Algoritmo de Deutsch
y phase kickback

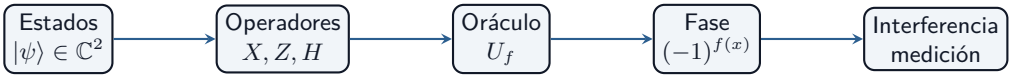
QNickel: algoritmos oraculares y ventaja por consulta

04 Junio de 2026

QMexico Summer School 2026

Ruta conceptual: de vectores a oráculos

Tipo: Resumen



- El problema no consiste en conocer todos los valores de f, sino en decidir una propiedad global: $f(0) \oplus f(1)$.
- La ventaja cuántica aparece porque una sola consulta a U_f modifica fases relativas que después se convierten en amplitudes observables.
- La notación se mantendrá fija: el primer registro almacena x y el segundo registro auxiliar almacena y.

Resultados esperados

Tipo: Resumen

- Formular $f : \{0,1\} \to \{0,1\}$ y distinguir funciones constantes y balanceadas.
- Demostrar por qué $|-\rangle$ es eigenestado de X con eigenvalor -1.
- Construir el oráculo reversible

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

- Probar, caso por caso, que

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

- Derivar la evolución completa de $|0\rangle |1\rangle$ hasta la medición del primer qubit.
- Interpretar la fase global, la fase relativa y la interferencia final.
- Implementar los cuatro oráculos de un bit con compuertas elementales.
- Diagnosticar cambios de condición: auxiliar incorrecto, medición incorrecta u orden de qubits ambiguo.

Mapa conceptual del tema

Tipo: Concepto

- **Motivación:** Reducir consultas a una caja negra permite separar costo de acceso a información y costo de procesamiento.
- **Definición formal:** Deutsch decide si $f(0) = f(1)$ o $f(0) \neq f(1)$ para f: $\{0,1\} \to \{0,1\}$.
- **Intuición:** La computación cuántica consulta una superposición de entradas, pero el resultado útil surge por interferencia.
- **Interpretación matemática:** La propiedad buscada es $f(0) \oplus f(1)$, no los dos valores por separado.
- **Ejemplo:** Si $(f(0), f(1)) = (0,1)$, entonces $f(0) \oplus f(1) = 1$ y la función es balanceada.
- **Aplicación:** El mismo mecanismo sostiene Deutsch–Jozsa y Bernstein–Vazirani como algoritmos oraculares.

Modelo de consulta: información global

Tipo: Concepto

- **Motivación:** Muchas tareas algorítmicas dependen de una función inaccesible salvo por llamadas controladas.
- **Definición formal:** Un algoritmo de consulta accede a f únicamente mediante una transformación permitida, aquí U_f.
- **Intuición:** La caja negra responde preguntas, pero la estrategia decide qué pregunta física se formula.
- **Interpretación matemática:** El recurso contado es el número de usos de U_f, no el número de compuertas auxiliares.
- **Ejemplo:** En el caso clásico exacto, conocer $f(0)$ no determina si $f(1)$ coincide o difiere.
- **Aplicación:** El modelo permite comparar de forma limpia algoritmos clásicos y cuánticos bajo el mismo acceso funcional.

Por qué Deutsch es un problema mínimo no trivial

Tipo: Concepto

- **Motivación:** Con una sola entrada no hay propiedad relacional; con dos entradas ya aparece una comparación.
- **Definición formal:** El dominio $\{0, 1\}$ contiene exactamente dos puntos: 0 y 1.
- **Intuición:** El problema pregunta si los dos valores de salida son iguales o diferentes.
- **Interpretación matemática:** La pregunta se comprime en un bit: $p = f(0) \oplus f(1)$.
- **Ejemplo:** $p = 0$ significa constante; $p = 1$ significa balanceada.
- **Aplicación:** Sirve como laboratorio algebraico para estudiar fases, oráculos e interferencia sin dimensión alta.

Notación de estados cuánticos

Tipo: Concepto

- **Motivación:** La notación de Dirac permite separar el vector físico, su base y las operaciones lineales aplicadas.
- **Definición formal:** Un qubit puro se escribe

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \alpha, \beta \in \mathbb{C}.$$

- **Intuición:** Las amplitudes no son probabilidades; las probabilidades son módulos cuadrados.
- **Interpretación matemática:** La base computacional es $\{|0\rangle\,, |1\rangle\}$, con $\langle 0|1\rangle = 0$.
- **Ejemplo:** $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ es una superposición normalizada.
- **Aplicación:** Las derivaciones de Deutsch se hacen siguiendo transformaciones lineales de estos vectores.

Amplitudes, probabilidades y normalización

Tipo: Método

Para que $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ represente un estado físico puro:

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

$$\begin{aligned}\langle\psi|\psi\rangle &= (\alpha^*\,\langle 0| + \beta^*\,\langle 1|)(\alpha\,|0\rangle + \beta\,|1\rangle)\\ &= |\alpha|^2\,\langle 0|0\rangle + \alpha^*\beta\,\langle 0|1\rangle + \beta^*\alpha\,\langle 1|0\rangle + |\beta|^2\,\langle 1|1\rangle\\ &= |\alpha|^2 + |\beta|^2.\end{aligned}$$

Conclusión: La condición de normalización es

$$|\alpha|^2 + |\beta|^2 = 1.$$

Producto tensorial de registros

Tipo: Concepto

- **Motivación:** Los oráculos actúan sobre registros compuestos, no sobre un qubit aislado.
- **Definición formal:** Si $|a\rangle \in \mathbb{C}^2$ y $|b\rangle \in \mathbb{C}^2$, entonces $|a\rangle \otimes |b\rangle \in \mathbb{C}^4$.
- **Intuición:** El primer factor codifica la entrada y el segundo factor codifica el auxiliar.
- **Interpretación matemática:** Por convención escrita:

$$|x\rangle\,|y\rangle = |x\rangle \otimes |y\rangle\,.$$

- **Ejemplo:** $|1\rangle\,|-\rangle = |1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
- **Aplicación:** U_f se define sobre pares $|x\rangle\,|y\rangle$ para conservar reversibilidad.

Orden de qubits y convención de índices

Tipo: Método

Usaremos la convención algebraica:

$$|x\rangle\,|y\rangle \equiv |x\rangle \otimes |y\rangle\,,$$

con x como registro de entrada y y como registro auxiliar.

- En circuitos, el índice de qubit puede mostrarse visualmente en un orden diferente al orden algebraico del vector de estado.
- Para evitar ambigüedad, toda expresión matemática declarará explícitamente qué registro es entrada y cuál es auxiliar.
- En código se fijará: qubit 0 como entrada y qubit 1 como salida auxiliar.

$$U_f : |x\rangle_{\text{in}}\,|y\rangle_{\text{aux}} \longmapsto |x\rangle_{\text{in}}\,|y \oplus f(x)\rangle_{\text{aux}}\,.$$

Fase global y fase relativa

Tipo: Concepto

- **Motivación:** Deutsch no lee directamente $f(0)$ y $f(1)$; lee una diferencia de fase convertida en medición.
- **Definición formal:** $|\psi\rangle$ y $e^{i\phi}|\psi\rangle$ son físicamente equivalentes para fase global $\phi \in \mathbb{R}$.
- **Intuición:** Multiplicar todo el estado por el mismo factor no cambia probabilidades.
- **Interpretación matemática:** Las fases relativas sí importan: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \neq \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
- **Ejemplo:** $|-\rangle$ y $-|-\rangle$ tienen las mismas probabilidades en cualquier medición proyectiva.
- **Aplicación:** En Deutsch se descarta la fase global, pero se conserva la fase relativa entre $|0\rangle$ y $|1\rangle$.

Ejemplo: dos estados físicamente equivalentes

Tipo: Ejemplo

Considere

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

Cálculo de probabilidades:

$$P_\psi(0) = |\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}, \qquad P_\psi(1) = |\frac{1}{\sqrt{2}}|^2 = \frac{1}{2},$$

$$P_\phi(0) = |-\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}, \qquad P_\phi(1) = |-\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}.$$

Interpretación: El signo común es una fase global $e^{i\pi} = -1$; no cambia estadísticas. En cambio,

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{y} \quad \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

se distinguen aplicando H, porque producen $|0\rangle$ y $|1\rangle$ respectivamente.

