{H}_n \cong \mathbb{C}^{2^n}.$$

Este crecimiento es una condición de posibilidad para trabajar con patrones globales, pero no constituye por sí mismo una ventaja computacional.

Interpretación correcta

El algoritmo no lee 2^n respuestas. Lo que hace es preparar amplitudes sobre 2^n caminos y después sumar esas amplitudes con signos controlados. La diferencia entre un recurso inútil y un algoritmo eficaz está en el diseño de la interferencia final.

Conclusión conceptual

El espacio grande permite representar patrones; el oráculo escribe el patrón; Hadamard lo analiza. Esta cadena lógica evita atribuir la ventaja a una idea imprecisa de paralelismo y la ubica en la manipulación coherente de amplitudes.

Hadamard como cambio de perspectiva

Tipo: Concepto

Definición necesaria

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Esta definición no debe verse solo como una forma de crear superposición. También define una transformación entre una base de valores y una base de contrastes.

Por qué es fundamental

Los oráculos de estos algoritmos escriben información como signos. Hadamard es el mecanismo que hace que esos signos sean legibles: transforma diferencias de fase en concentración o cancelación de amplitud. Por eso aparece antes del oráculo, para preparar caminos comparables, y después del oráculo, para leer el patrón resultante.

Implicación

En Deutsch–Jozsa, Hadamard pregunta si el paisaje de fases tiene componente uniforme. En Bernstein–Vazirani, invierte la representación de fase para recuperar una cadena oculta.

Producto interno módulo 2

Tipo: Concepto

Definición formal

Para $x, z \in \{0,1\}^n$, el producto interno binario se define como

$$x \cdot z = x_1 z_1 \oplus x_2 z_2 \oplus \cdots \oplus x_n z_n.$$

El resultado se calcula módulo 2, de modo que solo importa la paridad del número de posiciones en las que ambos bits son 1.

Por qué aparece

Cada qubit puede aportar un signo local. Al combinar n qubits, los signos se multiplican, y esa multiplicación se resume como una suma módulo 2 en el exponente de (-1). Por eso la expresión $(-1)^{x \cdot z}$ organiza los patrones de signos que Hadamard puede leer.

Papel algorítmico

En Deutsch–Jozsa, z etiqueta un patrón de lectura. En Bernstein–Vazirani, la cadena secreta s es precisamente el patrón lineal que determina los signos.

Hadamard multidimensional: fórmula mínima

Tipo: Método

Matemática estrictamente necesaria

La identidad que se usará como herramienta de lectura es

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

La demostración completa se deja en el material complementario; aquí se necesita su significado operativo.

Lectura conceptual

Aplicar $H^{\otimes n}$ a una etiqueta x produce una superposición sobre todos los posibles detectores z. Cada detector lleva un signo determinado por $x \cdot z$. Dicho de otro modo, Hadamard convierte etiquetas binarias en patrones de contraste.

Implicación

Esta fórmula es la versión binaria de una transformada de Fourier sobre $\{0,1\}^n$. Los algoritmos siguientes funcionan porque el oráculo prepara una señal de fase y Hadamard la analiza como patrón.

Qué aporta Hadamard al razonamiento

Tipo: Resumen

Resultado conceptual obtenido

Hadamard permite pasar de una descripción por valores a una descripción por patrones de signos. Esta operación no añade información externa; reorganiza la información presente en las amplitudes para hacer visibles ciertas correlaciones.

Por qué importa

Los algoritmos siguientes no buscan valores individuales de f. Buscan correlaciones entre el patrón de signos inducido por f y los patrones de lectura generados por Hadamard. Si la correlación es fuerte, una etiqueta aparece con alta probabilidad; si los signos se equilibran, la amplitud se cancela.

Significado físico

La fase relativa altera la interferencia. Caminos que llegan con signos compatibles se refuerzan; caminos que llegan con signos opuestos se cancelan. Esta es la traducción física del cálculo algebraico.

El oráculo como interfaz con una función desconocida

Tipo: Concepto

Qué problema resuelve

El oráculo modela el acceso a una función cuyo mecanismo interno no se inspecciona. Permite estudiar algoritmos que usan la función como caja negra y, por tanto, separa la pregunta algorítmica de los detalles de implementación de f.

Por qué fue necesario introducirlo

En computación cuántica, una función clásica no puede insertarse simplemente como una operación que borra información. La evolución cerrada debe ser reversible y unitaria. Por eso el acceso a f se reformula como una transformación sobre dos registros.

Implicación

El oráculo es el lugar donde la información clásica entra al circuito cuántico. La forma en que se prepare el registro auxiliar determinará si esa información queda como bit de salida o como fase relativa útil para interferencia.

Oráculo reversible

Tipo: Concepto

Definición operativa

Para una función $f : \{0,1\}^n \to \{0,1\}$, el oráculo estándar actúa como

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle .$$

El primer registro conserva la entrada y el segundo acumula el valor de la función por XOR.

Qué limitación supera

La transformación $|x\rangle \mapsto |f(x)\rangle$ no es reversible cuando varias entradas producen la misma salida. En cambio, conservar x y modificar y por XOR permite que la operación sea una permutación de estados base, y por tanto implementable como una operación unitaria.

Papel dentro del algoritmo

La reversibilidad no es una formalidad técnica. Es lo que permite consultar la función manteniendo coherencia entre los caminos x, condición necesaria para que las fases puedan interferir después.

El papel del qubit auxiliar

Tipo: Concepto

Qué problema resuelve

El auxiliar permite que el oráculo sea reversible y, al mismo tiempo, ofrece un mecanismo para transformar valores de función en fases. En una lectura clásica, y recibe $f(x)$ por XOR. En los algoritmos de fase, y se prepara para que esa acción se traduzca en un signo.

Por qué es fundamental

El auxiliar no está ahí para almacenar una respuesta que luego se medirá. Su función es actuar como transductor entre dos lenguajes: el lenguaje de bits de la función y el lenguaje de fases del registro de entrada.

Implicación

Cuando el auxiliar se prepara en $|-\rangle$, el cambio $y \mapsto y \oplus f(x)$ no produce una salida clásica visible; produce una fase relativa que queda asociada con el camino x.

Phase kickback: idea central

Tipo: Concepto

Enunciado mínimo

Si el auxiliar está en

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

entonces el oráculo satisface

$$U_f\,|x\rangle\,|-\rangle = (-1)^{f(x)}\,|x\rangle\,|-\rangle\,.$$

La demostración completa está en el material complementario; para la exposición principal basta identificar qué transforma esta identidad.

Interpretación

Aunque el oráculo aplica XOR sobre el auxiliar, el signo aparece multiplicando al camino etiquetado por x. La información de $f(x)$ cambia de soporte: deja de ser un bit almacenado y se convierte en una fase relativa del registro de entrada.

Implicación

Sin phase kickback, Deutsch–Jozsa y Bernstein–Vazirani no tendrían un patrón de fases que Hadamard pudiera analizar.

Qué significa el kickback

Tipo: Concepto

Qué acabamos de establecer

El valor $f(x)$ puede convertirse en un signo sin medir el auxiliar. Este punto es decisivo: la consulta no destruye la coherencia entre caminos, sino que modifica sus fases de manera controlada.

Por qué importa

Los signos de todos los caminos x pueden compararse por interferencia. Esa comparación es la fuente de información global. El algoritmo no aprende los valores individualmente; aprende cómo se organiza el patrón completo de signos.

Significado físico y computacional

La información no queda como bit visible en el auxiliar; queda como fase relativa entre componentes del registro de entrada. Computacionalmente, esto prepara los datos para que una transformación posterior convierta fase en probabilidad de medición.

