Fundamentos de computación cuántica

Andrés Sicard Ramírez

Mario Elkin Vélez Ruíz

Juan Fernando Ospina Giraldo

Luis Fernando Moreno (Grupo de Lógica y Computación. Universidad EAFIT, Medellín)

{asicard,mvelez,jospina,lmorenos}@eafit.edu.co

Cursillo en el X Encuentro ERM

Universidad de Medellín

Julio 12–16, 2004

Contenido

1. Introducción a la computación cuántica
2. Preliminares (matemáticos, físicos, informáticos)
3. Circuitos cuánticos
4. Algoritmos cuánticos (Deutsch, Deutsch-Jozsa, Shor)
5. Simuladores
6. Realización física

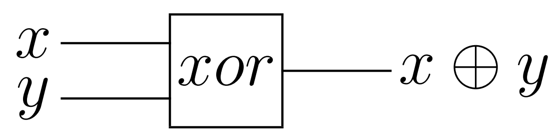
Recursos bibliográficos (introductorios)

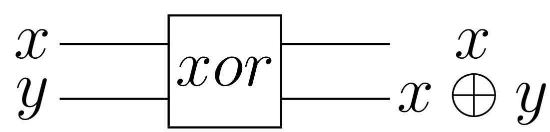
- Texto guía: Isaac L. Chuang y Michael A. Nielsen. *Quantum computation and quantum information*. Cambridge: Cambridge University Press, 2000 .
- N. David Mermin. *From cbits to qubits: teaching computer scientists quantum mechanics*. Eprint: `arXiv.org/abs/quant-ph/0207118`.
- Eleanor Rieffel y Wolfgang Polak, *An introduction to quantum computing for non-physicists*. Eprint: `arXiv.org/abs/quant-ph/9809016`.
- Dorit Aharonov. *Quantum computation*. Eprint: `arXiv.org/abs/quant-ph/9812037`.

Recursos Internet

- Servidor de los Alamos (`arxiv.org/`) (`xxx.lanl.gov`).
- *Virtual Journal of Quantum Computation* (`www.vjquantuminfo.org/`).
- Artículos clásicos (`pm1.bu.edu/~tt/qcl.html`).
- *Centre for Quantum Computation - Oxford* (`www.qubit.org/`)
- Simuladores (`www.vcpc.univie.ac.at/~ian/hotlist/qc/programming.shtml`)

- Alan Mathison Turing (1936): Máquina de Turing
- K. de Leeuw, E. F. Moore, C. E. Shannon y N. Shapiro (1956): Computación probabilista.
- Charles H. Bennett (1973): Computación reversible.

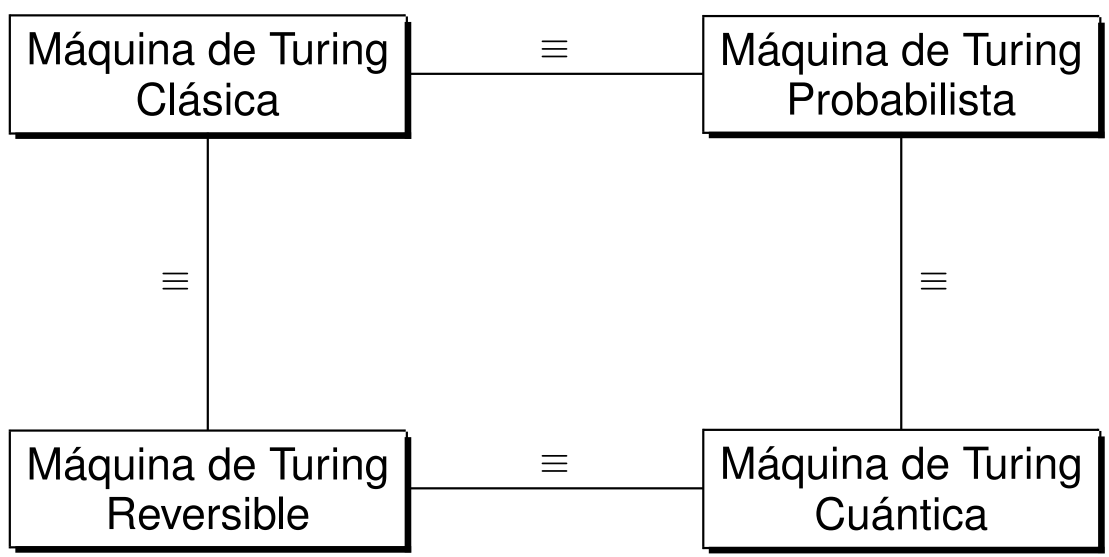
Compuerta no reversible: 

Compuerta reversible: 

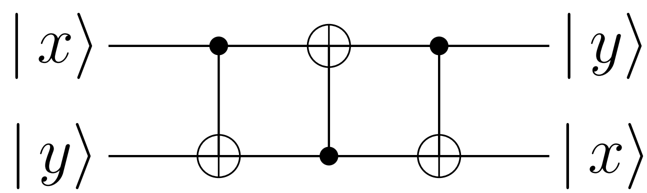
- Edward Fredkin y Tommaso Toffoli (1982): Compuertas universales reversibles.

$$z \oplus (x \wedge y) = \begin{cases} x \wedge y & \text{ssi } z = 0 \text{ (compuerta \textit{and})}, \\ x \oplus z & \text{ssi } y = 1 \text{ (compuerta \textit{xor})}, \\ \neg z & \text{ssi } x = y = 1 \text{ (compuerta \textit{not})}, \\ z & \text{ssi } x = 0; y = 1 \text{ (compuerta \textit{identidad})}. \end{cases}$$

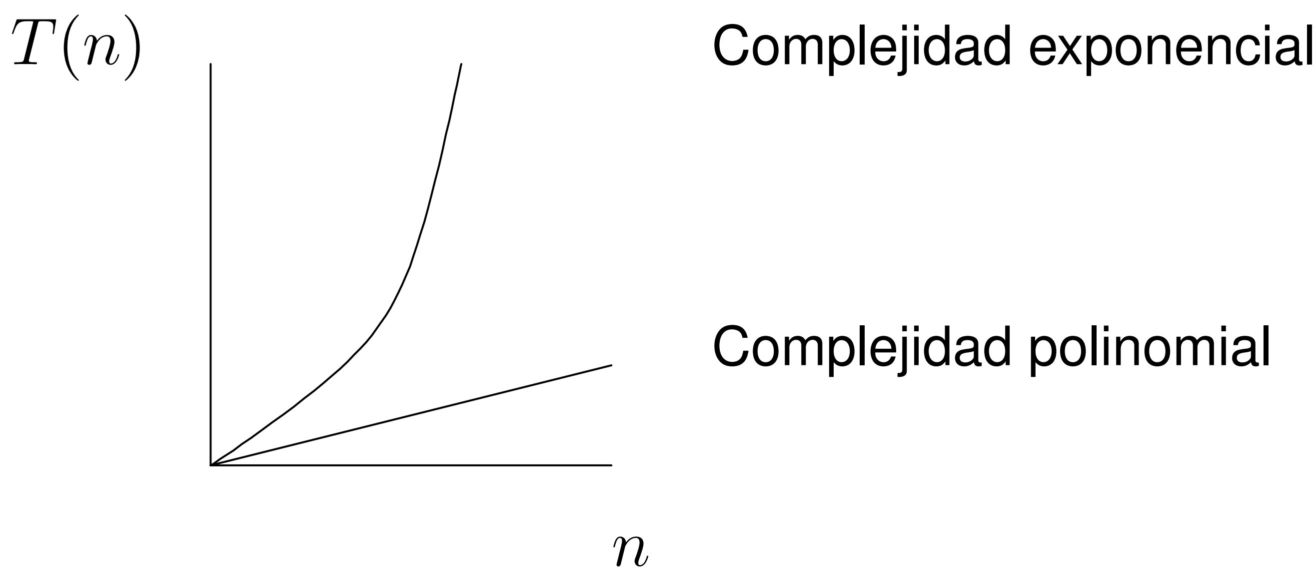
- Richard Feynman (1982, 1985): Computación mecánico-cuántica.
- David Deutsch (1985): Máquinas de Turing cuánticas.