Ejercicio: normalización y fase observable

Tipo: Ejercicio

Enunciado: Sea

$$|\psi\rangle = \frac{1+i}{2}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,.$$

Determine si está normalizado y decida si $-\,|\psi\rangle$ cambia las probabilidades de medición en la base computacional.

Desarrollo paso a paso:

$$\alpha = \frac{1+i}{2}, \qquad \beta = \frac{1}{\sqrt{2}},$$

$$|\alpha|^2 = \frac{(1+i)(1-i)}{4} = \frac{2}{4} = \frac{1}{2}, \qquad |\beta|^2 = \frac{1}{2},$$

$$|\alpha|^2 + |\beta|^2 = 1.$$

Justificación: La norma se calcula con conjugación compleja; $-1 = e^{i\pi}$multiplica todas las amplitudes por la misma fase.

Interpretación: El estado es físico y $-|\psi\rangle$es indistinguible por probabilidades; solo fases relativas pueden modificar interferencia.

Operador X: inversión de bit

Tipo: Concepto

- **Motivación:** El oráculo usa XOR sobre el auxiliar; físicamente eso se implementa con aplicar o no aplicar X.
- **Definición formal:**

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle.$$

- **Intuición:** X intercambia las etiquetas computacionales 0 y 1.
- **Interpretación matemática:** Para $\alpha|0\rangle + \beta|1\rangle$,

$$X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle.$$

- **Ejemplo:** $X|-\rangle = -|-\rangle$.
- **Aplicación:** Ese eigenvalor negativo es la fuente algebraica del phase kickback.

Operador Z: inversión de fase

Tipo: Concepto

- **Motivación:** Las fases relativas son información computacional; Z es el operador básico que invierte una fase.
- **Definición formal:**

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Z|0\rangle = |0\rangle, \quad Z|1\rangle = -|1\rangle.$$

- **Intuición:** Z no cambia la etiqueta de base, pero cambia el signo de $|1\rangle$.
- **Interpretación matemática:**

$$Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle.$$

- **Ejemplo:** $Z|+\rangle = |-\rangle$ y $Z|-\rangle = |+\rangle$.
- **Aplicación:** El resultado del kickback sobre el primer qubit actúa como una fase condicionada equivalente a un Z selectivo.

Eigenestados de Z

Tipo: Método

Buscamos $|v\rangle = a\,|0\rangle + b\,|1\rangle$ y λ tales que

$$Z\,|v\rangle = \lambda\,|v\rangle\,.$$

Sustituyendo:

$$\begin{aligned} Z(a\,|0\rangle + b\,|1\rangle) &= aZ\,|0\rangle + bZ\,|1\rangle \\ &= a\,|0\rangle - b\,|1\rangle\,, \\ \lambda(a\,|0\rangle + b\,|1\rangle) &= \lambda a\,|0\rangle + \lambda b\,|1\rangle\,. \end{aligned}$$

Igualando coeficientes en la base ortonormal:

$$a = \lambda a, \qquad -b = \lambda b.$$

Por tanto, si $a \neq 0$ entonces $\lambda = 1$ y $b = 0$; si $b \neq 0$ entonces $\lambda = -1$ y $a = 0$.

$$\boxed{Z\,|0\rangle = |0\rangle}, \qquad \boxed{Z\,|1\rangle = -\,|1\rangle}.$$

Ejemplo: acción de Z sobre superposiciones

Tipo: Ejemplo

Tomemos

$$|\psi\rangle = \frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle .$$

Aplicación lineal:

$$\begin{aligned} Z|\psi\rangle &= Z\left(\frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle\right) \\ &= \frac{3}{5}Z|0\rangle + \frac{4}{5}Z|1\rangle \\ &= \frac{3}{5}|0\rangle - \frac{4}{5}|1\rangle . \end{aligned}$$

Interpretación: Las probabilidades $9/25$ y $16/25$ no cambian en la base computacional, pero la fase relativa sí cambia; esa diferencia puede hacerse observable con una rotación posterior, por ejemplo con H.

Ejercicio: identificar eigenestados de Z

Tipo: Ejercicio

Enunciado: Determine cuáles de los estados $|0\rangle$, $|1\rangle$, $|+\rangle$ y $|-\rangle$ son eigenestados de Z.

Desarrollo paso a paso:

$$
\begin{aligned}
Z|0\rangle &= |0\rangle = 1 \cdot |0\rangle\,, \\
Z|1\rangle &= -|1\rangle = (-1) \cdot |1\rangle\,, \\
Z|+\rangle &= Z\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle\,, \\
Z|-\rangle &= Z\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle\,.
\end{aligned}
$$

Justificación: Un eigenestado debe regresar proporcional a sí mismo, no a otro estado linealmente independiente. **Interpretación:** Los eigenestados de Z son $|0\rangle$ y $|1\rangle$; $|+\rangle$ y $|-\rangle$ se intercambian bajo Z.

Variación: eigenestados de Z con fase compleja

Tipo: Ejercicio

Enunciado: Analice si $|\phi\rangle = i\,|1\rangle$ y $|\eta\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{i}{\sqrt{2}}\,|1\rangle$ son eigenestados de Z.

Desarrollo paso a paso:

$$Z(i\,|1\rangle) = iZ\,|1\rangle = -i\,|1\rangle = (-1)(i\,|1\rangle),$$
$$Z\,|\eta\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{i}{\sqrt{2}}\,|1\rangle\,.$$

Para $|\eta\rangle$ ser eigenestado, debería existir λ con

$$\frac{1}{\sqrt{2}} = \lambda\frac{1}{\sqrt{2}}, \qquad -\frac{i}{\sqrt{2}} = \lambda\frac{i}{\sqrt{2}}.$$

La primera igualdad exige $\lambda = 1$ y la segunda exige $\lambda = -1$; contradicción.

Justificación: Las fases complejas globales no destruyen un eigenestado, pero una superposición con dos componentes no nulas de eigenvalores distintos no es eigenestado.

Interpretación: $i|1\rangle$representa el mismo rayo físico que $|1\rangle$y conserva eigenvalor -1.

Operador H: cambio de base

Tipo: Concepto

- **Motivación:** Deutsch convierte una diferencia de fase en una diferencia de resultado medible usando H.
- **Definición formal:**

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

- **Intuición:** H cambia entre la base computacional y la base de signos $\{|+\rangle, |-\rangle\}$.

- **Interpretación matemática:**

$$H|0\rangle = |+\rangle, \quad H|1\rangle = |-\rangle, \quad H^2 = I.$$

- **Ejemplo:** Si el primer qubit queda en $|-\rangle$, el último H lo transforma en $|1\rangle$.
- **Aplicación:** El algoritmo mide en la base correcta aplicando H antes de observar.

Estados $|+\rangle$ y $|-\rangle$

Tipo: Concepto

- **Motivación:** El auxiliar $|-\rangle$ transforma una inversión de bit en una inversión de fase.
- **Definición formal:**

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

- **Intuición:** Ambos son superposiciones balanceadas; solo difieren en la fase relativa.
- **Interpretación matemática:** Forman una base ortonormal: $\langle +|-\rangle = 0$.
- **Ejemplo:** $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ y $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$.
- **Aplicación:** La preparación XH sobre un qubit inicial $|0\rangle$ produce $|-\rangle$.

Identidades de Hadamard útiles

Tipo: Método

Partimos de

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

Como H es lineal:

$$\begin{aligned} H|+\rangle &= H\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right] \\ &= \frac{1}{\sqrt{2}}(H|0\rangle + H|1\rangle) \\ &= \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] \\ &= \frac{1}{2}(2|0\rangle) = |0\rangle\,. \end{aligned}$$

Análogamente:

$$H|-\rangle = \frac{1}{\sqrt{2}}(H|0\rangle - H|1\rangle) = \frac{1}{2}[(|0\rangle + |1\rangle) - (|0\rangle - |1\rangle)] = |1\rangle\,.$$

Ejercicio: aplicar H y recuperar la base computacional

Tipo: Ejercicio

Enunciado: Calcule $H\,(-\,|-\rangle)$ y explique si el signo inicial altera el resultado observable.

Desarrollo paso a paso:

$$\begin{aligned} H(-\,|-\rangle) &= -H\,|-\rangle && \text{linealidad de } H, \\ &= -\,|1\rangle && \text{identidad } H\,|-\rangle = |1\rangle\,. \end{aligned}$$

Justificación: El signo $-$ se factoriza porque H es una transformación lineal. La medición en la base computacional da

$$P(1) = |-1|^2 = 1, \qquad P(0) = 0.$$

Interpretación: El estado $-\,|1\rangle$ y el estado $|1\rangle$ tienen la misma predicción física; el signo global no cambia la salida observable.