Interferencia como mecanismo de lectura

Tipo: Concepto

Problema que resuelve

Una fase relativa no se observa directamente con una medición en la base computacional. Para hacerla observable, el circuito debe transformar diferencias de fase en diferencias de probabilidad.

Por qué fue necesario introducirla

El oráculo por sí solo no entrega la respuesta. Después de phase kickback, la información está distribuida en signos. La interferencia producida por $H^{\otimes n}$ suma caminos positivos y negativos, y esa suma decide qué etiquetas sobreviven con amplitud distinta de cero.

Implicación

Los resultados medibles son etiquetas compatibles con el patrón de fase inducido por la función. Esta es la razón por la que la medición final puede representar una propiedad global sin revelar una tabla de verdad.

Ejemplo conceptual: paisajes de signos

Tipo: Ejemplo

Qué problema intenta resolver

Se busca distinguir si una función produce el mismo signo en todos los caminos o si separa el espacio de entradas en regiones con signos opuestos. Esta diferencia es invisible si se mira un único valor, pero se vuelve clara cuando se observa el patrón global.

Qué idea cuántica ilustra

La función se representa como un paisaje de fases sobre una superposición uniforme. Una función constante produce un paisaje plano; una función balanceada simple produce contraste. Hadamard no lee cada punto del paisaje, sino su estructura interferométrica.

Constante: $+ \; + \; + \; +$ Balanceada simple: $+ \; - \; + \; -$

Conclusión

El procedimiento se utiliza porque convierte una pregunta sobre muchos valores en una pregunta sobre la forma del paisaje de fases. La conclusión que debe extraerse es que la ventaja reside en comparar patrones, no en leer listas.

Ejercicio guiado: elegir el auxiliar

Tipo: Ejercicio

Enunciado

Queremos que el oráculo convierta el caso $f(x) = 1$ en un signo negativo asociado con el camino x. Entre $|0\rangle$, $|+\rangle$ y $|-\rangle$, ¿qué auxiliar permite ese comportamiento?

Desarrollo paso a paso

El cambio por XOR actúa como X sobre el auxiliar cuando $f(x) = 1$. Por tanto, se necesita un estado que no cambie de forma observable, pero que sí adquiera un signo negativo. Ese estado debe ser eigenvector de X con eigenvalor -1:

$$X\,|-\rangle = -\,|-\rangle\,, \qquad X\,|+\rangle = +\,|+\rangle\,.$$

Interpretación del resultado

El auxiliar adecuado es $|-\rangle$. No se elige por conveniencia estética, sino porque transforma una inversión de bit en una fase informativa. Esa fase es el dato que luego será leído por interferencia.

Qué cambia si el auxiliar no es $|-\rangle$

Tipo: Concepto

Auxiliar preparado en $|+\rangle$

El oráculo puede actuar, pero $X|+\rangle = |+\rangle$. Cuando $f(x) = 1$ no aparece un signo negativo que distinga al camino x. La consulta se vuelve insensible al valor de la función en el sentido requerido por estos algoritmos.

Auxiliar preparado en $|0\rangle$

El auxiliar queda correlacionado con $f(x)$. Esa correlación puede contener información, pero no produce automáticamente el patrón de fases que el último Hadamard sabe leer. El circuito cambia de naturaleza: ya no es una consulta de fase.

Implicación

La preparación del auxiliar es una condición estructural. Si se cambia, el oráculo deja de escribir el paisaje de fases apropiado y la interpretación de la medición final deja de estar garantizada.

Funciones booleanas y promesas

Tipo: Concepto

Qué problema resuelve la promesa

Una promesa restringe de antemano el conjunto de funciones posibles. En lugar de resolver un problema imposible de decidir con una sola medición para funciones arbitrarias, se define una familia con estructura suficiente para que la interferencia produzca una conclusión exacta.

Por qué fue necesario introducirla

Sin una promesa, una salida no puede interpretarse de manera unívoca. El mismo resultado de medición podría ser compatible con varias funciones de formas distintas. La promesa convierte el universo enorme de funciones en categorías o familias suficientemente separadas.

Implicación

La ventaja cuántica se formula respecto al problema prometido. En Deutsch–Jozsa la promesa es constante o balanceada; en Bernstein–Vazirani la promesa es linealidad booleana determinada por una cadena secreta.

Deutsch–Jozsa: formulación del problema

Tipo: Concepto

Enunciado

Se recibe acceso oracular a una función $f : \{0,1\}^n \to \{0,1\}$ con la promesa de que ocurre exactamente uno de dos casos: f es constante o f es balanceada. El objetivo es decidir cuál de los dos casos corresponde.

Qué significa constante o balanceada

Una función constante satisface $f(x) = c$ para toda entrada x. Una función balanceada produce 0 en exactamente la mitad de las entradas y 1 en la otra mitad. La promesa excluye todas las funciones intermedias.

Qué problema resuelve

Deutsch–Jozsa decide una propiedad global extrema sin reconstruir la tabla. Su interés conceptual está en mostrar que una consulta cuántica puede certificar una estructura que clásicamente requiere muchas consultas para verificarse con certeza.

Por qué la promesa constante/balanceada es esencial

Tipo: Concepto

Limitación previa

Si una función no es ni constante ni balanceada, el algoritmo puede producir una salida, pero esa salida no autoriza la misma conclusión. La regla de decisión solo es válida porque la función pertenece a una de dos categorías extremas.

Papel dentro del algoritmo

La promesa garantiza que el componente uniforme del paisaje de fases se comporte de manera radicalmente distinta en los dos casos. Para funciones constantes se conserva; para funciones balanceadas se cancela. Esa diferencia es exactamente lo que el último Hadamard traduce en medición.

Implicación para computación cuántica

El algoritmo enseña que la ventaja cuántica no es una propiedad aislada del circuito. Surge de la correspondencia entre promesa, oráculo, fase e interferencia.

Costo clásico determinista en Deutsch–Jozsa

Tipo: Método

Idea del peor caso

Mientras un procedimiento clásico solo haya observado valores iguales, todavía no puede excluir el caso constante. La dificultad no es encontrar evidencia cuando aparece temprano, sino garantizar una respuesta correcta en el peor caso.

Cota necesaria

Para descartar una función constante con certeza, puede ser necesario consultar más de la mitad de la tabla. En el peor caso, el primer valor opuesto aparece después de observar 2^{n-1} entradas iguales, de modo que se requieren

$$2^{n-1}+1$$

consultas.

Interpretación

La dificultad clásica exacta es certificar ausencia de uniformidad. Deutsch–Jozsa evita esa inspección punto por punto al convertir la uniformidad o el contraste en una firma interferométrica.

La idea cuántica de Deutsch–Jozsa

Tipo: Concepto

Qué intenta superar

El algoritmo evita revisar entradas individualmente. En lugar de preguntar por valores aislados, prepara una superposición uniforme de entradas y permite que el oráculo marque cada camino con un signo determinado por $f(x)$.

Por qué se utiliza este procedimiento

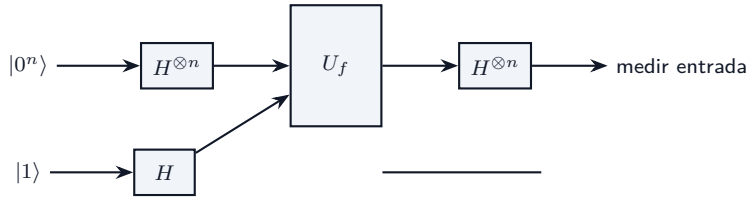
Si la función es constante, todos los caminos reciben el mismo signo y el paisaje de fases no tiene contraste. Si la función es balanceada, la mitad de los caminos recibe un signo y la otra mitad el signo opuesto, lo que cancela el componente uniforme.