- David Deutsch (1989): Circuitos cuánticos.
  Intercambio de qubits:



- Peter Shor (1994): Algoritmo para factorizar un número en sus factores primos de complejidad temporal polinomial



Algoritmo de Shor vs. algoritmo clásico

Número de dígitos	Algoritmo clásico	Algoritmo de Shor
129	1.85 años	45.9 minutos
250	2.1×10^6 años	3.4 horas
1000	4.5×10^{25} años	3.07 días

- Lov K. Grover (1996): Algoritmo de busqueda en una base de datos desorganizada.
- Implementación
  - 1998: 2-qubit (University of California Berkeley)
  - 1999: 3-qubit (IBM-Almaden)
  - 2000: 5-qubit (IBM-Almaden, Los Alamos)
  - 2001: 7-qubit (IBM-Almaden)

- Simuladores
  - Bernhard Ömer (1994): *QCL: A Programming Language for Quantum Computers* (para Linux).
  - Colin P. Williams y Scott H. Clearwater (1997): Simulador implementado en *MATHEMATICA*^{TM}.

Preliminares matemáticos

- Álgebra líneal
  - Espacios vectoriales y operadores líneales
  - Representaciones matriciales y espectros
  - Espacios y operadores unitarios
- Álgebra multilineal
  - Producto tensorial de espacios vectoriales
  - Producto tensorial de operadores lineales
- Análisis líneal
  - Funciones de operadores líneales
  - Ecuaciones de evolución
  - Espacios de Hilbert y álgebras Banach
  - Transformada cuántica de Fourier

Álgebra líneal

- Espacios vectoriales y operadores líneales
- Representaciones matriciales y espectros
- Espacios y operadores unitarios
- Matrices hermíticas, matrices de Pauli

Álgebra multilineal

- Producto tensorial de espacios vectoriales
- Producto tensorial de operadores líneales
- Matrices de Dirac y álgebras de Clifford
- Grupos y álgebras de Lie

Análisis líneal

- Funciones de operadores líneales
- Exponencial de operadores líneales
- Ecuaciones de evolución
- Espacios de Hilbert y álgebras Banach
- Transformada cuántica de Fourier

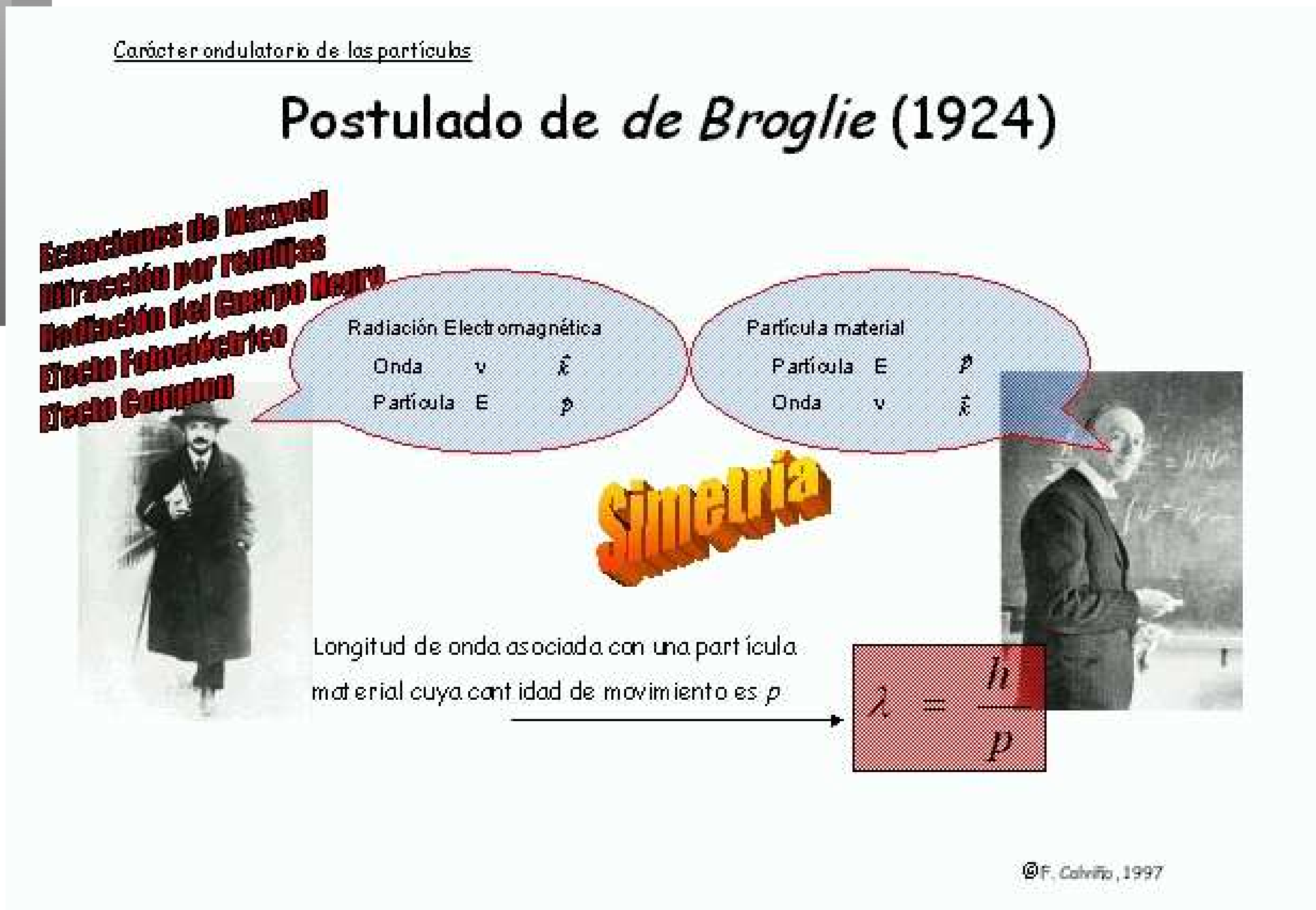
Preliminares físicos

Contenido

- Postulado de de Broglie (1924)
  - Interpretación de las leyes de cuantificación
  - Detección de la naturaleza ondulatoria de la materia
  - Experimento de Davisson-Germer (1927)
  - Interpretación del experimento de Davisson-Germer
- Experimento de la doble rendija (Young)
  - Dualidad onda-partícula
- Ondas de materia
- Interpretación de la función de onda
  - Función de onda. Densidad de probabilidad de presencia
- Ecuación de onda del campo eléctrico

Contenido (cont.)