Funciones booleanas de un bit

Tipo: Concepto

- **Motivación:** El algoritmo trabaja con funciones discretas cuyo comportamiento completo cabe en dos valores.
- **Definición formal:** Una función booleana de un bit es

$$f : \{0,1\} \to \{0,1\}, \quad x \mapsto f(x).$$

- **Intuición:** El dominio tiene dos entradas posibles y la salida también es un bit.
- **Interpretación matemática:** La función queda determinada por el par ordenado $(f(0), f(1))$.
- **Ejemplo:** $f(x) = x$ corresponde a $(0, 1)$.
- **Aplicación:** Los cuatro pares posibles generan los cuatro oráculos de Deutsch.

Conteo de funciones $f : \{0,1\} \to \{0,1\}$

Tipo: Método

El dominio tiene dos elementos: 0 y 1. Para cada entrada, la salida puede ser 0 o 1.

entrada	opciones de salida	número de opciones
0	$f(0) \in \{0,1\}$	2
1	$f(1) \in \{0,1\}$	2

Por el principio multiplicativo:

$$\#\{f : \{0,1\} \to \{0,1\}\} = 2 \cdot 2 = 2^2 = 4.$$

Más generalmente, si el dominio tiene m elementos y el codominio tiene k elementos:

$$\#\{f : A \to B\} = k^m.$$

Aquí $m = 2$ y $k = 2$.

Constante vs balanceada

Tipo: Concepto

- **Motivación:** La pregunta de Deutsch distingue igualdad de diferencia sin pedir los dos valores como salida explícita.
- **Definición formal:**

  constante $\iff f(0) = f(1)$, balanceada $\iff f(0) \neq f(1)$

- **Intuición:** Constante significa que ambas entradas producen la misma salida; balanceada significa una salida 0 y una salida 1.

- **Interpretación matemática:**

  $f(0) \oplus f(1) = 0 \iff$ constante, $f(0) \oplus f(1) = 1 \iff$ balan

- **Ejemplo:** $(1, 1)$ es constante y $(1, 0)$ es balanceada.
- **Aplicación:** La medición final devuelve precisamente esa paridad.

Tabla completa de las cuatro funciones

Tipo: Ejemplo

Nombre algebraico	$f(0)$	$f(1)$	Categoría
$f_0(x) = 0$	0	0	constante
$f_1(x) = 1$	1	1	constante
$f_2(x) = x$	0	1	balanceada
$f_3(x) = 1 \oplus x$	1	0	balanceada

Interpretación: No hay más casos porque el par $(f(0), f(1))$ ya agota todas las posibilidades binarias. **Conexión:** Cada fila tendrá una implementación reversible diferente como U_f.

Ejemplo: decisión por tabla de verdad

Tipo: Ejemplo

Suponga que una función tiene la tabla:

x	0	1
$f(x)$	1	0

Paso 1: Extraer los dos valores:

$$f(0) = 1, \qquad f(1) = 0.$$

Paso 2: Comparar:

$$f(0) \neq f(1).$$

Paso 3: Calcular paridad:

$$f(0) \oplus f(1) = 1 \oplus 0 = 1.$$

Interpretación: La función es balanceada. En el algoritmo cuántico, el primer qubit terminará en $|1\rangle$ antes de la medición, salvo una fase global.

Ejercicio: categorizar funciones de un bit

Tipo: Ejercicio

Enunciado: Categorice las funciones dadas por los pares $(f(0), f(1)) = (1,1)$, $(1,0)$, $(0,0)$ y $(0,1)$.

Desarrollo paso a paso:

$(f(0), f(1))$	$f(0) = f(1)$?	$f(0) \oplus f(1)$	categoría
$(1,1)$	sí	0	constante
$(1,0)$	no	1	balanceada
$(0,0)$	sí	0	constante
$(0,1)$	no	1	balanceada

Justificación: Para dominio de un bit, las únicas alternativas son igualdad o diferencia entre los dos valores. **Interpretación:** La categoría coincide exactamente con la paridad $f(0) \oplus f(1)$.

Variación: decisión por paridad $f(0) \oplus f(1)$

Tipo: Ejercicio

Enunciado: Sin usar una tabla de nombres, decida la categoría de f si $f(0) \oplus f(1) = 0$. Después repita para $f(0) \oplus f(1) = 1$.

Desarrollo paso a paso:

$$f(0) \oplus f(1) = 0 \iff f(0) = f(1) \qquad \text{propiedad del XOR binario}$$
$$\iff f \text{ es constante.}$$

$$f(0) \oplus f(1) = 1 \iff f(0) \neq f(1)$$
$$\iff f \text{ es balanceada.}$$

Justificación: En bits, $a \oplus b$ vale 0 solo cuando $a = b$ y vale 1 solo cuando $a \neq b$. **Interpretación:** Deutsch computa una propiedad relacional; no necesita reportar $f(0)$ ni $f(1)$ individualmente.

Variación: conteo para entradas de n bits

Tipo: Ejercicio

Enunciado: ¿Cuántas funciones booleanas existen de n bits a un bit, es decir, $f : \{0,1\}^n \to \{0,1\}$?

Desarrollo paso a paso:

$$|\{0,1\}^n| = 2^n \qquad \text{número de cadenas binarias de longitud } n,$$
$$|\{0,1\}| = 2 \qquad \text{dos salidas posibles por entrada,}$$
$$\#\{f : \{0,1\}^n \to \{0,1\}\} = 2^{|\{0,1\}^n|} = 2^{2^n}.$$

Justificación: Una función queda determinada al elegir una salida para cada una de las 2^n entradas, de forma independiente.
Interpretación: Para $n = 1$ se recupera $2^2 = 4$. El crecimiento doble exponencial explica por qué las propiedades globales de oráculos son relevantes.

Consulta clásica exacta

Tipo: Concepto

- **Motivación:** La ventaja cuántica se mide contra el número mínimo de consultas clásicas necesarias.
- **Definición formal:** Una consulta clásica devuelve un valor $f(x)$ para un $x \in \{0, 1\}$ elegido.
- **Intuición:** Preguntar por una entrada deja desconocida la otra entrada.
- **Interpretación matemática:** Tras consultar $x = 0$, las funciones $(f(0), 0)$ y $(f(0), 1)$ siguen siendo compatibles.
- **Ejemplo:** Si se observa $f(0) = 0$, aún pueden ocurrir $(0, 0)$ o $(0, 1)$.
- **Aplicación:** Una solución clásica exacta requiere dos consultas en el peor caso.

Por qué una consulta clásica no basta

Tipo: Método

Suponga que un algoritmo clásico consulta una sola entrada. Sin pérdida de generalidad, consulta $x = 0$.

Si la respuesta es $f(0) = 0$, quedan dos funciones compatibles:

$$f_a = (0, 0), \qquad f_b = (0, 1).$$

Pero:

$$f_a \text{ es constante}, \qquad f_b \text{ es balanceada}.$$

Como ambas producen exactamente la misma información observada tras una consulta, ningún criterio determinista puede distinguirlas con certeza.

El mismo argumento aplica si la respuesta es $f(0) = 1$:

$$(1, 1) \text{ constante}, \qquad (1, 0) \text{ balanceada}.$$

Argumento de adversario elemental

Tipo: Método

Una forma rigurosa de ver el límite clásico es imaginar que, después de la primera consulta, un adversario elige una función compatible con la respuesta ya observada.

1. El algoritmo elige consultar $x \in \{0,1\}$.
2. El adversario responde con un bit $b = f(x)$.
3. Aún existen dos extensiones compatibles:

$$f_{\text{const}}(x) = b, \quad f_{\text{const}}(1-x) = b,$$

$$f_{\text{bal}}(x) = b, \quad f_{\text{bal}}(1-x) = 1 \oplus b.$$

4. Ambas coinciden en la consulta realizada y difieren en la propiedad buscada.

Conclusión: Una consulta no determina la propiedad con certeza.

Ejemplo: decisión clásica con información incompleta

Tipo: Ejemplo

Considere la estrategia clásica: consultar primero $f(1)$.

Si se obtiene $f(1) = 1$, las funciones compatibles son:

$$(f(0), f(1)) = (1, 1) \quad \text{y} \quad (0, 1).$$

La primera es constante y la segunda es balanceada.