Qué significa el resultado

La medición no identifica la función completa. Certifica si el paisaje de fases corresponde a uniformidad o a cancelación bajo la promesa. Esa es la respuesta computacional que el problema pide.

Circuito Deutsch–Jozsa como proceso

Tipo: Concepto



Lectura del circuito

El circuito debe leerse como una secuencia conceptual: preparar caminos coherentes, consultar el oráculo como operación de fase, aplicar una transformación de lectura y medir el registro de entrada. El auxiliar se usa para inducir fase y después deja de contener la respuesta principal.

Implicación

El mismo diagrama puede parecer breve, pero concentra tres ideas físicas: reversibilidad, phase kickback e interferencia. La medición final solo tiene significado porque esos tres componentes fueron ensamblados de manera coherente.

Paso 1: preparar una consulta coherente

Tipo: Concepto

Qué problema resuelve

La preparación inicial permite que cada entrada x participe en una misma evolución cuántica. El objetivo no es obtener respuestas múltiples, sino crear un escenario en el que todos los caminos puedan acumular fases comparables.

Estado conceptual

Después de aplicar Hadamard al registro de entrada y preparar el auxiliar en $|-\rangle$, la estructura relevante es

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle\,|-\rangle\,.$$

Interpretación

En este punto todavía no hay información sobre si f es constante o balanceada. Lo que se ha construido es una base coherente para que el oráculo escriba la función como fase sobre todos los caminos.

Paso 2: el oráculo escribe el paisaje de fases

Tipo: Concepto

Operación esencial

El oráculo, con el auxiliar preparado en $|-\rangle$, transforma el estado de entrada en

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle\,|-\rangle \quad \longmapsto \quad \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)}\,|x\rangle\,|-\rangle\,.$$

Significado físico

Cada camino conserva su etiqueta x, pero recibe un signo determinado por el valor de la función. La función deja de aparecer como una lista de bits y pasa a ser un paisaje de fases sobre el registro de entrada.

Significado computacional

Este paso es la única consulta al oráculo. Toda la diferencia entre constante y balanceada queda codificada en si el paisaje de fases es uniforme o tiene cancelación global.

Paso 3: Hadamard compara patrones

Tipo: Concepto

Intuición

El último $H^{\otimes n}$ actúa como un analizador de patrones. Pregunta, en términos de interferencia, a qué patrón básico de signos se parece el paisaje creado por f.

Papel dentro del algoritmo

Si el paisaje es uniforme, todos los caminos se refuerzan en la etiqueta 0^n. Si el paisaje tiene la cancelación balanceada prometida, la amplitud de 0^n desaparece. La medición distingue esos dos comportamientos.

Implicación

La salida no debe leerse como el valor de f en una entrada. Debe leerse como una evidencia interferométrica sobre la estructura global del paisaje de fases.

Fórmula mínima de amplitud

Tipo: Método

Cantidad que decide la medición

Después del último Hadamard, la amplitud de observar una etiqueta z puede escribirse como

$$\alpha_z = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot z + f(x)}.$$

Esta es la única fórmula global que necesitamos en la presentación principal.

Lectura conceptual

Cada entrada aporta un voto $+1$ o -1. La amplitud es el promedio coherente de esos votos. Cuando los votos se alinean, hay interferencia constructiva; cuando se equilibran, hay interferencia destructiva.

Conexión

El material complementario desarrolla la derivación completa. Aquí la fórmula se usa para interpretar por qué 0^n aparece en funciones constantes y desaparece en funciones balanceadas.

Qué significa la fórmula de amplitud

Tipo: Concepto

Interpretación matemática

La medición final es una correlación entre dos patrones: el patrón de la función, $(-1)^{f(x)}$, y el patrón de lectura, $(-1)^{x \cdot z}$. Cada posible salida z pregunta por una manera distinta de comparar signos.

Significado físico

La cancelación no representa ignorancia ni falta de información. Representa interferencia destructiva de amplitudes coherentes. Del mismo modo, una amplitud grande no significa que se haya contado una mayoría clásica, sino que los caminos llegaron con fases compatibles.

Implicación computacional

Deutsch–Jozsa usa esta correlación para decidir si el componente uniforme del paisaje de fases está presente. Esa es la propiedad relevante bajo la promesa constante/balanceada.

Caso constante

Tipo: Concepto

Patrón de fases

Si $f(x) = c$ para toda entrada x, todos los caminos reciben el mismo factor $(-1)^c$. Ese factor común no introduce contraste entre caminos; es una fase global respecto al registro de entrada.

Resultado suficiente

El último Hadamard concentra toda la probabilidad en 0^n:

$$\Pr(0^n) = 1.$$

Lo importante no es el signo global, sino la ausencia de diferencias relativas entre caminos.

Interpretación

Un paisaje de fase uniforme se lee como frecuencia cero. La etiqueta 0^n no significa que se hayan observado todos los ceros ni todos los unos; significa que no había contraste en el patrón de fases.

Caso balanceado

Tipo: Concepto

Patrón de fases

Si f es balanceada, la mitad de los caminos recibe signo $+1$ y la otra mitad signo -1. En la componente uniforme, esos signos se suman directamente y se cancelan.

Resultado suficiente

Para $z = 0^n$, el patrón de lectura no agrega signos extra. Por tanto, la amplitud de 0^n se anula:

$$\alpha_{0^n} = 0.$$

Interpretación

Un resultado distinto de 0^n certifica que había contraste. Bajo la promesa de Deutsch–Jozsa, ese contraste solo puede corresponder al caso balanceado. La salida exacta distinta de cero no identifica necesariamente la función completa.

Regla de decisión Deutsch–Jozsa

Tipo: Concepto

Medición del registro de entrada	Conclusión	Significado
0^n	constante	paisaje de fases uniforme
Distinto de 0^n	balanceada	contraste detectado por interferencia

Qué afirma la regla

La regla decide la categoría prometida usando una sola consulta. Su fuerza está en que la interferencia convierte una propiedad global extrema en un criterio de medición simple.

Qué no afirma

No identifica qué función balanceada específica se tenía, salvo en familias especiales. Tampoco es válida para funciones arbitrarias fuera de la promesa. La semántica de la salida depende del problema definido.

Ejemplo: función constante cero

Tipo: Ejemplo

Qué problema intenta resolver

Analizar el caso $f(x) = 0$ para toda entrada permite fijar la interpretación correcta de la salida 0^n. Se trata del caso más simple de paisaje de fases uniforme.

Qué idea cuántica ilustra

El oráculo no introduce ningún signo relativo. Todos los caminos permanecen coherentes en la misma dirección, de modo que el último Hadamard revierte la preparación inicial y concentra la probabilidad en 0^n.

Qué significa el resultado

La medición 0^n significa patrón uniforme. No significa que el algoritmo haya inspeccionado todos los valores de la tabla. La conclusión académica es que una propiedad global puede tener una firma de interferencia inequívoca.

Ejemplo: función constante uno

Tipo: Ejemplo

Qué problema intenta resolver

Este ejemplo pregunta si $f(x) = 1$ para toda entrada produce una lectura distinta de $f(x) = 0$. La respuesta es negativa en términos observables, y eso aclara la diferencia entre fase global y fase relativa.

Qué idea cuántica ilustra

Todos los caminos reciben el mismo factor -1. Como el factor es común, no cambia las probabilidades de medición. El paisaje sigue siendo uniforme, aunque tenga signo global opuesto.

Conclusión

Deutsch–Jozsa distingue constante frente a balanceada; no determina cuál valor constante se tenía. Computacionalmente, esto es correcto porque el problema no pide separar $f(x) = 0$ de $f(x) = 1$, sino distinguir uniformidad de balance.