- Paquete de onda
  - Ejemplo. Suma de dos ondas armónicas
  - Paquetes localizados
  - Definiciones y propiedades
- Principio de incertidumbre de Heisemberg (1927)
- Ecuación de Schrödinger (1925)
- Síntesis y Conclusión


Carácter ondulatorio de las partículas
Postulado de *de Broglie* (1924)
Ecuaciones de Maxwell
Difracción por rendijas
Radiación del Cuerpo Negro
Efecto Fotoeléctrico
Efecto Compton
Radiación Electromagnética
Onda ν $\vec{k}$
Partícula E $\vec{p}$
Partícula material
Partícula E $\vec{p}$
Onda ν $\vec{k}$
Simetría
Longitud de onda asociada con una partícula material cuya cantidad de movimiento es p
$\lambda = \frac{h}{p}$
©F. Calviño, 1997

Interpretación de las leyes de cuantificación

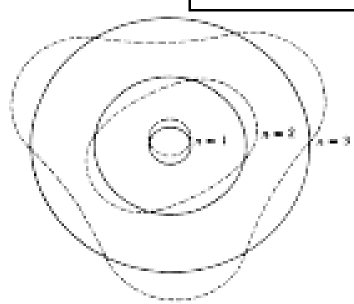
Átomo de Bohr (1913)

Regla: $L = pr = n\hbar$

de Broglie: $\lambda = \dfrac{h}{p}$

$$\boxed{2\pi r = n\lambda}$$

Solo son posibles las órbitas cuya circunferencia pueda contener un número entero de longitudes de onda



Movimiento periódico

En el caso de una partícula cuyo movimiento esté restringido a una región de dimensión ***a*** teníamos,

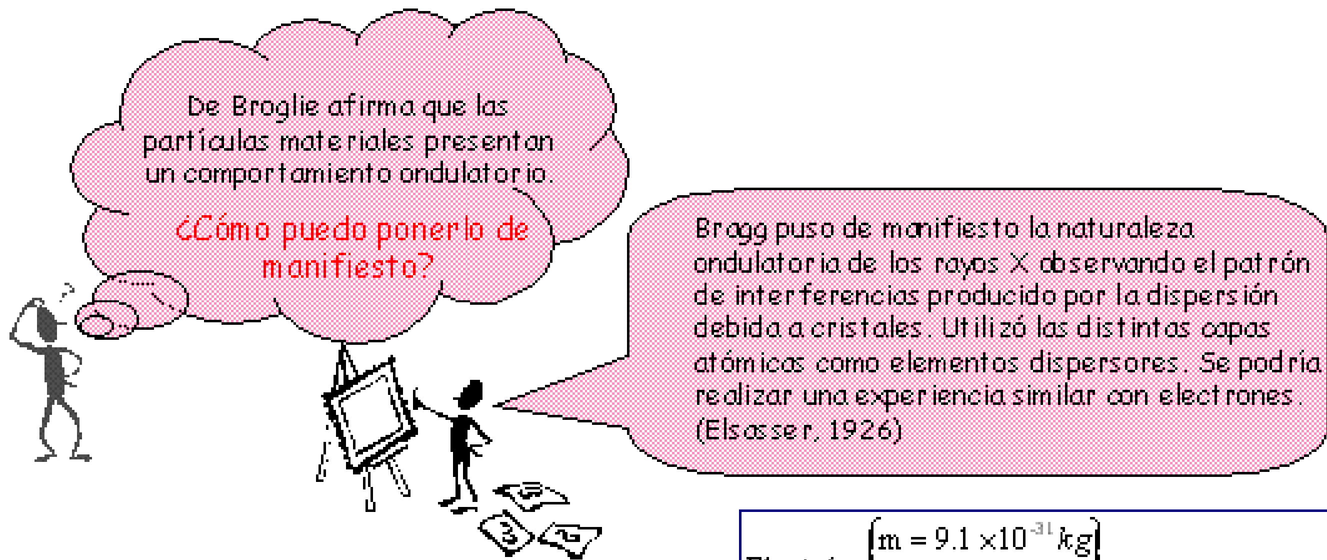
Regla: $p2a = nh$

de Broglie: $\lambda = \dfrac{h}{p}$

$$\boxed{2a = n\lambda}$$

Onda Estacionaria

Detección de la naturaleza ondulatoria de la materia



Para producir un patrón de interferencias necesito una separación entre "rendijas", a, del mismo orden de magnitud que la longitud de onda, λ

$$\lambda = \frac{h}{\sqrt{2mE_c}}$$

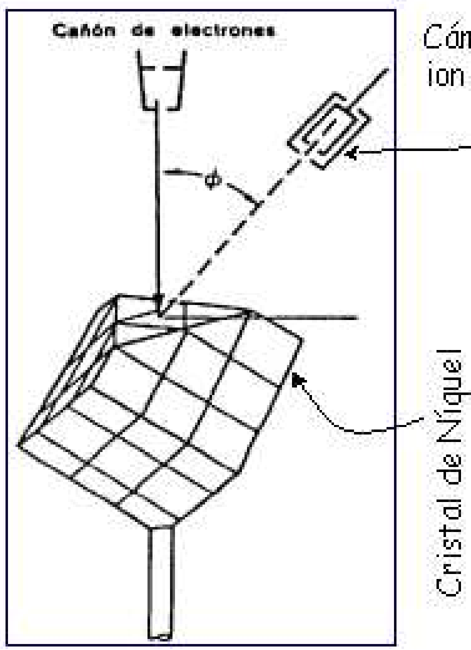
$$\text{Electrón}\begin{Bmatrix} m = 9.1\times10^{-31}\,kg \\ E_c = 50\,eV \end{Bmatrix}$$

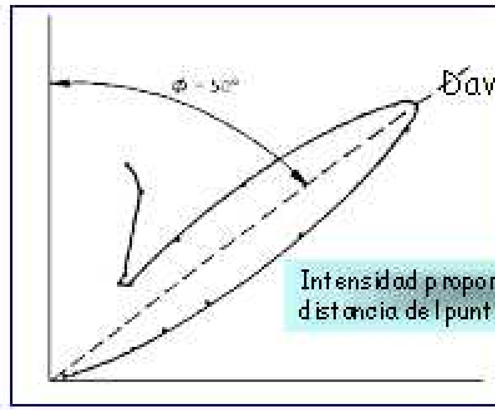
$$\lambda = \frac{6.6\times10^{-34}\,Js}{\left(2\times9.1\times10^{-31}\,kg\times50\,eV\times1.6\times10^{-19}\,J\,eV^{-1}\right)^{1/2}} = 1.7\times10^{-10}\,m = 1.7\,\text{Å}$$

distancia interatómica

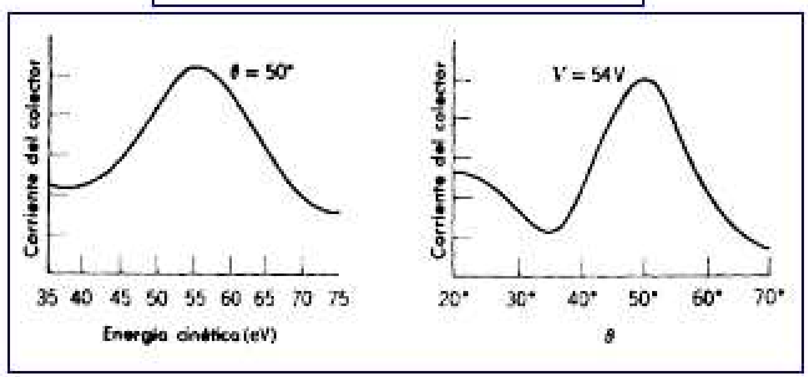
Carácter ondulatorio de las partículas

Experimento de Davisson-Germer (1927)





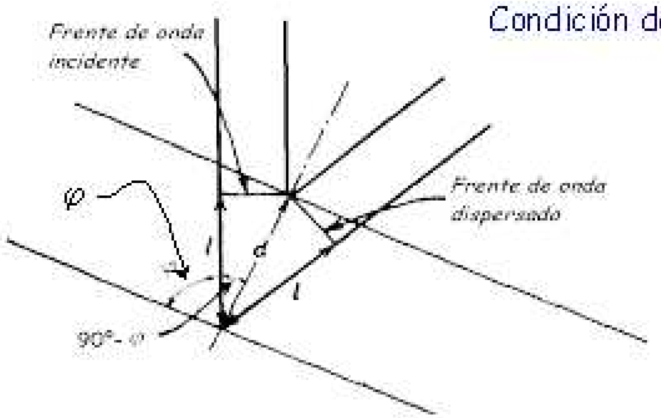
Davisson-Germer



©F. Calviño, 1997

Carácter ondulatorio de las partículas

Interpretación del experimento de Davisson-Germer



Condición de interferencia constructiva (Bragg)

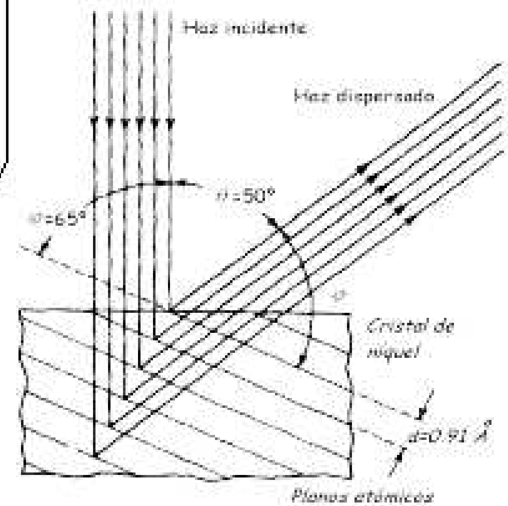
$$\boxed{\begin{aligned} n\lambda &= 2d\,\cos(90-\varphi) \\ &= 2d\,\sin(\varphi) \end{aligned}}$$

$\boxed{\text{de Broglie}} \longrightarrow \lambda(E = 54eV) = 1.66\,\mathring{A}$

$$\Downarrow$$

$$\varphi(n = 1) = 65.8^{\circ}$$

Coinciden...