Interpretación: La incertidumbre no proviene de ruido ni de probabilidad física; proviene de información insuficiente. Para una respuesta exacta se debe consultar también $f(0)$. **Conexión:** El algoritmo cuántico evita este cuello de botella codificando la diferencia entre los dos valores como fase relativa.

Oráculos como cajas negras unitarias

Tipo: Concepto

- **Motivación:** La evolución cuántica cerrada debe ser unitaria; las funciones irreversibles requieren un registro adicional.
- **Definición formal:** Un oráculo cuántico para f es una unitaria U_f que implementa f reversiblemente.
- **Intuición:** No se borra x; se escribe $f(x)$ mediante XOR sobre el auxiliar.

- **Interpretación matemática:**

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

- **Ejemplo:** Si $f(x) = x$, entonces U_f es una compuerta controlada CX.
- **Aplicación:** La definición permite consultar f sobre superposiciones por linealidad.

Reversibilidad y conservación de información

Tipo: Concepto

- **Motivación:** Una transformación unitaria debe ser invertible y preservar productos internos.
- **Definición formal:** U es unitaria si $U^\dagger U = I$; por tanto es biyectiva.
- **Intuición:** Dos entradas distintas no pueden colapsar al mismo vector bajo una evolución unitaria.
- **Interpretación matemática:** El mapa $|x\rangle \mapsto |f(x)\rangle$ no es invertible si f es constante.
- **Ejemplo:** $f(0) = f(1) = 0$ enviaría $|0\rangle$ y $|1\rangle$ a $|0\rangle$.
- **Aplicación:** El auxiliar y evita borrar información porque $y \mapsto y \oplus f(x)$ es invertible para cada x.

Definición formal de U_f

Tipo: Método

Para $x, y \in \{0,1\}$ definimos

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

Verificación de reversibilidad: Aplique U_f dos veces:

$$\begin{aligned} U_f^2 \left|x\right\rangle \left|y\right\rangle &= U_f \left|x\right\rangle \left|y \oplus f(x)\right\rangle \\ &= \left|x\right\rangle \left|(y \oplus f(x)) \oplus f(x)\right\rangle \\ &= \left|x\right\rangle \left|y \oplus (f(x) \oplus f(x))\right\rangle \\ &= \left|x\right\rangle \left|y \oplus 0\right\rangle \\ &= \left|x\right\rangle \left|y\right\rangle . \end{aligned}$$

Por tanto,

$$U_f^2 = I \quad \Rightarrow \quad U_f^{-1} = U_f .$$

Matriz de U_f para cada función

Tipo: Método

Use el orden de base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, con x primero y y segundo.

$(f(0), f(1))$	acción sobre y	forma de circuito
$(0,0)$	$y \mapsto y$	I
$(1,1)$	$y \mapsto y \oplus 1$	X en auxiliar
$(0,1)$	$y \mapsto y \oplus x$	CX
$(1,0)$	$y \mapsto y \oplus (1 \oplus x)$	X-CX-X sobre control

Matriz ejemplo para $(0,1)$:

$$CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Justificación: Cada oráculo permuta vectores de base; toda matriz de permutación es unitaria.

Ejemplo: $f(x) = x$ y la compuerta CX

Tipo: Ejemplo

Si $f(x) = x$, entonces

$$U_f \, |x\rangle \, |y\rangle = |x\rangle \, |y \oplus x\rangle \, .$$

Calculemos sobre la base:

entrada	salida
$\|0\rangle \, \|0\rangle$	$\|0\rangle \, \|0 \oplus 0\rangle = \|00\rangle$
$\|0\rangle \, \|1\rangle$	$\|0\rangle \, \|1 \oplus 0\rangle = \|01\rangle$
$\|1\rangle \, \|0\rangle$	$\|1\rangle \, \|0 \oplus 1\rangle = \|11\rangle$
$\|1\rangle \, \|1\rangle$	$\|1\rangle \, \|1 \oplus 1\rangle = \|10\rangle$

Interpretación: El segundo qubit se invierte solo cuando $x = 1$; esa es exactamente la acción de CX con control en la entrada y objetivo en el auxiliar.

Ejercicio: construir la tabla de U_f

Tipo: Ejercicio

Enunciado: Para $f(0) = 1$ y $f(1) = 1$, construya la tabla de U_f.

Desarrollo paso a paso:

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus 1\right\rangle .$$

$\left\|x\right\rangle \left\|y\right\rangle$	$y \oplus 1$	$U_f \left\|x\right\rangle \left\|y\right\rangle$
$\left\|00\right\rangle$	1	$\left\|01\right\rangle$
$\left\|01\right\rangle$	0	$\left\|00\right\rangle$
$\left\|10\right\rangle$	1	$\left\|11\right\rangle$
$\left\|11\right\rangle$	0	$\left\|10\right\rangle$

Justificación: La salida de f no depende de x; siempre se invierte el auxiliar. **Interpretación:** El circuito es X aplicado al segundo qubit. La entrada se conserva y el auxiliar almacena el XOR.

Variación: oráculo para $f(x) = 1 \oplus x$

Tipo: Ejercicio

Enunciado: Construya U_f para $f(0) = 1$ y $f(1) = 0$ usando compuertas elementales.

Desarrollo paso a paso:

$$f(x) = 1 \oplus x,$$
$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus (1 \oplus x)\right\rangle .$$

Una realización es: invertir el control, aplicar CX, e invertir de nuevo el control.

Justificación: El CX se activa cuando el control transformado vale 1, es decir, cuando el x original vale 0. **Interpretación:** El auxiliar se invierte para $x = 0$ y permanece igual para $x = 1$, como exige $f(0) = 1, f(1) = 0$.

Qubit auxiliar y operación XOR

Tipo: Concepto

- **Motivación:** El auxiliar hace compatible una función clásica con evolución reversible.
- **Definición formal:** El registro auxiliar entra como $|y\rangle$y sale como $|y \oplus f(x)\rangle$.
- **Intuición:** El valor de $f(x)$ decide si se aplica Io Xal auxiliar.
- **Interpretación matemática:**

$$y \oplus f(x) = \begin{cases} y, & f(x) = 0, \\ 1 - y, & f(x) = 1. \end{cases}$$

- **Ejemplo:** Si y= 0, entonces el auxiliar sale como $|f(x)\rangle$.
- **Aplicación:** Si el auxiliar es $|-\rangle$, el cambio de bit se transforma en fase.

Preparación del auxiliar en $|-\rangle$

Tipo: Método

Partimos de un auxiliar inicial $|0\rangle$.

$$|0\rangle \xrightarrow{X} |1\rangle \xrightarrow{H} |-\rangle\,.$$

Detalle:

$$X\,|0\rangle = |1\rangle\,,$$
$$H\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle\,.$$

Entonces:

$$(HX)\,|0\rangle = H\,|1\rangle = |-\rangle\,.$$

Razón algebraica: Se elige $|-\rangle$ porque es eigenestado de X con eigenvalor -1; así, aplicar X introduce un signo detectable como fase relativa.

Derivación de $X\left|-\right\rangle = -\left|-\right\rangle$

Tipo: Método

Por definición:

$$\left|-\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle).$$

Aplique X usando linealidad:

$$\begin{aligned} X\left|-\right\rangle &= X\left[\frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle)\right] \\ &= \frac{1}{\sqrt{2}}(X\left|0\right\rangle - X\left|1\right\rangle) \\ &= \frac{1}{\sqrt{2}}(\left|1\right\rangle - \left|0\right\rangle) \\ &= -\frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) \\ &= -\left|-\right\rangle. \end{aligned}$$

Conclusión: $\left|-\right\rangle$ es eigenestado de X con eigenvalor -1:

$$X\left|-\right\rangle = (-1)\left|-\right\rangle.$$

Phase kickback: enunciado formal

Tipo: Concepto

- **Motivación:** Queremos que $f(x)$ modifique la fase del registro de entrada sin medirlo.
- **Definición formal:** Para $x \in \{0, 1\}$,

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

- **Intuición:** El auxiliar devuelve el eigenvalor de la operación que se le aplica.
- **Interpretación matemática:** Si $f(x) = 0$, se aplica I; si $f(x) = 1$, se aplica X y aparece -1.
- **Ejemplo:** Para $f(1) = 1$, $U_f \left|1\right\rangle \left|-\right\rangle = -\left|1\right\rangle \left|-\right\rangle$.
- **Aplicación:** En superposición, diferentes x reciben signos distintos; eso codifica la propiedad global.