Ejemplo: función balanceada $f(x) = x_2$

Tipo: Ejemplo

Qué problema intenta resolver

Se analiza una función que cambia de valor al cambiar el segundo bit. Es un caso balanceado con estructura lineal simple, útil para visualizar cómo se forma un contraste de fases.

Qué idea cuántica ilustra

Las entradas con $x_2 = 0$ y las entradas con $x_2 = 1$ reciben signos opuestos. El paisaje de fases queda dividido en franjas. Hadamard transforma ese contraste en una etiqueta de salida distinta de 0^n.

Interpretación del resultado

La medición certifica balance porque la componente uniforme fue cancelada por interferencia destructiva. La conclusión que debe extraerse no es que se haya leído cada franja, sino que el patrón global dejó una firma medible.

Qué enseña el ejemplo balanceado

Tipo: Concepto

Qué acabamos de ver

Una función balanceada simple produce un patrón de signos con una dirección de contraste clara. En el caso $f(x) = x_2$, el contraste se asocia con el segundo bit, pero Deutsch–Jozsa solo necesita saber que existe contraste suficiente para eliminar la salida 0^n.

Por qué importa

Una función balanceada general puede no tener una dirección lineal tan simple. Aun así, por definición, tendrá tantas fases positivas como negativas en el componente uniforme. Por eso la amplitud de 0^n se cancela bajo la promesa.

Conclusión conceptual

El criterio principal en Deutsch–Jozsa no es identificar qué salida no nula aparece, sino determinar si aparece 0^n. La presencia o ausencia de esa etiqueta codifica la respuesta al problema.

Ejercicio guiado: clasificar una tabla

Tipo: Ejercicio

Enunciado

Para $n = 2$, considere $f(00) = 0$, $f(01) = 1$, $f(10) = 1$, $f(11) = 0$. Bajo la promesa de Deutsch–Jozsa, ¿qué salida cualitativa esperamos?

Desarrollo paso a paso

La tabla contiene dos salidas 0 y dos salidas 1. Por definición, la función es balanceada. En el algoritmo, el componente uniforme del paisaje de fases se cancela, de modo que la amplitud de 00 debe ser cero.

Interpretación

La medición no debe producir 00 en el modelo ideal. Cualquier resultado distinto de 00 confirma el caso balanceado dentro de la promesa. El ejercicio no busca calcular toda la distribución, sino interpretar la firma de cancelación.

Variación conceptual: función no prometida

Tipo: Ejercicio

Enunciado

Para $n = 3$, una función produce seis ceros y dos unos. ¿Qué conclusión autoriza el algoritmo Deutsch–Jozsa si se aplica sin respetar la promesa?

Desarrollo

La función no es constante, porque no todos los valores coinciden. Tampoco es balanceada, porque una función balanceada en tres bits debe tener cuatro ceros y cuatro unos. Por tanto, la función queda fuera del problema prometido.

Interpretación

La regla "0^n implica constante; distinto de 0^n implica balanceada" solo es correcta cuando la función pertenece a una de las dos categorías permitidas. Sin promesa, el resultado puede indicar no uniformidad, pero no certifica balance.

Error conceptual: creer que se calcularon todos los valores

Tipo: Concepto

Por qué es incorrecto

Al medir el registro, solo se obtiene una cadena. Los valores individuales $f(x)$ no quedan disponibles como datos clásicos. Si el algoritmo realmente hubiera calculado una tabla, tendría que existir un procedimiento para leerla, y no lo hay.

Qué ocurre realmente

El oráculo deja una huella de fase. La interferencia comprime la propiedad prometida en una salida observable. Esta compresión depende de la estructura del problema y no puede transferirse automáticamente a funciones arbitrarias.

Implicación pedagógica

Deutsch–Jozsa debe entenderse como detector de estructura, no como generador de tablas de verdad. Esta diferencia es la base para interpretar correctamente otros algoritmos oraculares.

Qiskit: qué debe expresar el código

Tipo: Método

Objetivo del circuito

El código debe reflejar la secuencia conceptual: preparar $|-\rangle$, colocar la entrada en superposición uniforme, componer el oráculo, aplicar Hadamards finales y medir solo el registro de entrada. Si el código no expresa esa estructura, puede producir resultados numéricos sin significado algorítmico correcto.

Lectura computacional

La simulación no sustituye la interpretación. Los conteos observados son la consecuencia de la interferencia final, no una impresión de los valores de f. Por eso el estudiante debe revisar primero qué oráculo se implementó y qué promesa representa.

Implicación

Un circuito correcto debe preservar la separación entre entrada y auxiliar. Medir el auxiliar o invertir el orden de bits sin control puede producir salidas aparentemente contradictorias, aunque el algoritmo conceptual sea correcto.

Circuito Deutsch–Jozsa en Qiskit

Tipo: Método

Código mínimo con significado conceptual

```
from qiskit import QuantumCircuit

def dj_circuit(n, oracle):
    qc = QuantumCircuit(n + 1, n)
    qc.x(n); qc.h(n)        # auxiliar en |->
    qc.h(range(n))          # entrada uniforme
    qc.compose(oracle, inplace=True)
    qc.h(range(n))          # interferencia final
    for i in range(n):
        qc.measure(i, n - 1 - i)
    return qc
```

Interpretación

La medición se aplica solo al registro de entrada. La elección $n-1-i$ en el bit clásico ordena la cadena impresa según la convención conceptual usada para escribir $x = x_1 \cdots x_n$.

Oráculos Deutsch–Jozsa en Qiskit

Tipo: Método

Patrones útiles

Una función constante se implementa con identidad o con X en el auxiliar. Una función balanceada lineal simple se implementa con CNOTs controlados por los bits que participan en la paridad. Estos ejemplos cubren familias suficientes para observar el comportamiento del algoritmo.

```
def constant_oracle(n, c=0):
    qc = QuantumCircuit(n + 1)
    if c == 1:
        qc.x(n)
    return qc

def linear_balanced_oracle(mask):
    n = len(mask)
    qc = QuantumCircuit(n + 1)
    for i, bit in enumerate(mask):
        if bit == '1':
            qc.cx(i, n)
    return qc
```

Ejemplo Qiskit: cómo interpretar conteos

Tipo: Ejemplo

Qué problema intenta resolver

La simulación permite verificar que la implementación reproduce la regla conceptual del algoritmo. Sin embargo, los conteos no deben interpretarse como una tabla de valores de f, sino como la distribución producida después de la interferencia.

Qué idea cuántica ilustra

Para una función constante, los conteos se concentran en 0^n. Para una función balanceada simple, 0^n desaparece en el modelo ideal y aparece alguna cadena no nula. Esa diferencia refleja interferencia constructiva o destructiva, no inspección de entradas.

Conclusión

La simulación confirma una firma de fase. Si el resultado contradice la regla esperada, el diagnóstico debe comenzar por el auxiliar, el oráculo, el orden de bits y el registro que se midió.

Ejercicio guiado Qiskit: oráculo balanceado

Tipo: Ejercicio

Enunciado

Construir conceptualmente un oráculo balanceado para $f(x) = x_1 \oplus x_3$ con $n = 4$. ¿Qué compuertas deben aparecer y qué salida cualitativa debe producir Deutsch–Jozsa?

Desarrollo

El auxiliar debe cambiar si $x_1 = 1$ y también si $x_3 = 1$. En Qiskit esto se representa con dos CNOTs hacia el auxiliar, una controlada por el qubit correspondiente a x_1 y otra por el de x_3. Si ambos bits son 1, el auxiliar cambia dos veces y vuelve a su valor original, como exige la suma módulo 2.