©F. Calviño, 1997

Experimento de la doble rendija (Young)

Ondas

Onda original dividida en dos cuya superposición produce el patrón de interferencias.

Partículas

Substituyendo la pantalla por una de material fotoeléctrico, y midiendo la energía y estructura temporal de los fotoelectrones.

Comportamiento diferenciado dependiendo del experimento

Paradoja

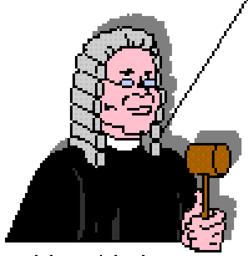
Considerando la radiación electromagnética como fotones, éstos pasarán por una rendija determinada,

¿Cómo es posible que un fotón sufra el efecto de una rendija por la que no ha pasado?

Falacia

No es posible saber por cuál rendija "pasa" el fotón sin medirlo. Ésta medida afectaría de tal forma al comportamiento de los fotones que el patrón de interferencia desaparecería

Dualidad onda-partícula



Un clásico

Un cuántico

En vista de lo expuesto, ¿Cuál es la verdadera naturaleza de un fotón o de un electrón?

¿Onda o partícula?

Los modelos corpuscular y ondulatorio son complementarios; si una medida prueba el carácter ondulatorio, entonces es imposible poner de manifiesto la naturaleza corpuscular en el mismo experimento, y viceversa.

El modelo que se utilice lo determina la naturaleza del experimento

N.Bohr, Principio de Complementariedad

Dualidad: Radiación y materia no son ni simplemente ondas ni simplemente partículas

Conocimiento incompleto a menos que se determinen tanto los aspectos ondulatorios como los corpusculares

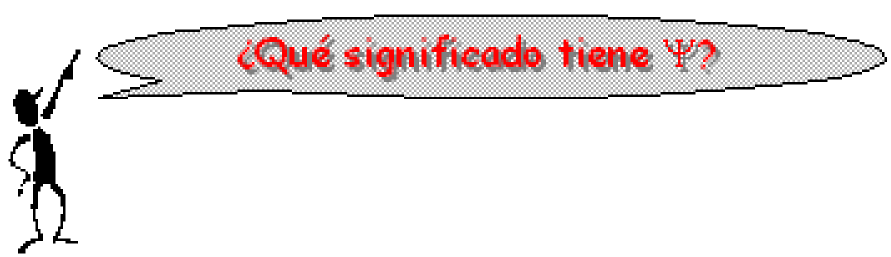
Carácter ondulatorio de las partículas

Ondas de materia

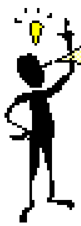
Según de Broglie a toda partícula se le asocia una función de onda.

La función de onda más sencilla que se puede asociar a una partícula de energía, *E*, y cantidad de movimiento, $\vec{p}$, es una onda plana,

$$\Psi(\vec{x},t) = \Psi_0 e^{i(\vec{k}\vec{x} - wt)} \quad \textbf{donde} \quad \begin{cases} w = \dfrac{E}{\hbar} & \text{Pulsación} \\ \vec{k} = \dfrac{\vec{p}}{\hbar} & \text{Vector de onda} \end{cases}$$



Interpretación de la función de onda



Debería ser análoga a la interpretación de las ondas electromagnéticas

EM-Onda

$\varepsilon(x,t)$	Función de onda (Campo eléctrico)
$\lvert\varepsilon(x,t)\rvert^2 \propto$	Densidad de energía (Relacionada con el vector de Poynting)

Fotones (Einstein)

Un haz de fotones de energía, $h\nu$, darán lugar a una densidad energética, $N\,h\nu$, siendo N la densidad promedio de fotones.

Por tanto N es proporcional a $\lvert\varepsilon(x,t)\rvert^2$

$\lvert\varepsilon(x,t)\rvert^2$ indica la densidad de fotones del haz

Materia

$\lvert\Psi(x,t)\rvert^2$ densidad de partículas de un haz

Interpretación

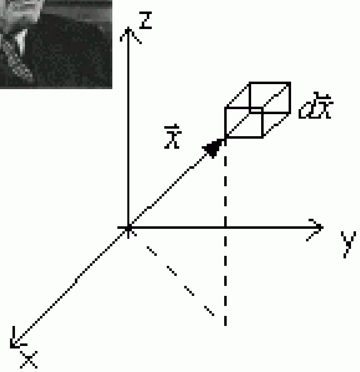
para $\Psi(x,t)$ de una partícula

qué significado tiene $\lvert\Psi(x,t)\rvert^2$

Carácter ondulatorio de las partículas

Función de onda. Densidad de probabilidad de presencia

Max Born, en 1926, interpreta $\left|\Psi(\vec{x},t)\right|^2$ como la **densidad de probabilidad de presencia**



$$\left|\Psi(\vec{x},t)\right|^2 d\vec{x}$$

Representa la probabilidad de encontrar la partícula en $d\vec{x}$ situado en el punto $\vec{x}$, al realizar una medida en el instante t

$$\boxed{\oint\left|\Psi(\vec{x},t)\right|^2 d\vec{x} = 1}$$

Condición de Probabilidad

Onda plana

$$\Psi(\vec{x},t) = \Psi_0 e^{i(\vec{k}\vec{x}-wt)}$$

$$\oint\left|\Psi(\vec{x},t)\right|^2 d\vec{x} = \left|\Psi_0\right|^2 \oint d\vec{x} = \infty$$

Completamente deslocalizada

!

Una partícula "ocupa" solo una fracción de todo el espacio, por tanto, una onda plana no es una buena representación de la partícula

Ecuación de onda del campo eléctrico

Utilizamos el campo eléctrico en el vacío, como ejemplo "bien conocido", para estudiar algunas propiedades comunes a todas la ondas

- Ecuación de onda

Ecuación diferencial lineal que permite obtener las características del "campo" en el espacio y su evolución temporal

$$\frac{\partial^2 \varepsilon}{\partial x^2} - \frac{1}{c^2}\frac{\partial^2 \varepsilon}{\partial t^2} = 0$$

- Función de onda

Solución de la ecuación de onda

$$\varepsilon = \varepsilon(x,t)$$

- Ecuación diferencial lineal

Si $\varepsilon_1(x,t)$ y $\varepsilon_2(x,t)$ son soluciones, entonces cualquier combinación lineal de ambos también es solución,

$$\varepsilon(x,t) = a \cdot \varepsilon_1(x,t) + b \cdot \varepsilon_2(x,t)$$

Principio de Superposición

k, número de onda

w, pulsación

- Soluciones útiles

Armónicas	$\varepsilon(x,t) = \varepsilon_0 \cos(kx - wt)$ $\varepsilon(x,t) = \varepsilon_0 \sin(kx - wt)$
Onda Plana	$\varepsilon(x,t) = \varepsilon_0 e^{i(kx-wt)}$

con $k = \dfrac{w}{c}$

Paquete de onda

Pulsos, por ejemplo un destello de luz, no puede ser descrito por una onda plana (tampoco una partícula puede ser descrita por una onda plana de materia)