Caso $f(x) = 0$: demostración explícita

Tipo: Método

Si $f(x) = 0$, entonces

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus 0\rangle = |x\rangle |y\rangle .$$

Como

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

se obtiene

$$\begin{aligned} U_f |x\rangle |-\rangle &= U_f |x\rangle \left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] \\ &= \frac{1}{\sqrt{2}} \left(U_f |x\rangle |0\rangle - U_f |x\rangle |1\rangle\right) \\ &= \frac{1}{\sqrt{2}} \left(|x\rangle |0\rangle - |x\rangle |1\rangle\right) \\ &= |x\rangle |-\rangle \\ &= (-1)^0 |x\rangle |-\rangle . \end{aligned}$$

Caso $f(x) = 1$: demostración explícita

Tipo: Método

Si $f(x) = 1$, entonces $y \mapsto y \oplus 1$ y el auxiliar se invierte:

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle X \left|y\right\rangle .$$

Ahora:

$$\begin{aligned} U_f \left|x\right\rangle \left|-\right\rangle &= \left|x\right\rangle \ X \left|-\right\rangle \\ &= \left|x\right\rangle (- \left|-\right\rangle) \\ &= - \left|x\right\rangle \left|-\right\rangle \\ &= (-1)^1 \left|x\right\rangle \left|-\right\rangle . \end{aligned}$$

Interpretación: La operación física actúa sobre el auxiliar, pero el signo queda multiplicando al término asociado a $|x\rangle$.

Demostración unificada del kickback

Tipo: Método

El oráculo puede escribirse condicionalmente como

$$U_f \left|x\right\rangle \left|\varphi\right\rangle = \left|x\right\rangle \, X^{f(x)} \left|\varphi\right\rangle ,$$

porque $X^0 = I$ y $X^1 = X$. Para $\left|\varphi\right\rangle = \left|-\right\rangle$:

$$\begin{aligned} U_f \left|x\right\rangle \left|-\right\rangle &= \left|x\right\rangle \, X^{f(x)} \left|-\right\rangle \\ &= \left|x\right\rangle \, (-1)^{f(x)} \left|-\right\rangle && \text{porque } X \left|-\right\rangle = - \left|-\right\rangle \\ &= (-1)^{f(x)} \left|x\right\rangle \left|-\right\rangle . \end{aligned}$$

Resultado clave:

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

Interpretación física: fase condicionada

Tipo: Concepto

- **Motivación:** El efecto parece actuar hacia atrás desde el auxiliar hacia el control; algebraicamente es eigenvalor condicionado.
- **Definición formal:** Para una superposición $\sum_x a_x |x\rangle |-\rangle$,

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

- **Intuición:** Cada rama x acumula un signo según el valor de $f(x)$.
- **Interpretación matemática:** El auxiliar se factoriza de nuevo; la información queda en fases del registro de entrada.
- **Ejemplo:** Si solo $f(1) = 1$, cambia el signo de la amplitud de $|1\rangle$.
- **Aplicación:** La fase condicionada es el puente entre el oráculo y la interferencia de Hadamard.

Ejemplo: $U_f |0\rangle |-\rangle$ y $U_f |1\rangle |-\rangle$

Tipo: Ejemplo

Considere $f(0) = 0$ y $f(1) = 1$.

Para $x = 0$:

$$U_f |0\rangle |-\rangle = (-1)^{f(0)} |0\rangle |-\rangle = (-1)^0 |0\rangle |-\rangle = |0\rangle |-\rangle .$$

Para $x = 1$:

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

Interpretación: El oráculo $f(x) = x$ deja intacta la rama $|0\rangle$ y cambia el signo de la rama $|1\rangle$. Esto es equivalente a aplicar Z al primer qubit cuando el auxiliar está preparado en $|-\rangle$.

Ejercicio: estado de tres qubits bajo fases dadas

Tipo: Ejercicio

Enunciado: Sea el registro $|00\rangle\,|-\rangle$ y un oráculo de fase con signos

$$g(00) = -1, \quad g(01) = 1, \quad g(10) = 1, \quad g(11) = -1.$$

Determine la salida.

Desarrollo paso a paso: El estado tiene soporte solo en la entrada 00 del primer registro. Por tanto:

$$|00\rangle\,|-\rangle \longmapsto g(00)\,|00\rangle\,|-\rangle = (-1)\,|00\rangle\,|-\rangle\,.$$

Luego:

$$\boxed{-\,|00\rangle\,|-\rangle}\,.$$

Justificación: Los valores $g(01)$, $g(10)$ y $g(11)$ no contribuyen porque sus amplitudes iniciales son cero. **Interpretación:** El signo es global para este único término; sería relativo solo si hubiera superposición con otras entradas.

Variación: cambio de signo en un patrón de dos bits

Tipo: Ejercicio

Enunciado: Con los mismos signos $g(00) = -1$, $g(01) = 1$, $g(10) = 1$, $g(11) = -1$, aplique el oráculo al estado

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)\,|-\rangle\,.$$

Desarrollo paso a paso:

$$\begin{aligned}\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)\,|-\rangle \longmapsto \frac{1}{\sqrt{2}}(g(00)\,|00\rangle + g(01)\,|01\rangle)\,|-\rangle \\ = \frac{1}{\sqrt{2}}(-\,|00\rangle + |01\rangle)\,|-\rangle\,.\end{aligned}$$

Justificación: La linealidad aplica el signo correspondiente a cada componente de la superposición. **Interpretación:** Ahora el signo no es global: cambia la fase relativa entre $|00\rangle$ y $|01\rangle$, por lo que puede producir interferencia observable después.

Del kickback a la interferencia

Tipo: Concepto

- **Motivación:** Una fase no observada directamente debe convertirse en una diferencia de probabilidad.
- **Definición formal:** Interferencia es suma algebraica de amplitudes antes de calcular módulos cuadrados.
- **Intuición:** Dos caminos con el mismo signo se refuerzan; con signos opuestos se cancelan.

- **Interpretación matemática:** El último H calcula sumas y diferencias:

$$\begin{pmatrix} a \\ b \end{pmatrix} \mapsto \frac{1}{\sqrt{2}} \begin{pmatrix} a+b \\ a-b \end{pmatrix}.$$

- **Ejemplo:** $\begin{pmatrix} 1 \\ 1 \end{pmatrix}/\sqrt{2} \mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ y $\begin{pmatrix} 1 \\ -1 \end{pmatrix}/\sqrt{2} \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.
- **Aplicación:** La igualdad o diferencia de $f(0)$ y $f(1)$ determina cuál amplitud se anula.

Estado inicial del algoritmo

Tipo: Método

El circuito comienza con dos qubits:

$$|\psi_0\rangle = |0\rangle\,|0\rangle\,.$$

Se prepara el auxiliar mediante X:

$$|\psi_1\rangle = (I \otimes X)\,|0\rangle\,|0\rangle\,.$$

Cálculo:

$$\begin{aligned}(I \otimes X)\,|0\rangle\,|0\rangle &= I\,|0\rangle \otimes X\,|0\rangle \\ &= |0\rangle \otimes |1\rangle \\ &= |0\rangle\,|1\rangle\,.\end{aligned}$$

Razón: El auxiliar se coloca en $|1\rangle$ para que el siguiente Hadamard lo convierta en $|-\rangle$.

Primera capa de Hadamards

Tipo: Método

Aplique $H \otimes H$ a $|0\rangle\,|1\rangle$:

$$\begin{aligned}|\psi_2\rangle &= (H \otimes H)\,|0\rangle\,|1\rangle \\ &= H\,|0\rangle \otimes H\,|1\rangle \\ &= |+\rangle\,|-\rangle \\ &= \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]|-\rangle\,.\end{aligned}$$

Forma expandida:

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\,|0\rangle\,|-\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,|-\rangle\,.$$

Interpretación:
El primer qubit está en superposición uniforme de entradas; el auxiliar está preparado para devolver eigenvalores.

Evolución antes del oráculo

Tipo: Método

Expanda completamente $|+\rangle\,|-\rangle$:

$$\begin{aligned}|+\rangle\,|-\rangle &= \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]\left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] \\ &= \frac{1}{2}(|0\rangle\,|0\rangle - |0\rangle\,|1\rangle + |1\rangle\,|0\rangle - |1\rangle\,|1\rangle) \\ &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle).\end{aligned}$$

Justificación: El producto tensorial distribuye como producto bilineal. **Interpretación:** Aunque la expansión muestra cuatro términos, el auxiliar seguirá factorizado después del oráculo si está en $|-\rangle$.