Interpretación

El oráculo representa una función lineal balanceada. Por tanto, Deutsch–Jozsa debe devolver una cadena distinta de 0000 en el modelo ideal. La salida específica puede depender de la estructura lineal y de la convención de bits.

Resumen conceptual de Deutsch–Jozsa

Tipo: Resumen

Qué problema resuelve

Deutsch–Jozsa decide si una función prometida es constante o balanceada. El problema no pide conocer la tabla ni distinguir todas las funciones posibles, sino separar dos categorías extremas.

Por qué funciona

El oráculo convierte valores en fases; Hadamard prueba si el paisaje de fase tiene componente uniforme. Si la componente uniforme sobrevive, se mide 0^n; si se cancela, se obtiene una cadena no nula.

Implicación

El algoritmo muestra una separación exacta en el modelo de consulta bajo una promesa fuerte. Su mensaje profundo es que una propiedad global puede codificarse en interferencia y extraerse sin reconstruir los datos locales.

Transición: de propiedad global a parámetro oculto

Tipo: Concepto

Cambio de pregunta

Deutsch–Jozsa pregunta por una categoría de función. Bernstein–Vazirani pregunta por una cadena secreta que define una función lineal. Por tanto, cambia la semántica de la salida: ya no basta distinguir 0^n de no 0^n; ahora se espera recuperar una cadena completa.

Qué se conserva

Se conserva el mecanismo físico: superposición uniforme, oráculo usado como operación de fase, interferencia con Hadamard y medición del registro de entrada. La arquitectura es parecida porque ambas tareas explotan patrones de signos.

Qué cambia

La promesa es más estructurada. La función no es cualquier balanceada; tiene la forma $f_s(x) = x \cdot s$ módulo 2. Esa linealidad permite que Hadamard reconstruya el parámetro s exactamente.

Bernstein–Vazirani: formulación del problema

Tipo: Concepto

Enunciado

Existe una cadena secreta $s \in \{0,1\}^n$ y el oráculo implementa una función lineal booleana

$$f_s(x) = x \cdot s \pmod 2.$$

El objetivo es recuperar s usando el menor número de consultas.

Qué problema resuelve

El problema identifica todos los coeficientes de una regla de paridad. Cada bit de s indica si el bit correspondiente de entrada participa o no en la salida de la función.

Implicación

Bernstein–Vazirani convierte la lectura de varios coeficientes clásicos en una sola lectura interferométrica. La salida buscada no es una categoría; es el parámetro que define al oráculo.

Por qué Bernstein–Vazirani fue importante

Tipo: Concepto

Limitación clásica

Clásicamente, para recuperar todos los bits de s se consulta la función en los vectores unitarios e_i. Cada consulta revela un solo coeficiente s_i, por lo que el procedimiento natural requiere n consultas.

Idea cuántica

Una sola consulta en superposición produce el patrón completo de fases $(-1)^{x \cdot s}$. Ese patrón no es una colección de respuestas clásicas; es una representación coherente de la máscara lineal.

Significado

El algoritmo muestra cómo un parámetro distribuido en muchos bits puede leerse como un único patrón de interferencia. Esta es una lección central para algoritmos basados en transformadas y muestreo de Fourier.

La cadena secreta como máscara lineal

Tipo: Concepto

Interpretación

El bit s_i indica si el bit de entrada x_i participa en la paridad. La función puede escribirse como

$$f_s(x) = x_1 s_1 \oplus x_2 s_2 \oplus \cdots \oplus x_n s_n.$$

Si $s_i = 0$, cambiar x_i no afecta la salida; si $s_i = 1$, cambiar x_i invierte la salida cuando los demás bits se fijan.

Papel dentro del algoritmo

El oráculo no revela s directamente. Lo codifica como un patrón de signos. Hadamard reconoce ese patrón porque coincide con la representación de Hadamard de la etiqueta s.

Implicación

Recuperar s equivale a descubrir qué variables controlan la paridad. El resultado final describe la estructura de dependencia de la función, no un valor particular.

Estrategia clásica para recuperar s

Tipo: Método

Consulta a vectores unitarios

Sea e_i la cadena con un único 1 en la posición i. Entonces

$$f_s(e_i) = e_i \cdot s = s_i.$$

Cada consulta clásica a e_i revela exactamente un bit de la máscara.

Interpretación

El método clásico es claro y eficiente en términos ordinarios, pero aprende la máscara componente por componente. Si se requieren todos los bits, hacen falta n consultas deterministas.

Conexión con la ventaja cuántica

Bernstein–Vazirani no supera una dificultad aritmética complicada. Supera la necesidad de interrogar bit por bit al oráculo, usando una consulta coherente que codifica todos los coeficientes como fase.

Intuición cuántica de Bernstein–Vazirani

Tipo: Concepto

Qué intenta superar

El algoritmo evita aprender s bit por bit. La consulta cuántica se formula para que todos los caminos x reciban simultáneamente el signo que corresponde a la paridad $x \cdot s$.

Por qué se utiliza este procedimiento

La función lineal tiene una estructura compatible con Hadamard. El patrón de fases $(-1)^{x \cdot s}$ no es arbitrario: es exactamente el patrón que identifica a la cadena s en la base de Hadamard.

Conclusión conceptual

La medición final devuelve s porque el último Hadamard invierte la representación de fase. La interferencia no solo decide una categoría; reconstruye el parámetro completo de una familia lineal.

El oráculo BV como escritor de fase

Tipo: Concepto

Antes del oráculo

Todos los caminos x tienen la misma amplitud y el auxiliar está preparado en $|-\rangle$. El sistema está listo para que cada camino acumule una fase comparable sin que se mida la función.

Después del oráculo

Cada camino recibe el signo

$$(-1)^{f_s(x)} = (-1)^{x \cdot s}.$$

La cadena secreta no se almacena en un registro aparte; queda codificada en la geometría de las fases relativas del registro de entrada.

Implicación

El oráculo transforma una regla lineal clásica en una señal interferométrica. Esta es la razón por la que la etapa final puede recuperar una cadena completa después de una sola consulta.

Identidad mínima de Bernstein–Vazirani

Tipo: Método

Matemática estrictamente necesaria

Por la identidad de Hadamard,

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

Por tanto, el estado de fase producido por el oráculo es exactamente $H^{\otimes n}\,|s\rangle$.

Lectura conceptual

La fórmula dice que la cadena s tiene una huella de fase característica. Si el oráculo escribe esa huella, el último Hadamard puede invertir el cambio de base y devolver $|s\rangle$.

Conexión

La derivación formal está en el material complementario. En la presentación principal, la identidad se usa como puente entre la fase escrita por el oráculo y la medición exacta de la cadena.

Qué significa la identidad BV

Tipo: Concepto

Qué acabamos de establecer

El paisaje de fase generado por f_s es la representación de Hadamard de la cadena oculta. No se trata de una coincidencia algebraica menor; es la correspondencia estructural que hace funcionar al algoritmo.

Por qué importa

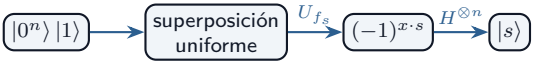
Aplicar Hadamard otra vez deshace el cambio de base. Como $H^{\otimes n}$ es su propia inversa, el patrón de fase se concentra en la etiqueta s con probabilidad uno en el modelo ideal.

Implicación computacional

Bernstein–Vazirani demuestra que una máscara lineal completa puede recuperarse por interferencia exacta. La información no se obtiene acumulando respuestas independientes, sino decodificando un patrón global coherente.