Es necesario realizar una superposición (suma o integral) de ondas armónicas o planas de distinta frecuencias, es decir un **paquete de ondas**

El intervalo, Δk, de número de ondas, o el, Δw, de pulsaciones, necesarios para "construir" un pulso están relacionados con la extensión espacial, Δx, o la duración temporal, Δt, del mismo

En general,

$$\Delta k \Delta x \sim 1$$

$$\Delta w \Delta t \sim 1$$

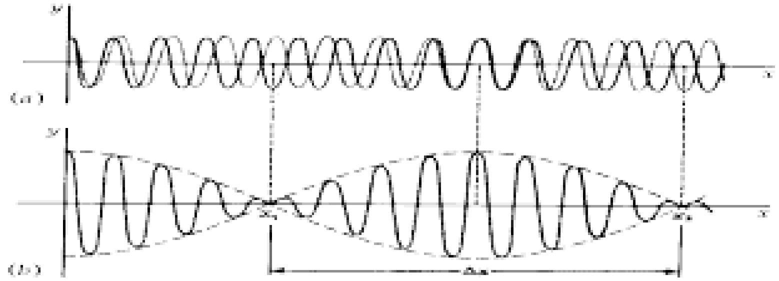
Pulsos localizados espacial o temporalmente, requieren un conjunto de número de ondas o pulsaciones extenso (y viceversa)

Ejemplo. Suma de dos ondas armónicas

Sumando dos ondas armónicas de igual amplitud, cuyas pulsaciones y número de ondas difieren ligeramente, se obtiene una onda resultante modulada

$$\varepsilon(x,t) = \varepsilon_1(x,t) + \varepsilon_2(x,t)$$
$$\varepsilon_1(x,t) = \varepsilon_0 \cos(k_1 x - w_1 t)$$
$$\varepsilon_2(x,t) = \varepsilon_0 \cos(k_2 x - w_2 t)$$

$$\begin{aligned}
\varepsilon(x,t) &= \varepsilon_0 \left(\cos(k_1 x - w_1 t) + \cos(k_2 x - w_2 t)\right) \\
&= 2\varepsilon_0 \cos\left[\frac{1}{2}(k_1 - k_2)x - \frac{1}{2}(w_1 - w_2)t\right] \times \cos\left[\frac{1}{2}(k_1 + k_2)x - \frac{1}{2}(w_1 + w_2)t\right] \\
&= 2\varepsilon_0 \cos\left(\frac{1}{2}\Delta k x - \frac{1}{2}\Delta w t\right) \times \cos\left(\bar{k}x - \bar{w}t\right)
\end{aligned}$$

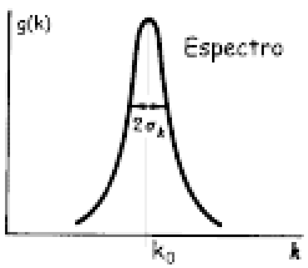


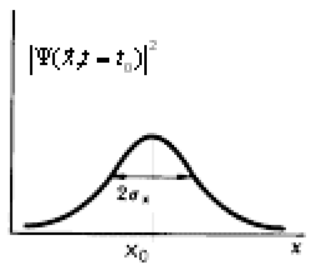
Paquetes localizados

Sumando un número discreto de ondas armónicas, o planas, **no se puede** construir un paquete cuya amplitud al cuadrado sea solo distinta de cero en una zona del espacio o un intervalo de tiempo.
Es necesario utilizar un **número infinito** de número de ondas y/o pulsaciones.

$$\sum_k g_k \cdots \quad \Downarrow \quad \int g(k) \ldots dk$$

$$\Psi(\vec{x},t) = \int g(\vec{k}) e^{i\left(\vec{k}\vec{x} - w(k)t\right)} dk$$





En general w=w(k)

Onda de materia

$$w(k) = \frac{E}{\hbar} = \frac{\left(p^2/2m\right)}{\hbar} = \frac{\hbar}{2m} k^2$$

Onda EM

$$w(k) = \frac{E}{\hbar} = \frac{pc}{\hbar} = ck$$

Paquete de Ondas. Definiciones y propiedades

X_0,	Centro del paquete
K_0,	Centro del espectro
ΔX,	Anchura del paquete ← Zona donde $\lvert\Psi(\vec{x}, t=t_0)\rvert^2 > 0$
Δk,	Anchura del espectro

Velocidad de Grupo, v_g

Velocidad a la que se desplaza el centro del paquete

$$\vec{v}_g = \left.\frac{dw}{d\vec{k}}\right]_{k=k_0}$$

No confundir con la velocidad de fase de cada una de las componentes del paquete.

$$v_f = \frac{w}{k}$$

$\Delta k_x \Delta x \geq 1$
para x,y,z

Paquetes muy localizados se construyen con espectros muy amplios

Casos extremos

- Cantidad de movimiento bien definido pero totalmente deslocalizadas

Onda plana

$$\Psi(\vec{x},t) = \Psi_0 e^{i(\vec{k}\vec{x}-wt)} \longrightarrow \begin{matrix}\Delta k = 0 \\ \Delta x = \infty\end{matrix}$$

- Totalmente localizadas pero de cantidad de movimiento absolutamente indefinido

$$\Psi(\vec{x},t) = \delta(x - x_0, t) \longrightarrow \begin{matrix}\Delta k = \infty \\ \Delta x = 0\end{matrix}$$

Delta de Dirac

Principio de incertidumbre de Heisemberg (1927)

En un sistema físico no se pueden conocer simultáneamente y con absoluta precisión los valores de dos variables canónico-conjugadas

Golpe final a la Física clásica

$$\Delta p_x \Delta x \geq \hbar \quad x, y, z$$

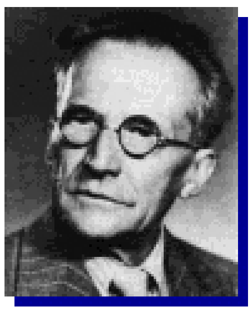
$$\Delta E \Delta t \geq \hbar \quad 4^a \text{ relación}$$

Determinismo clásico
Conociendo las condiciones iniciales de una partícula, y las fuerzas que sobre ella actúan, se puede determinar exactamente su evolución futura (trayectoria)

Interpretación de Heisemberg
La premisa es falsa pues no puedo conocer "exactamente" las condiciones iniciales

Compatible con una representación de las partículas a través de paquete de ondas

Ecuación de Schrödinger (1925)



Ecuación de ondas cuyas soluciones son las funciones de ondas que caracterizan a las partículas sometidas a la acción de fuerzas.

Debe dar lugar a soluciones compatibles con los resultados experimentales

$$\boxed{-\frac{\hbar^2}{2m}\frac{\partial^2\Psi(x,t)}{\partial x^2}+\underbrace{V(x)}_{\text{Potencial}}\Psi(x,t)-i\hbar\frac{\partial\Psi(x,t)}{\partial t}=0}$$

Si V(x)=cte

$$\Psi(\vec{x},t)=\Psi_0 e^{i(\vec{k}\vec{x}-wt)}$$ es solución

$$\Psi(\vec{x},t)=\Psi_0\sin(\vec{k}\vec{x}-wt)$$ no es solución

Carácter ondulatorio de las partículas

Síntesis y Conclusión

Efecto fotoeléctrico

Cuerpo negro

Planck (1901), emisión
Einstein (1905), absorción } de "paquetes" de energía

$$E = h\nu = \hbar w = \frac{hc}{\lambda}$$

Compton (1923), difusión de rayos X por electrones

$$p = \frac{h}{\lambda} = \hbar k$$

→ Interpretación corpuscular de la Radiación EM

De Broglie (1924): Asociar Onda de Materia a las partículas

Davisson-Germer (1927), Difracción de e^- en cristal de Ni

→ Interpretación ondulatoria de las partículas

→ Dualidad Onda-Partícula

Heisemberg (1927), Principio de Indeterminación → **Es necesario "crear" una nueva teoría**

Postulados de la mecánica cuántica

- **Primer postulado:** A cada sistema físico descrito por la mecánica cuántica se le asocia un espacio de Hilbert, y a cada estado del sistema un vector (ket), de ese espacio.
- **Segundo postulado:** Toda cantidad física medible está descrita por un operador $\hat{A}$ que actúa sobre el espacio de Hilbert, este operador es un observable.
- **Tercer postulado:** El único resultado posible de una medida física, es un autovalor del correspondiente observable.