Aplicación de U_f

Tipo: Método

Partimos de

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}|0\rangle|-\rangle + \frac{1}{\sqrt{2}}|1\rangle|-\rangle\,.$$

Por linealidad:

$$\begin{aligned}|\psi_3\rangle &= U_f|\psi_2\rangle \\ &= \frac{1}{\sqrt{2}}U_f|0\rangle|-\rangle + \frac{1}{\sqrt{2}}U_f|1\rangle|-\rangle \\ &= \frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle|-\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle|-\rangle\,.\end{aligned}$$

Resultado:

$$|\psi_3\rangle = \left[\frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle\right]|-\rangle\,.$$

Factorización del auxiliar

Tipo: Método

Desde

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(-1)^{f(0)}\,|0\rangle\,|-\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}\,|1\rangle\,|-\rangle\,,$$

se factoriza el segundo registro:

$$|\psi_3\rangle = \left(\frac{1}{\sqrt{2}}(-1)^{f(0)}\,|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}\,|1\rangle\right) \otimes |-\rangle\,.$$

Justificación: Ambos términos tienen el mismo factor $|-\rangle$ en el auxiliar. **Interpretación:** Después de la consulta, el auxiliar no contiene información distinguible sobre f; la información útil está en la fase relativa del primer qubit.

Estado del primer qubit tras el oráculo

Tipo: Concepto

- **Motivación:** El cálculo de Deutsch se reduce a analizar un solo qubit después del kickback.
- **Definición formal:** Defina

$$|\chi_f\rangle = \frac{1}{\sqrt{2}}(-1)^{f(0)}\,|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}\,|1\rangle\,.$$

- **Intuición:** Los valores de f aparecen como signos delante de las ramas 0 y 1.

- **Interpretación matemática:** La fase relativa es

$$\frac{(-1)^{f(1)}}{(-1)^{f(0)}} = (-1)^{f(0)\oplus f(1)}.$$

- **Ejemplo:** Si $f(0) \neq f(1)$, entonces $|\chi_f\rangle = \pm\,|-\rangle$.
- **Aplicación:** El último H convierte $\pm\,|+\rangle$ en $|0\rangle$ y $\pm\,|-\rangle$ en $|1\rangle$ hasta fase global.

Caso constante: forma algebraica

Tipo: Método

Si f es constante, entonces $f(0) = f(1) = c$, con $c \in \{0, 1\}$.

$$\begin{aligned}\left|\chi_f\right\rangle &= \frac{1}{\sqrt{2}}(-1)^{f(0)}\left|0\right\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}\left|1\right\rangle \\ &= \frac{1}{\sqrt{2}}(-1)^{c}\left|0\right\rangle + \frac{1}{\sqrt{2}}(-1)^{c}\left|1\right\rangle \\ &= (-1)^{c}\frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle) \\ &= (-1)^{c}\left|+\right\rangle .\end{aligned}$$

Después del último Hadamard:

$$H\left|\chi_f\right\rangle = (-1)^{c}H\left|+\right\rangle = (-1)^{c}\left|0\right\rangle .$$

Interpretación: La fase $(-1)^c$ es global; la medición devuelve 0 con probabilidad 1.

Caso balanceado: forma algebraica

Tipo: Método

Si f es balanceada, entonces los valores son distintos. Existen dos casos.

Caso A: $f(0) = 0,\ f(1) = 1$.

$$\left|\chi_f\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle - \frac{1}{\sqrt{2}}\left|1\right\rangle = \left|-\right\rangle.$$

Caso B: $f(0) = 1,\ f(1) = 0$.

$$\left|\chi_f\right\rangle = -\frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle = -\left|-\right\rangle.$$

En ambos casos:

$$\left|\chi_f\right\rangle = \pm\left|-\right\rangle.$$

Después del último Hadamard:

$$H\left|\chi_f\right\rangle = \pm H\left|-\right\rangle = \pm\left|1\right\rangle.$$

Interpretación: El signo global no altera la medición; se observa 1 con probabilidad 1.

Último Hadamard: cálculo general

Tipo: Método

Escriba el primer qubit como vector:

$$\left|\chi_f\right\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} (-1)^{f(0)} \\ (-1)^{f(1)} \end{pmatrix}.$$

Aplique $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$:

$$\begin{aligned} H\left|\chi_f\right\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} (-1)^{f(0)} \\ (-1)^{f(1)} \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} (-1)^{f(0)} + (-1)^{f(1)} \\ (-1)^{f(0)} - (-1)^{f(1)} \end{pmatrix}. \end{aligned}$$

Lectura: Si los signos son iguales, se anula la segunda componente. Si son opuestos, se anula la primera.

Resultado medible y criterio de decisión

Tipo: Concepto

- **Motivación:** El objetivo final es convertir una propiedad de f en un bit observado.
- **Definición formal:** El criterio de Deutsch es

  medición $0 \Rightarrow f$ constante, medición $1 \Rightarrow f$ balanceada.

- **Intuición:** Igualdad de signos produce interferencia constructiva en $|0\rangle$; diferencia de signos en $|1\rangle$.
- **Interpretación matemática:**

$$H\,|\chi_f\rangle = (-1)^{f(0)}\,|f(0)\oplus f(1)\rangle\,.$$

- **Ejemplo:** Si $(f(0), f(1)) = (1, 0)$, el resultado es $-\,|1\rangle$.
- **Aplicación:** Una consulta cuántica a U_f decide la categoría con certeza en el modelo ideal.

Demostración completa expandida

Tipo: Método

$$
\begin{aligned}
|\psi_0\rangle &= |0\rangle\,|0\rangle\,,\\
|\psi_1\rangle &= (I\otimes X)\,|\psi_0\rangle = |0\rangle\,|1\rangle\,,\\
|\psi_2\rangle &= (H\otimes H)\,|\psi_1\rangle = |+\rangle\,|-\rangle\\
&= \left[\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\right]|-\rangle\,,\\
|\psi_3\rangle &= U_f\,|\psi_2\rangle = \left[\frac{1}{\sqrt{2}}(-1)^{f(0)}\,|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}\,|1\rangle\right]|-\rangle\,,\\
|\psi_4\rangle &= (H\otimes I)\,|\psi_3\rangle\\
&= \left[\frac{1}{2}((-1)^{f(0)}+(-1)^{f(1)})\,|0\rangle + \frac{1}{2}((-1)^{f(0)}-(-1)^{f(1)})\,|1\rangle\right]|-\rangle\,.
\end{aligned}
$$

Conclusión: Si $f(0)=f(1)$ queda $\pm\,|0\rangle\,|-\rangle$; si $f(0)\neq f(1)$ queda $\pm\,|1\rangle\,|-\rangle$.

Ejemplo resuelto: $f(0) = 0,\ f(1) = 0$

Tipo: Ejemplo

Para $f(0) = f(1) = 0$:

$$\left|\chi_f\right\rangle = \frac{1}{\sqrt{2}}(-1)^0 |0\rangle + \frac{1}{\sqrt{2}}(-1)^0 |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle\,.$$

Aplicando el último Hadamard:

$$H\left|\chi_f\right\rangle = H|+\rangle = |0\rangle\,.$$

Con auxiliar:

$$|\psi_4\rangle = |0\rangle\,|-\rangle\,.$$

Interpretación: La función es constante; el primer qubit se mide como 0 con probabilidad 1.

Ejemplo resuelto: $f(0) = 1,\ f(1) = 1$

Tipo: Ejemplo

Para $f(0) = f(1) = 1$:

$$\left|\chi_f\right\rangle = \frac{1}{\sqrt{2}}(-1)^1 |0\rangle + \frac{1}{\sqrt{2}}(-1)^1 |1\rangle = -\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = -|+\rangle\,.$$

Aplicando H:

$$H\left|\chi_f\right\rangle = H(-|+\rangle) = -H|+\rangle = -|0\rangle\,.$$

Con auxiliar:

$$|\psi_4\rangle = -|0\rangle\,|-\rangle\,.$$

Interpretación: El signo global no cambia la medición; se obtiene 0 con certeza.