Circuito BV: mismo esqueleto, otra promesa

Tipo: Concepto



Punto pedagógico

La forma del circuito se parece a Deutsch–Jozsa porque ambos algoritmos usan la misma gramática: preparación coherente, oráculo de fase y lectura por Hadamard. La interpretación cambia porque la promesa sobre f es distinta.

Implicación

No basta reconocer el diagrama. Hay que saber qué familia de funciones implementa el oráculo. En BV, la salida se interpreta como máscara lineal; en Deutsch–Jozsa, como categoría constante/balanceada.

Medición exacta de la cadena

Tipo: Concepto

Resultado

El último Hadamard transforma el estado de fase en $|s\rangle$. Por tanto, la medición del registro de entrada devuelve s con probabilidad 1 en el modelo ideal.

Qué significa

El algoritmo no estima s ni produce una muestra parcial de sus bits. Lo recupera exactamente porque la función prometida es lineal, el oráculo es coherente y la identidad de Hadamard coincide con la estructura del problema.

Implicación

El caso BV muestra una diferencia cualitativa con Deutsch–Jozsa. La interferencia no solo elimina o preserva una componente uniforme; también puede decodificar un parámetro completo cuando la familia prometida tiene estructura suficiente.

Ejemplo: recuperar $s = 11$

Tipo: Ejemplo

Qué problema intenta resolver

La función cumple $f(00) = 0$, $f(01) = 1$, $f(10) = 1$, $f(11) = 0$. Se busca identificar qué máscara lineal explica esa tabla.

Qué idea cuántica ilustra

La tabla corresponde a la paridad de los dos bits. Cambiar cualquiera de ellos, manteniendo fijo el otro, puede invertir la salida. Por eso ambos bits participan en la máscara y se obtiene $s = 11$.

Procedimiento e interpretación

BV no consulta 00, 01, 10 y 11 por separado. Usa una consulta en superposición para crear el patrón de fase de $s = 11$. La medición final devuelve 11, que significa que ambos bits participan en la paridad oculta.

Ejemplo: máscara $s = 0110$

Tipo: Ejemplo

Qué problema intenta resolver

Este ejemplo aclara qué significa una cadena secreta con ceros intermedios. No todos los bits de entrada tienen por qué influir en la función.

Qué idea cuántica ilustra

Solo los bits con $s_i = 1$ contribuyen al signo $(-1)^{x \cdot s}$. Los bits con $s_i = 0$ no modifican la fase. Por tanto, el paisaje de fases depende únicamente de las posiciones activas de la máscara.

Interpretación computacional

La salida 0110 informa que los bits segundo y tercero determinan la paridad. La conclusión no es una lista de valores particulares, sino la estructura de dependencia de la función.

Qué enseñan los ejemplos BV

Tipo: Concepto

Qué se observa

Una tabla lineal puede parecer una colección de valores, pero su estructura real es una máscara de paridad. BV está diseñado para leer esa estructura directamente, no para reconstruir cada entrada de la tabla.

Por qué importa

La computación cuántica explota la estructura global de la máscara en fase. Cuando la función tiene la forma $x \cdot s$, el patrón de signos está perfectamente alineado con una base de Hadamard y puede decodificarse sin ambigüedad.

Implicación

Si la función no tiene la forma lineal prometida, la lectura "la medición es s" deja de ser válida. El significado de la salida depende de la promesa, no solo del circuito.

Ejercicio guiado: recuperar s desde valores unitarios

Tipo: Ejercicio

Enunciado

Para $n = 3$, se sabe que $f(100) = 1$, $f(010) = 0$ y $f(001) = 1$. Si $f(x) = x \cdot s$, ¿cuál es s?

Desarrollo paso a paso

Cada vector unitario revela un bit de la máscara: $f(100) = s_1 = 1$, $f(010) = s_2 = 0$ y $f(001) = s_3 = 1$. Por tanto, la máscara compatible con esos valores es $s = 101$.

Interpretación

Este razonamiento reproduce el método clásico bit por bit. El algoritmo cuántico produce el mismo resultado mediante una consulta coherente que escribe todos esos coeficientes como un patrón de fase y luego lo decodifica por Hadamard.

Variación conceptual: el caso $s = 0^n$

Tipo: Ejercicio

Enunciado

¿Qué ocurre en Bernstein–Vazirani si la cadena secreta es $s = 0^n$?

Desarrollo

Si $s = 0^n$, entonces $x \cdot s = 0$ para toda entrada x, por lo que $f_s(x) = 0$ siempre. El oráculo no introduce fase relativa entre caminos y el paisaje de fases es uniforme.

Interpretación

El último Hadamard devuelve 0^n. Este caso conecta BV con la intuición de Deutsch–Jozsa para funciones constantes, pero la interpretación es distinta: en BV, 0^n es la máscara secreta; en Deutsch–Jozsa, 0^n certifica uniformidad bajo la promesa.

Oráculo BV con compuertas CNOT

Tipo: Método

Regla de construcción

Para cada bit $s_i = 1$, se coloca una compuerta CX desde el qubit de entrada i hacia el auxiliar. Si $s_i = 0$, no se coloca compuerta. Las CNOTs acumulan en el auxiliar la paridad de los bits seleccionados por s.

```
def bv_oracle(s):
    n = len(s)
    qc = QuantumCircuit(n + 1)
    for i, bit in enumerate(s):
        if bit == '1':
            qc.cx(i, n)
    return qc
```

Por qué funciona

Cuando el auxiliar está en $|-\rangle$, cada CNOT activa contribuye a la fase. La composición de CNOTs escribe exactamente la paridad $x \cdot s$.

Circuito BV completo en Qiskit

Tipo: Método

```
def bv_circuit(s):
    n = len(s)
    qc = QuantumCircuit(n + 1, n)
    qc.x(n); qc.h(n)        # auxiliar en |->
    qc.h(range(n))          # entrada uniforme
    qc.compose(bv_oracle(s), inplace=True)
    qc.h(range(n))          # recupera |s>
    for i in range(n):
        qc.measure(i, n - 1 - i)
    return qc
```

Interpretación

La medición de los qubits de entrada debe devolver la cadena usada para construir el oráculo, salvo convenciones de orden de bits. El código expresa la misma secuencia física: preparación, escritura de fase, lectura por Hadamard y medición.

Orden de bits en Qiskit

Tipo: Concepto

Problema práctico

Qiskit muestra cadenas clásicas con el bit de mayor índice a la izquierda. Si se mide cada qubit en un bit clásico con el mismo índice, la cadena impresa puede aparecer invertida respecto a la convención conceptual usada para escribir $s = s_1 \cdots s_n$.

Procedimiento usado

Medimos el qubit i en el bit clásico $n - 1 - i$ para que la cadena impresa se lea en el mismo orden conceptual que la máscara. Esta decisión no cambia la física del circuito; solo fija la representación textual de la salida.

Implicación

Un resultado aparentemente invertido suele ser un problema de convención, no una falla del algoritmo. Separar convención de contenido físico es parte del rigor computacional.

Ejemplo Qiskit: interpretar una salida BV

Tipo: Ejemplo

Qué problema intenta resolver

El simulador devuelve conteos concentrados en una cadena. La pregunta conceptual es qué significa esa cadena y por qué aparece con probabilidad idealmente unitaria.

Qué idea cuántica ilustra

La concentración en un único resultado indica interferencia constructiva perfecta sobre $|s\rangle$. Los caminos que no corresponden a esa etiqueta se cancelan por la estructura del patrón $(-1)^{x\cdot s}$.

Interpretación computacional

Si los conteos se concentran en 0110, la regla oculta depende de los bits marcados por esa máscara. La salida se interpreta como parámetro del oráculo, no como valor de una entrada específica.