- **Cuarto postulado (caso discreto no degenerado):** Cuando una cantidad física es medida sobre un sistema, el cual está en un estado normalizado $|\,x\rangle$, la probabilidad de encontrar el autovalor a_n correspondiente a un observable $\hat{A}$ es:

$$P(a_n) = |\langle n|x\rangle|^2,$$

donde $|\,n\rangle$ son los autovectores normalizados de $\hat{A}$, asociados a los autovalores a_n.

- **Quinto postulado:** Si la medida de una cantidad física sobre un sistema que está en un estado $|\,x\rangle$ da un resultado a_n, el estado del sistema está, inmediatamente después de la medida, en la proyección normalizada,

$$\frac{\hat{P}_n\,|\,x\rangle}{\sqrt{\langle x|\hat{P}_n|x\rangle}},$$

de $|\,x\rangle$ sobre el auto-subespacio asociado a a_n.

- **Sexto postulado:** La evolución en el tiempo del vector de estado $|\, x(t) \rangle$ es gobernada por la ecuación de Schrödinger:

$$i\hbar \frac{d}{dt} \,|\, x(t) \rangle = H(t) \,|\, x(t) \rangle \,,$$

donde $H(t)$ es el Hamiltoniano del sistema, observable asociado con la energía.

Preliminares informáticos

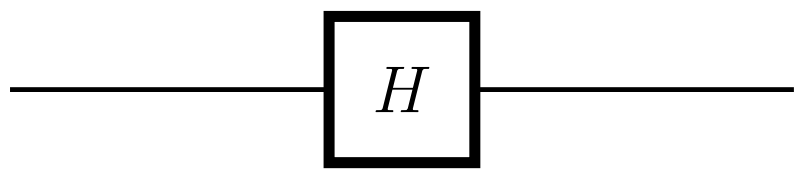
- In(computabilidad)
  - Máquinas de Turing
  - Máquina universal de Turing
  - Compuertas lógicas universales
- In(tratabilidad)
  - Notación asintótica
  - Complejidad algorítmica
  - Clases de complejidad P y NP
  - Problemas NP-completos

Circuitos cuánticos

- Compuertas cuánticas de 1-qubit
  Espacio vectorial de 1-qubit
  Operador unitario sobre 1-qubit
  Matrices de Pauli (X, Y, Z)
  Compuertas de Hadamard (H), fase (S) y $\pi/8$ (T)
  Operadores de rotación y descomposiciones
- Compuertas cuánticas controladas
  Compuerta $CNOT$
  Compuerta U controlada y su implementación
  Compuerta $C^2(U)$ y su implementación
- Compuertas cuánticas universales