Ejemplo resuelto: $f(0) = 0,\ f(1) = 1$

Tipo: Ejemplo

Para $f(0) = 0$ y $f(1) = 1$:

$$\left|\chi_f\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle - \frac{1}{\sqrt{2}}\left|1\right\rangle = \left|-\right\rangle.$$

Aplicando H:

$$H\left|\chi_f\right\rangle = H\left|-\right\rangle = \left|1\right\rangle.$$

Con auxiliar:

$$\left|\psi_4\right\rangle = \left|1\right\rangle\left|-\right\rangle.$$

Interpretación: La función es balanceada; el resultado 1 surge por cancelación de la amplitud de $|0\rangle$ y refuerzo de la amplitud de $|1\rangle$.

Ejemplo resuelto: $f(0) = 1,\ f(1) = 0$

Tipo: Ejemplo

Para $f(0) = 1$ y $f(1) = 0$:

$$\left|\chi_f\right\rangle = -\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle = -\,|-\rangle\,.$$

Aplicando H:

$$H\left|\chi_f\right\rangle = H(-\,|-\rangle) = -H\,|-\rangle = -\,|1\rangle\,.$$

Con auxiliar:

$$|\psi_4\rangle = -\,|1\rangle\,|-\rangle\,.$$

Interpretación: Aunque aparece un signo global, la medición del primer qubit devuelve 1 con probabilidad 1.

Ejercicio: primer qubit para función balanceada

Tipo: Ejercicio

Enunciado: Dado

$$|\chi_f\rangle = \frac{1}{\sqrt{2}}(-1)^{f(0)}\,|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}\,|1\rangle\,,$$

determine los posibles estados del primer qubit si f es balanceada.

Desarrollo paso a paso:

$$(f(0), f(1)) = (0,1) \Rightarrow |\chi_f\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle = |-\rangle\,,$$
$$(f(0), f(1)) = (1,0) \Rightarrow |\chi_f\rangle = -\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle = -\,|-\rangle\,.$$

Justificación: Balanceada implica signos opuestos, por lo que la superposición queda proporcional a $|-\rangle$. **Interpretación:** Los posibles estados son $|-\rangle$ y $-\,|-\rangle$; ambos se miden como 1 después de aplicar H.

Variación: signos permitidos antes de medir

Tipo: Ejercicio

Enunciado: Determine qué estados entre $|+\rangle$, $-|+\rangle$, $|-\rangle$, $-|-\rangle$ pueden aparecer antes del último H para funciones constantes o balanceadas.

Desarrollo paso a paso:

$$|\chi_f\rangle = \frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle\,.$$

Si f es constante, $f(0) = f(1)$ y los signos son iguales:

$$|\chi_f\rangle = (-1)^{f(0)}|+\rangle \in \{|+\rangle\,, -|+\rangle\}.$$

Si f es balanceada, los signos son opuestos:

$$|\chi_f\rangle \in \{|-\rangle\,, -|-\rangle\}.$$

Justificación: La fase común $(-1)^{f(0)}$ es global; la fase relativa decide entre $|+\rangle$ y $|-\rangle$. **Interpretación:** El algoritmo distingue las dos bases de signo, no el signo global dentro de cada caso.

Fase global frente a medición

Tipo: Concepto

- **Motivación:** Varias derivaciones producen estados con signo global; no deben interpretarse como resultados distintos.
- **Definición formal:** Dos estados $|\psi\rangle$ y $e^{i\phi}|\psi\rangle$ definen el mismo rayo físico.
- **Intuición:** Un detector responde a probabilidades, no a la etiqueta algebraica del signo global.

- **Interpretación matemática:**

$$|\langle k| e^{i\phi} |\psi\rangle|^2 = |e^{i\phi}|^2 |\langle k|\psi\rangle|^2 = |\langle k|\psi\rangle|^2.$$

- **Ejemplo:** $-|1\rangle$ se mide como 1 con probabilidad 1.
- **Aplicación:** Los casos $(1,1)$ y $(0,0)$ producen el mismo bit final.

Ejercicio: detectar un error de fase global

Tipo: Ejercicio

Enunciado: Un estudiante concluye que $-|1\rangle$ representa un resultado diferente de $|1\rangle$. Corrija la afirmación.

Desarrollo paso a paso:

$$-|1\rangle = e^{i\pi}|1\rangle\,.$$

Para medir en la base computacional:

$$P(1) = |\langle 1|-1\rangle|^2 = |-1|^2 = 1, \qquad P(0) = |\langle 0|-1\rangle|^2 = 0.$$

De forma más explícita:

$$\langle 1|(-|1\rangle)\rangle = -\langle 1|1\rangle = -1.$$

Justificación: El módulo cuadrado elimina una fase global de módulo uno. **Interpretación:** La afirmación correcta es: $-|1\rangle$ y $|1\rangle$ producen exactamente el mismo resultado observable.

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

Tipo: Concepto

- **Motivación:** El algoritmo depende de una condición específica: el auxiliar debe ser eigenestado de X con eigenvalor no trivial.
- **Definición formal:** Si $X|\varphi\rangle = \lambda|\varphi\rangle$, entonces

$$U_f|x\rangle|\varphi\rangle = \lambda^{f(x)}|x\rangle|\varphi\rangle\,.$$

- **Intuición:** Solo un eigenvalor distinto de 1 deja una marca de fase útil.
- **Interpretación matemática:** Para $|-\rangle$, $\lambda = -1$; para $|+\rangle$, $\lambda = 1$.
- **Ejemplo:** Con auxiliar $|+\rangle$ no aparece signo: $X|+\rangle = |+\rangle$.
- **Aplicación:** El diseño de algoritmos oraculares suele elegir auxiliares que convierten acciones controladas en fases.

Auxiliar $|0\rangle$: ausencia de kickback útil

Tipo: Método

Si el auxiliar entra como $|0\rangle$:

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

Para una superposición de entrada:

$$U_f\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle\right] = \frac{1}{\sqrt{2}}\,|0\rangle\,|f(0)\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,|f(1)\rangle\,.$$

Problema: Si $f(0) \neq f(1)$, el primer registro queda entrelazado con el auxiliar y no queda simplemente una fase relativa. **Consecuencia:** Aplicar H solo al primer qubit ya no implementa la prueba determinista de Deutsch en la misma forma.

Auxiliar $|+\rangle$: eigenvalor positivo

Tipo: Método

Como

$$X|+\rangle = |+\rangle\,,$$

se tiene para cualquier x:

$$\begin{aligned} U_f|x\rangle|+\rangle &= |x\rangle\, X^{f(x)}|+\rangle \\ &= |x\rangle\,(+1)^{f(x)}|+\rangle \\ &= |x\rangle|+\rangle\,. \end{aligned}$$

Interpretación: El oráculo no deja ninguna fase dependiente de $f(x)$.

Si el primer qubit estaba en $|+\rangle$, queda en $|+\rangle$ para todas las funciones. El último H siempre produce $|0\rangle$, de modo que el criterio de Deutsch falla.

Ejercicio: comparar $|-\rangle$, $|+\rangle$ y $|0\rangle$

Tipo: Ejercicio

Enunciado: Para $f(0) = 0$, $f(1) = 1$, compare la salida sobre $|+\rangle\,|-\rangle$, $|+\rangle\,|+\rangle$ y $|+\rangle\,|0\rangle$.

Desarrollo paso a paso:

$$U_f\,|+\rangle\,|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,|-\rangle = |-\rangle\,|-\rangle\,,$$
$$U_f\,|+\rangle\,|+\rangle = |+\rangle\,|+\rangle\,,$$
$$U_f\,|+\rangle\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle).$$

Justificación: En el primer caso $X\,|-\rangle = -\,|-\rangle$; en el segundo $X\,|+\rangle = |+\rangle$; en el tercero $|0\rangle$ no es eigenestado de X.
Interpretación: Solo $|-\rangle$ produce una fase útil sin dejar información en el auxiliar.

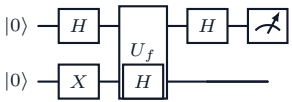
Representación en circuitos

Tipo: Concepto

- **Motivación:** El circuito traduce la derivación algebraica a operaciones ejecutables.
- **Definición formal:** El circuito de Deutsch implementa

$$(H \otimes I)\, U_f\, (H \otimes H)\, (I \otimes X).$$

- **Intuición:** Preparar, consultar, interferir, medir.
- **Interpretación matemática:** La medición del primer qubit estima $f(0) \oplus f(1)$ con certeza ideal.
- **Ejemplo:**



- **Aplicación:** El patrón se reutiliza en generalizaciones con más qubits de entrada.