Ejercicio guiado Qiskit: cadena oculta

Tipo: Ejercicio

Enunciado

Si el oráculo BV contiene CNOTs desde los qubits 0, 2 y 3 hacia el auxiliar, ¿qué cadena debe recuperar el circuito para $n = 4$ usando la convención de medición indicada?

Desarrollo

Cada CNOT indica que el bit correspondiente participa en la paridad. Por tanto, la máscara tiene unos en las posiciones 0, 2 y 3, y un cero en la posición restante. En el orden conceptual usado, la cadena esperada es $s = 1011$.

Interpretación

La medición final debe concentrarse en 1011 si el orden de bits se configuró de forma consistente. Si aparece la cadena invertida, primero debe revisarse la convención de lectura antes de atribuir el resultado a un error físico.

Error conceptual: separación exponencial en BV

Tipo: Concepto

Aclaración

Bernstein–Vazirani compara una consulta cuántica contra n consultas clásicas deterministas para recuperar todos los bits de s. Es una ventaja clara en el modelo de consulta, pero no debe describirse como una separación exponencial frente a algoritmos probabilísticos en la forma básica del problema.

Por qué importa

La precisión en el tipo de ventaja es parte del rigor. Deutsch–Jozsa y BV tienen mensajes conceptuales distintos: uno ilustra una separación exacta bajo una promesa extrema; el otro muestra recuperación exacta de una máscara lineal con una sola consulta.

Implicación

Nombrar correctamente la ventaja evita sobreinterpretar los resultados y prepara al estudiante para analizar algoritmos oraculares posteriores, donde las separaciones pueden tener condiciones más sutiles.

Qué demuestra realmente Bernstein–Vazirani

Tipo: Concepto

Resultado computacional

Una consulta cuántica puede recuperar una máscara lineal completa. La consulta no devuelve n bits como respuestas clásicas separadas; produce una señal de fase cuya estructura equivale a esos n bits.

Idea física

El oráculo escribe la máscara como un patrón de fase. Hadamard invierte la representación y concentra amplitud en la cadena secreta. La información se vuelve observable porque se eligió una base de lectura compatible con la familia de funciones.

Implicación pedagógica

BV enseña que el poder de los algoritmos oraculares no está solo en consultar en superposición, sino en elegir la base correcta para consultar y la base correcta para leer.

Comparación Deutsch–Jozsa vs Bernstein–Vazirani

Tipo: Resumen

Aspecto	Deutsch–Jozsa	Bernstein–Vazirani
Pregunta	¿constante o balanceada?	¿cuál es s?
Promesa	dos categorías extremas	función lineal $x \cdot s$
Salida	0^n o no 0^n	la cadena s
Mecanismo	cancelación del componente uniforme	decodificación de una máscara de fase
Consulta cuántica	una	una

Conclusión

La forma del circuito se parece; la semántica de la medición depende de la promesa. Esta comparación impide confundir arquitectura de circuito con problema computacional.

Mismo circuito, diferente significado

Tipo: Concepto

Qué problema resuelve esta distinción

Evita confundir el diagrama del circuito con el problema computacional. Dos algoritmos pueden usar la misma arquitectura general y responder preguntas distintas porque el oráculo y la promesa definen qué significa la salida.

Por qué fue necesario aclararlo

En ambos algoritmos se prepara una superposición, se usa phase kickback y se aplica Hadamard al final. Sin embargo, en Deutsch–Jozsa una salida no nula significa balance bajo promesa; en BV, una salida no nula significa que la máscara secreta tiene bits activos.

Implicación

El circuito por sí solo no cuenta toda la historia. La interpretación correcta exige leer conjuntamente la familia de funciones, la construcción del oráculo y la regla de medición.

Vista física: paisajes de fase

Tipo: Concepto

Deutsch–Jozsa

El algoritmo pregunta si el paisaje de fase tiene componente uniforme o si esa componente se cancela. La medición 0^n indica ausencia de contraste; una salida distinta indica contraste suficiente para certificar balance bajo la promesa.

Bernstein–Vazirani

El algoritmo pregunta qué patrón lineal exacto generó el paisaje de fase. La cadena observada no es una categoría, sino la etiqueta del patrón lineal que el oráculo escribió.

Idea común

La medición final es una lectura interferométrica. No mide fases directamente; mide sus consecuencias en amplitudes. Esta lectura transforma una propiedad invisible en la base computacional antes del último Hadamard en una salida observable después de él.

Vista computacional: complejidad por consulta

Tipo: Concepto

Qué se mide

Se mide el número de accesos al oráculo, no el número de compuertas elementales ni el tiempo de ejecución en un simulador. Esta medida aísla la diferencia informacional entre preguntar de forma clásica y preguntar en una base cuántica coherente.

Por qué esta medida es útil

En problemas de caja negra, el costo dominante puede ser obtener información de la función desconocida. La complejidad por consulta pregunta cuántos accesos son necesarios para que una conclusión sea posible.

Implicación

Una ventaja por consulta muestra una separación de información extraíble por acceso. No debe confundirse automáticamente con una promesa de rendimiento en hardware ruidoso o con ventaja práctica universal.

Qué cambia si el auxiliar se prepara mal

Tipo: Concepto

Problema que resuelve esta pregunta

Permite distinguir condiciones estructurales de detalles superficiales del circuito. La preparación del auxiliar no es una convención: determina si el oráculo actuará como consulta de fase.

Respuesta conceptual

Si el auxiliar no convierte X en un signo, el oráculo no produce el paisaje de fases requerido. Sin ese paisaje, el último Hadamard no tiene la estructura adecuada para leer la propiedad global o la máscara lineal.

Implicación

El estado $|-\rangle$ habilita phase kickback. Cambiarlo puede convertir el algoritmo en otro procedimiento, con otra distribución de salida y sin la garantía de interpretación original.

Qué cambia si hay ruido

Tipo: Concepto

Modelo ideal

Las conclusiones anteriores suponen compuertas perfectas, oráculo exacto y medición sin errores. Bajo esas condiciones, la interferencia destructiva puede anular completamente ciertas amplitudes y la constructiva puede concentrar probabilidad en una etiqueta.

Efecto conceptual del ruido

El ruido degrada coherencia. Si las fases ya no se conservan, la interferencia se vuelve imperfecta y aparecen conteos fuera del resultado ideal. En Deutsch–Jozsa esto puede producir apariciones espurias de 0^n; en BV puede dispersar probabilidad fuera de s.

Implicación

El algoritmo explica una ventaja informacional ideal. La implementación física requiere control de errores, calibración y análisis estadístico para separar estructura algorítmica de imperfecciones del dispositivo.

Qué cambia sin promesa

Tipo: Concepto

Deutsch–Jozsa

Sin promesa, un resultado distinto de 0^n solo indica que el paisaje no fue completamente uniforme; no certifica balance. Una función con seis ceros y dos unos en tres bits puede producir contraste, pero no pertenece a la categoría balanceada.

Bernstein–Vazirani

Sin linealidad, una salida no puede interpretarse como cadena secreta exacta. El último Hadamard puede seguir produciendo alguna distribución, pero ya no existe una máscara s que explique necesariamente el resultado.

Implicación

El algoritmo, el oráculo y la promesa forman una unidad lógica. Quitar la promesa cambia el problema y, por tanto, cambia el significado de la medición.

Diagnóstico de errores en circuitos

Tipo: Resumen

Si Deutsch–Jozsa constante no produce 0^n

Debe revisarse la preparación del auxiliar, la medición del registro correcto y la composición del oráculo. Un error en cualquiera de esos puntos impide que la fase uniforme sea leída como componente 0^n.