Compuerta Hadamard

- Circuito

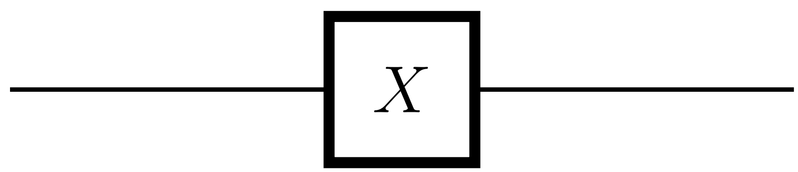


- Representación matricial

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

Compuerta de Pauli X

- Circuito

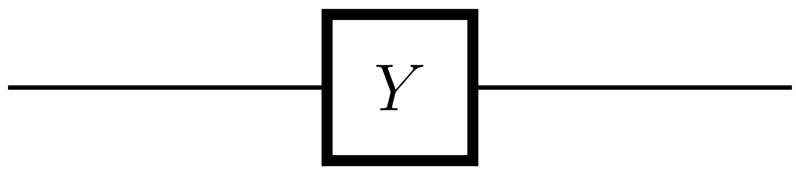


- Representación matricial

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Compuerta de Pauli Y

- Circuito

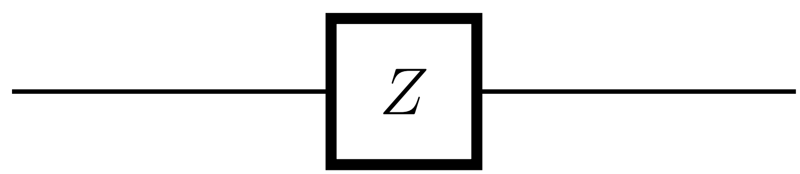


- Representación matricial

$$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Compuerta de Pauli Z

- Circuito

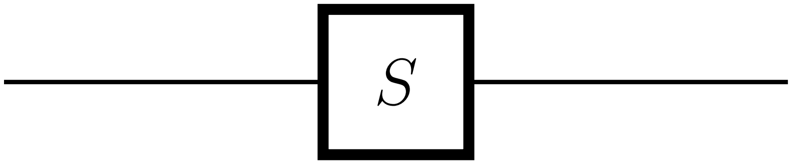


- Representación matricial

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Compuerta de fase

- Circuito

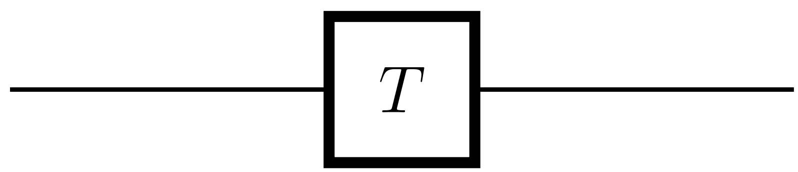


- Representación matricial

$$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

Compuerta $\pi/8$

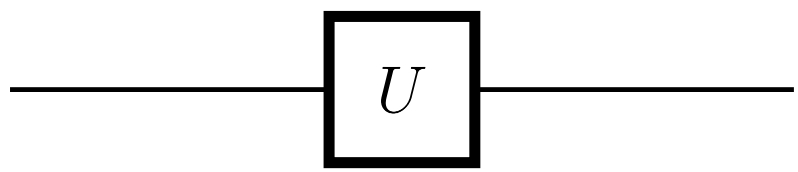
- Circuito



- Representación matricial

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

- Circuito

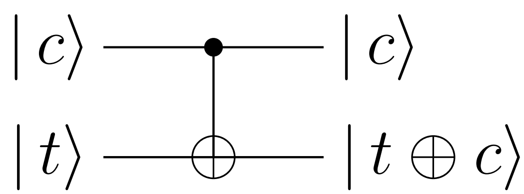


- Representación matricial

$$U = e^{i\alpha} AXBXC, ABC = I$$

Compuerta $CNOT$

- Circuito

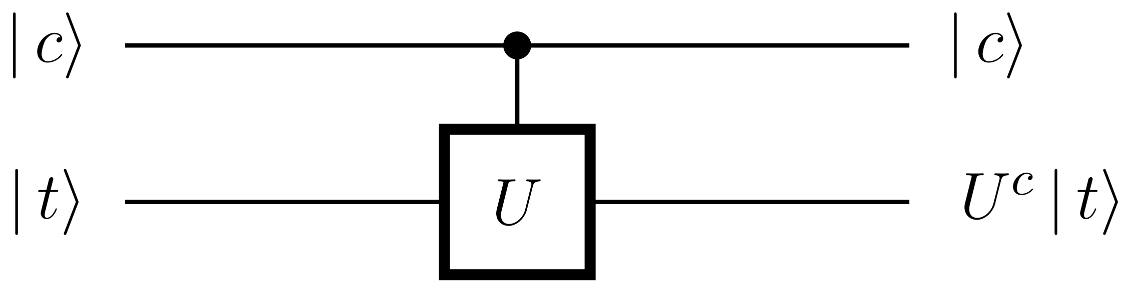


- Representación matricial

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Operación U controlada

- Circuito

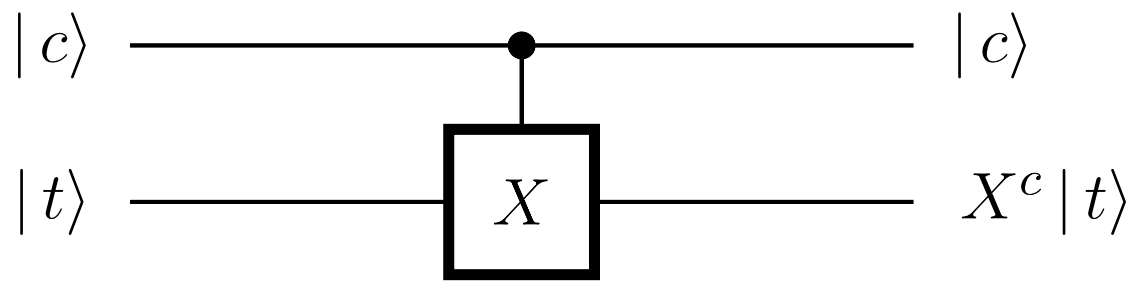


- Representación matricial

$$\begin{bmatrix} I & 0 \\ 0 & U^c \end{bmatrix}$$

Compuerta X controlada

- Circuito

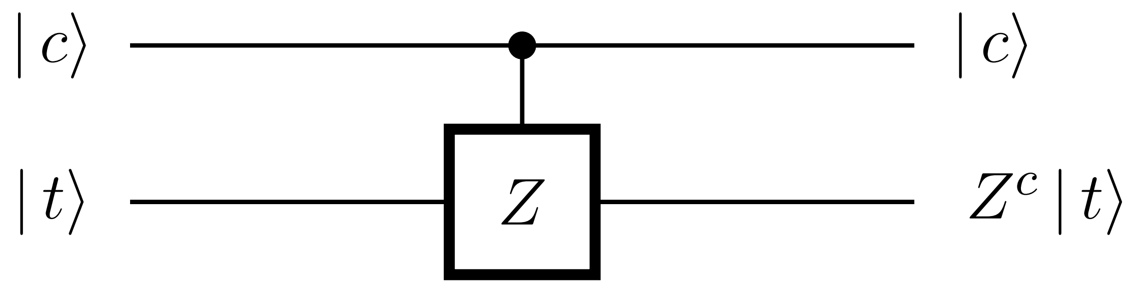


- Representación matricial

$$\begin{bmatrix} I & 0 \\ 0 & X^c \end{bmatrix}$$

Compuerta Z controlada

- Circuito

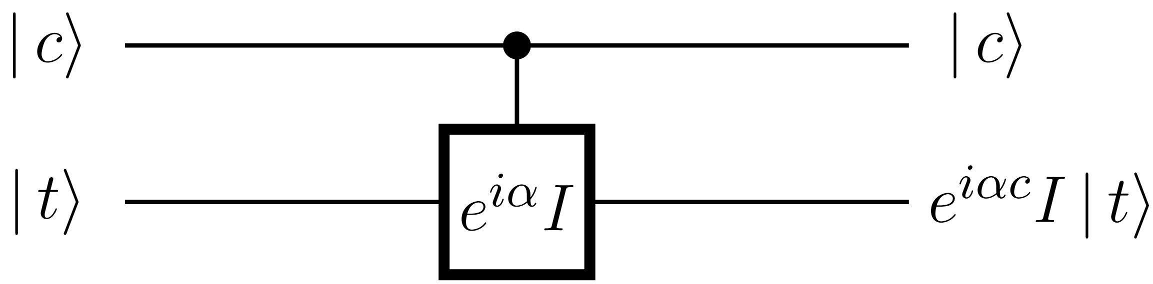


- Representación matricial

$$\begin{bmatrix} I & 0 \\ 0 & Z^c \end{bmatrix}$$

Compuerta corrimiento de fase controlada

- Circuito

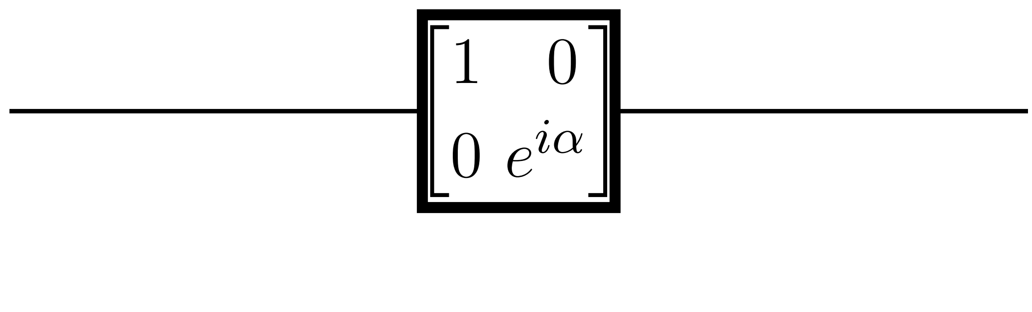


- Representación matricial

$$\begin{bmatrix} I & 0 \\ 0 & e^{i\alpha c}I \end{bmatrix}$$

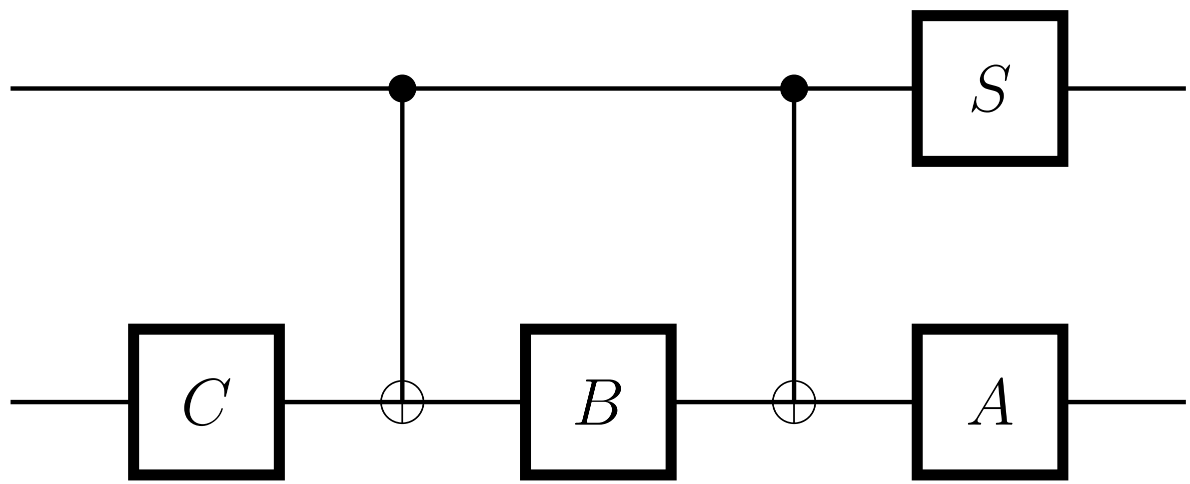
Compuerta corrimiento de fase controlada