Convención de qubits en Qiskit

Tipo: Método

Usaremos la convención de implementación:

$$q_0 = x \quad \text{entrada}, \qquad q_1 = y \quad \text{auxiliar}.$$

```
from qiskit import QuantumCircuit
from qiskit_aer import AerSimulator

circuit = QuantumCircuit(2, 1)
# q_0: input register x
# q_1: auxiliary/output register y
```

Regla operativa: La medición relevante se realiza sobre q_0, porque el algoritmo devuelve la categoría de f en el registro de entrada después de la interferencia. **Precaución:** El dibujo del circuito y el orden de bitstrings del simulador pueden requerir lectura cuidadosa; la convención debe fijarse antes de interpretar resultados.

Oráculo identidad para $f(x) = 0$

Tipo: Método

Para $f(0) = f(1) = 0$:

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus 0\rangle = |x\rangle |y\rangle .$$

Implementación:

```
def oracle_zero():
    circuit = QuantumCircuit(2)
    return circuit
```

Justificación: No se aplica ninguna compuerta porque el auxiliar nunca debe cambiar. **Interpretación:** Este oráculo es la identidad sobre ambos qubits.

Oráculo con X en salida para $f(x) = 1$

Tipo: Método

Para $f(0) = f(1) = 1$:

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus 1\right\rangle .$$

Implementación:

```
def oracle_one():
    circuit = QuantumCircuit(2)
    circuit.x(1)
    return circuit
```

Justificación: La salida auxiliar debe invertirse para cualquier valor de entrada. **Interpretación:** La entrada q_0 permanece intacta; q_1 almacena el XOR con 1.

Oráculo CX para $f(x) = x$

Tipo: Método

Para $f(0) = 0$ y $f(1) = 1$:

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

Implementación:

```
def oracle_identity_bit():
    circuit = QuantumCircuit(2)
    circuit.cx(0, 1)
    return circuit
```

Justificación: $CX(0, 1)$ invierte el qubit auxiliar 1 exactamente cuando el qubit de entrada 0 vale 1.

Interpretación: El circuito implementa el par de valores $(f(0), f(1)) = (0, 1)$.

Oráculo para $f(x) = 1 \oplus x$

Tipo: Método

Para $f(0) = 1$ y $f(1) = 0$:

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus (1 \oplus x)\right\rangle .$$

Implementación:

```
def oracle_not_bit():
    circuit = QuantumCircuit(2)
    circuit.x(0)
    circuit.cx(0, 1)
    circuit.x(0)
    return circuit
```

Justificación: Se activa el CX cuando el x original es 0; los dos X restauran el valor de entrada. **Interpretación:** La transformación es reversible y conserva x al final.

Circuito completo en Python/Qiskit

Tipo: Método

```python
def deutsch_circuit(oracle):
    circuit = QuantumCircuit(2, 1)

    # Prepare auxiliary qubit q_1 in |->
    circuit.x(1)
    circuit.h(1)

    # Prepare input qubit q_0 in |+>
    circuit.h(0)

    # One oracle query
    circuit.compose(oracle(), inplace=True)

    # Interference on the input register
    circuit.h(0)
    circuit.measure(0, 0)
    return circuit
```

Interpretación: El bit clásico medido vale 0 para funciones constantes y 1 para funciones balanceadas, en el modelo ideal sin ruido.

Ejercicio: completar un oráculo $f(0) = 0,\ f(1) = 1$

Tipo: Ejercicio

Enunciado: Complete una función que devuelva el oráculo para $f(x) = x$ con q_0 como entrada y q_1 como auxiliar.

Desarrollo paso a paso:

```
def oracle():
    circuit = QuantumCircuit(2)
    circuit.cx(0, 1)
    return circuit
```

Justificación: La tabla deseada es

$$|x\rangle\,|y\rangle \mapsto |x\rangle\,|y \oplus x\rangle\,.$$

Si $x = 0$, no se invierte y; si $x = 1$, se invierte y. Esa es exactamente la semántica de $CX(0, 1)$. **Interpretación:** El oráculo es balanceado y producirá resultado final 1 en el algoritmo de Deutsch ideal.

Variación: completar un oráculo $f(0) = 1,\ f(1) = 0$

Tipo: Ejercicio

Enunciado: Escriba el oráculo para la función complementaria $f(x) = 1 \oplus x$.

Desarrollo paso a paso:

```
def oracle():
    circuit = QuantumCircuit(2)
    circuit.x(0)
    circuit.cx(0, 1)
    circuit.x(0)
    return circuit
```

Justificación: El primer X convierte $x = 0$ en control activo; el segundo X restaura el registro de entrada. El auxiliar cambia solo para el x original igual a 0. **Interpretación:** Este oráculo también es balanceado. Aunque difiere por una fase global en la derivación, la medición final sigue siendo 1.

Verificación por tabla de verdad simulada

Tipo: Ejemplo

Para verificar un oráculo, prepare cada entrada de base y observe la salida esperada.

```
def truth_table_for_oracle(oracle):
    rows = []
    for x in [0, 1]:
        for y in [0, 1]:
            qc = QuantumCircuit(2, 2)
            if x == 1:
                qc.x(0)
            if y == 1:
                qc.x(1)
            qc.compose(oracle(), inplace=True)
            qc.measure([0, 1], [0, 1])
            counts = AerSimulator().run(qc, shots=1).result().get_counts()
            rows.append(((x, y), counts))
    return rows
```

Interpretación:
La verificación por entradas base confirma la acción reversible $|x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$ antes de usar superposición.

Errores comunes de implementación

Tipo: Resumen

- **Medir el auxiliar:** El bit de decisión está en el registro de entrada después del último H; medir solo q_1 no decide la propiedad de f.
- **Preparar $|+\rangle$ en el auxiliar:** Con $X|+\rangle = |+\rangle$, el oráculo no genera fase dependiente de $f(x)$.
- **Olvidar el primer X del auxiliar:** Si se aplica solo H a $|0\rangle$, el auxiliar queda en $|+\rangle$ y desaparece el kickback útil.
- **Confundir fase global con fase relativa:** $-|1\rangle$ no es un resultado distinto de $|1\rangle$, pero $|+\rangle$ y $|-\rangle$ sí son distinguibles.
- **Invertir control y objetivo:** $CX(0,1)$ y $CX(1,0)$ implementan transformaciones distintas.

Conexión con Deutsch–Jozsa y Bernstein–Vazirani

Tipo: Concepto

- **Motivación:** Deutsch es el caso base donde se observa por primera vez el patrón consulta–fase–interferencia.
- **Definición formal:** Deutsch–Jozsa extiende $f : \{0,1\}^n \to \{0,1\}$ y decide si f es constante o balanceada bajo una promesa.
- **Intuición:** La superposición ahora recorre todas las 2^n entradas.

- **Interpretación matemática:**

$$\sum_{x\in\{0,1\}^n} a_x \,|x\rangle\,|-\rangle \mapsto \sum_{x\in\{0,1\}^n} a_x (-1)^{f(x)} \,|x\rangle\,|-\rangle\,.$$

- **Ejemplo:** Bernstein–Vazirani usa $f_s(x) = s \cdot x \pmod 2$ para recuperar una cadena oculta.
- **Aplicación:** El mismo kickback convierte propiedades globales de funciones en patrones de interferencia medibles.

Resumen integrador y fuentes académicas

Tipo: Resumen

Cadena lógica:

$$|0\rangle\,|0\rangle \xrightarrow{I\otimes X} |0\rangle\,|1\rangle \xrightarrow{H\otimes H} |+\rangle\,|-\rangle$$
$$\xrightarrow{U_f} \left[\frac{1}{\sqrt{2}}(-1)^{f(0)}\,|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}\,|1\rangle\right]|-\rangle$$
$$\xrightarrow{H\otimes I} |f(0)\oplus f(1)\rangle\,|-\rangle \quad \text{hasta fase global.}$$

- Resultado 0: función constante.
- Resultado 1: función balanceada.
- Una consulta cuántica reemplaza dos consultas clásicas exactas.

Fuentes académicas base:

- D. Deutsch, *Quantum theory, the Church–Turing principle and the universal quantum computer*, Proc. R. Soc. A, 1985.
- M. A. Nielsen e I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press.
- IBM Quantum Learning, material de algoritmos de consulta y Deutsch.
- QWorld Nickel, notebooks de algoritmos convencionales en Qiskit.

Idea central: El oráculo no entrega los valores individualmente; el diseño de estados y bases convierte una propiedad global en un resultado determinista.