Si Bernstein–Vazirani devuelve la cadena invertida

La causa más frecuente es una convención de bits clásicos. Antes de modificar el oráculo, conviene verificar cómo se mapean qubits a bits de salida en la medición.

Si aparecen varios conteos en simulación ideal

Debe revisarse que no se haya medido el auxiliar, que el oráculo no incluya operaciones extra y que la función implementada coincida con la promesa del algoritmo.

Por qué una sola consulta puede bastar

Tipo: Concepto

Respuesta corta pero profunda

Una consulta puede bastar cuando la función prometida tiene una estructura que puede escribirse como patrón de fase y cuando existe una transformación final que decodifica ese patrón. La consulta cuántica no devuelve más bits clásicos; devuelve una modificación coherente de amplitudes.

Diferencia con el enfoque clásico

Clásicamente, cada consulta produce un valor local. Cuánticamente, una consulta puede hacer que todos los caminos acumulen fases relacionadas con f. La diferencia no está en observar más respuestas, sino en permitir que esas fases se sumen o cancelen antes de medir.

Implicación

La ventaja se entiende como una ganancia en información estructural por acceso al oráculo. Es una afirmación precisa dentro del modelo de consulta y bajo promesas concretas.

Origen de la fórmula de amplitud

Tipo: Concepto

Origen de la expresión

La fórmula de amplitud aparece al aplicar Hadamard como familia de patrones de signos. El oráculo ya escribió el patrón $(-1)^{f(x)}$; el último Hadamard compara ese patrón con cada patrón de lectura $(-1)^{x \cdot z}$.

Interpretación

La suma que define α_z no es un cálculo mecánico aislado. Es una correlación. Mide, en lenguaje de amplitudes, cuánto se parece el paisaje de fases de la función al patrón etiquetado por z.

Implicación

Cuando la correlación es total, aparece interferencia constructiva. Cuando los signos se equilibran, la amplitud se cancela. Esta lectura convierte el álgebra en una explicación física del resultado.

Significado físico del resultado

Tipo: Concepto

En Deutsch–Jozsa

El resultado indica si el componente uniforme del paisaje de fases sobrevivió o fue cancelado. La etiqueta 0^n representa ausencia de contraste; una etiqueta distinta representa contraste bajo la promesa.

En Bernstein–Vazirani

El resultado indica qué patrón lineal generó las fases. La cadena s aparece porque el paisaje de fases coincide con la transformada de Hadamard de $|s\rangle$ y la operación final invierte esa representación.

Implicación

Físicamente, la medición revela consecuencias de la interferencia, no fases individuales. Computacionalmente, esas consecuencias se interpretan como respuesta al problema prometido.

Cambio de condiciones

Tipo: Concepto

Cambio del auxiliar

Si el auxiliar no está en $|-\rangle$, la consulta puede dejar de ser una consulta de fase. El oráculo puede seguir siendo unitario, pero el algoritmo pierde el mecanismo que hace legible la propiedad global.

Cambio de la promesa

Si la función no cumple la promesa, la misma salida puede perder su significado. Un resultado no nulo en Deutsch–Jozsa ya no certifica balance, y una salida en BV ya no necesariamente representa una cadena secreta.

Cambio por ruido

Si se degrada la coherencia, la interferencia ideal se vuelve imperfecta. La estructura matemática del algoritmo sigue siendo correcta, pero la distribución experimental requiere análisis estadístico.

Dónde quedan las derivaciones completas

Tipo: Resumen

Material complementario

Las pruebas completas de la identidad de Hadamard multidimensional, phase kickback, la amplitud final de Deutsch–Jozsa y la exactitud de Bernstein–Vazirani se colocan fuera de la presentación principal. Esa separación permite sostener el rigor sin convertir la exposición en una cadena larga de álgebra.

Uso recomendado

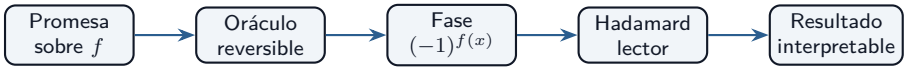
Durante la exposición, la matemática mínima justifica las conclusiones principales. Para estudio detallado, el documento complementario y el notebook desarrollan los pasos algebraicos completos y permiten reproducir los circuitos en Qiskit.

Mensaje conceptual

La meta principal de la presentación es entender cómo oráculo, fase e interferencia producen información computacional. Las derivaciones formalizan esa idea, pero no reemplazan su interpretación.

Mapa integrado de ambos algoritmos

Tipo: Resumen



Mensaje central

La promesa determina qué patrón de fase esperamos; el oráculo escribe ese patrón; Hadamard determina qué salida se vuelve probable. La interpretación de la medición es correcta solo cuando esos elementos encajan.

Implicación

Este mapa también explica por qué los algoritmos posteriores cambian la familia de funciones pero conservan la idea de interferencia estructurada.

Síntesis de Deutsch–Jozsa y Bernstein–Vazirani

Tipo: Resumen

Deutsch–Jozsa

Una consulta detecta si el paisaje de fase es uniforme o si se cancela el componente 0^n. La salida decide una categoría prometida: constante o balanceada.

Bernstein–Vazirani

Una consulta produce el paisaje de fase de una máscara lineal y Hadamard lo convierte en $|s\rangle$. La salida recupera un parámetro del oráculo: la cadena secreta.

Idea que organiza ambos casos

Los algoritmos oraculares tempranos muestran que la computación cuántica no solo calcula valores. Manipula interferencia para revelar estructura, siempre que el problema esté formulado con una promesa compatible con esa lectura.

Microdiscusión: por qué no medimos el auxiliar

Tipo: Concepto

Problema que resuelve

Esta pregunta aclara por qué el circuito ignora el qubit que aparentemente recibe $f(x)$. En una lectura clásica, parecería natural medir el auxiliar; en estos algoritmos, eso perdería la información relevante.

Respuesta conceptual

Con el auxiliar en $|-\rangle$, la información útil se transfiere como fase al registro de entrada. Medir el auxiliar no revela la propiedad global y puede destruir la coherencia necesaria para que los caminos interfieran correctamente.

Implicación

El auxiliar habilita la consulta de fase; la salida relevante está en el registro de entrada. Esta separación de funciones entre registros es una característica estructural del diseño del algoritmo.

Microdiscusión: qué significa una salida no nula

Tipo: Concepto

En Deutsch–Jozsa

Una salida distinta de 0^n significa que el componente uniforme desapareció. Bajo la promesa, eso certifica balance. No identifica necesariamente cuál función balanceada se implementó.

En Bernstein–Vazirani

Una salida no nula no significa "balance". Significa que la máscara secreta contiene bits activos. La cadena observada es el parámetro de la función lineal, no una categoría cualitativa.

Conclusión

La misma cadena observada puede tener significados distintos según el problema prometido. Esta es una lección general: la semántica de una medición depende del circuito y de la especificación del oráculo.

Cierre conceptual final

Tipo: Resumen

Idea principal

El oráculo no es una subrutina clásica insertada sin cambios en un circuito. Es una interacción reversible que puede usarse para escribir información en fase. Esa fase, mientras se conserve la coherencia, puede ser leída por interferencia.

Por qué importa

Una vez que la información está en fase, Hadamard actúa como analizador de patrones. Esa es la razón por la que los resultados principales salen de una sola consulta: no porque se lean todas las respuestas, sino porque se decodifica una estructura global.

Continuidad conceptual

Algoritmos posteriores cambian la promesa y la familia de patrones, pero conservan la idea de interferencia estructurada. Deutsch–Jozsa y Bernstein–Vazirani son el punto de entrada natural a esa forma de pensar.