- Circuito equivalente



Operación U controlada

- Circuito

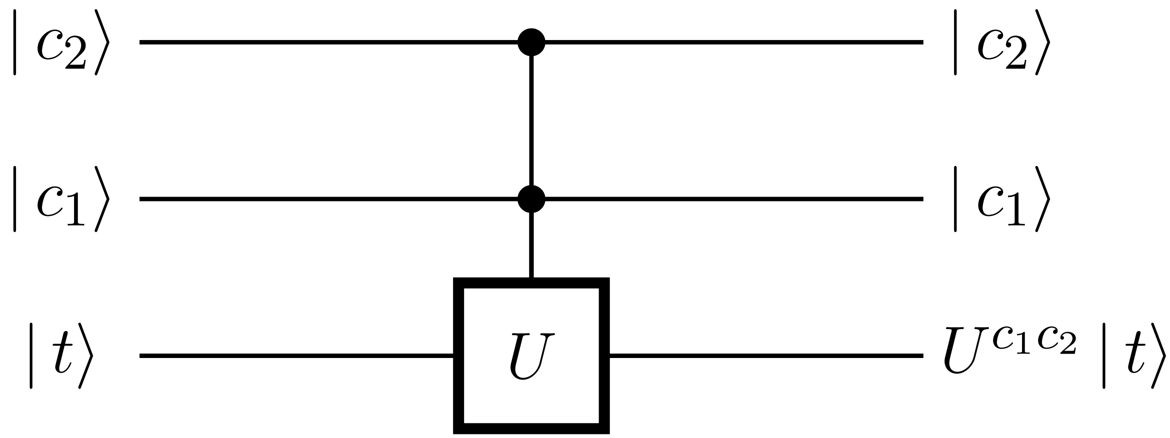


- Representación matricial

$$U = e^{i\alpha} AXBXC, ABC = I$$

Operación $C^2(U)$

- Circuito

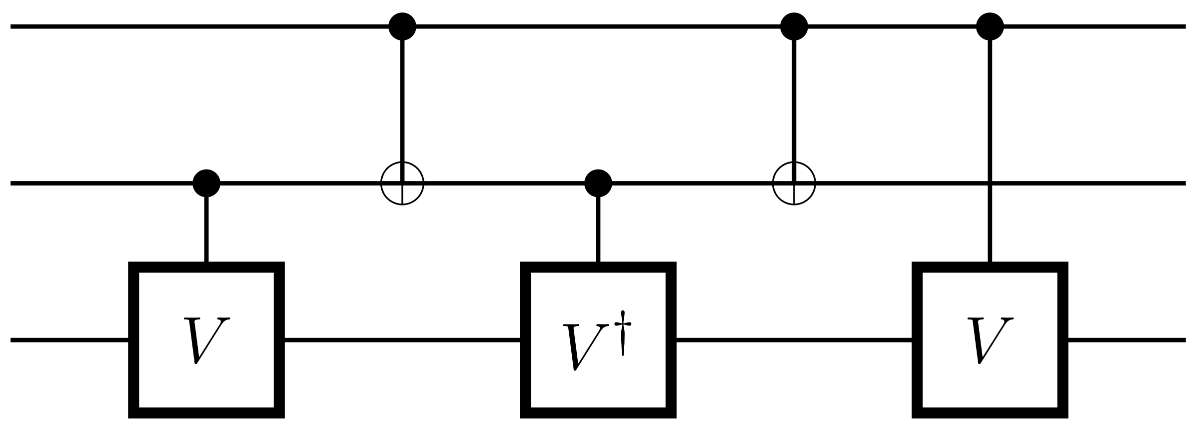


- Representación matricial

$$\begin{bmatrix} I & 0 \\ 0 & U^{c_1c_2} \end{bmatrix}, I = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}$$

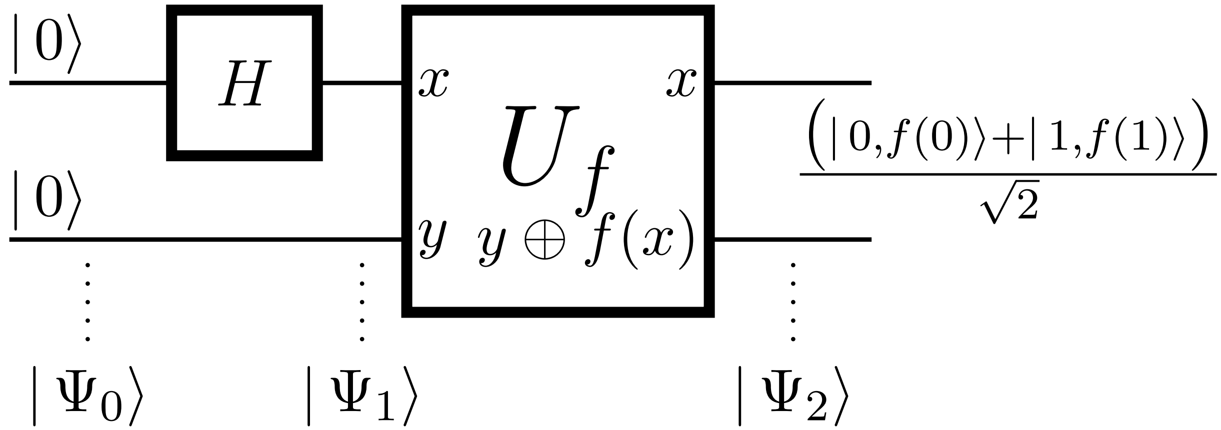
Operacion $C^2(U)$

- Circuito



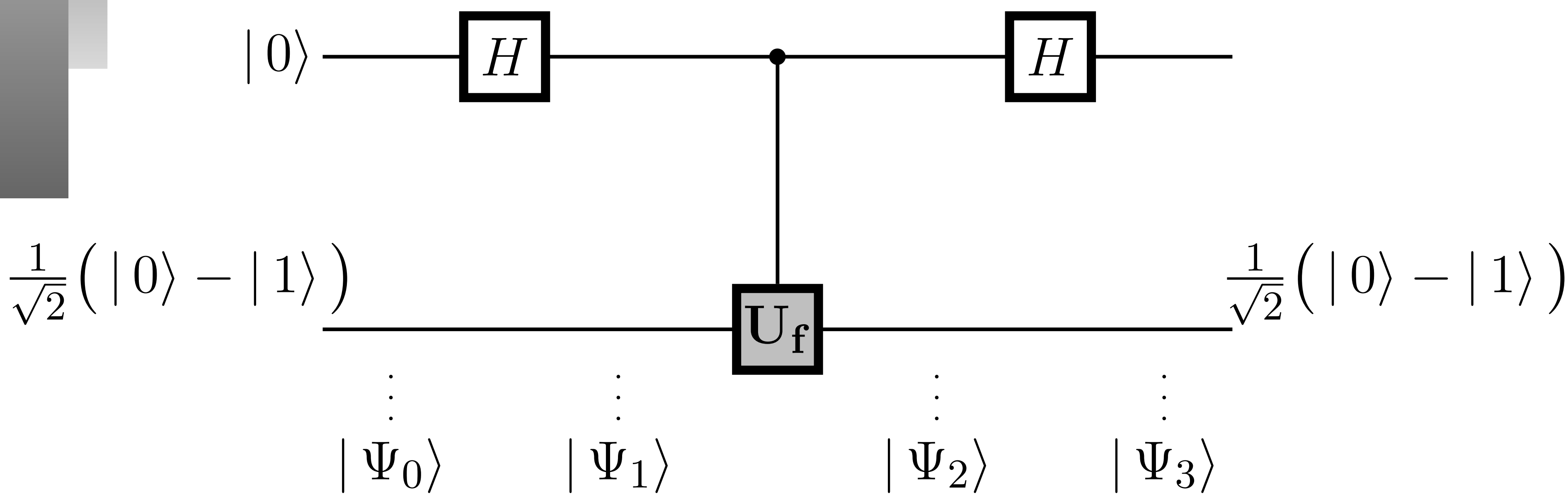
V es cualquier operador unitario que satisface $V^2 = U$. $V \equiv (1-i)(I+iX)/2$ corresponde a la compuerta Toffoli.

Algoritmos cuánticos



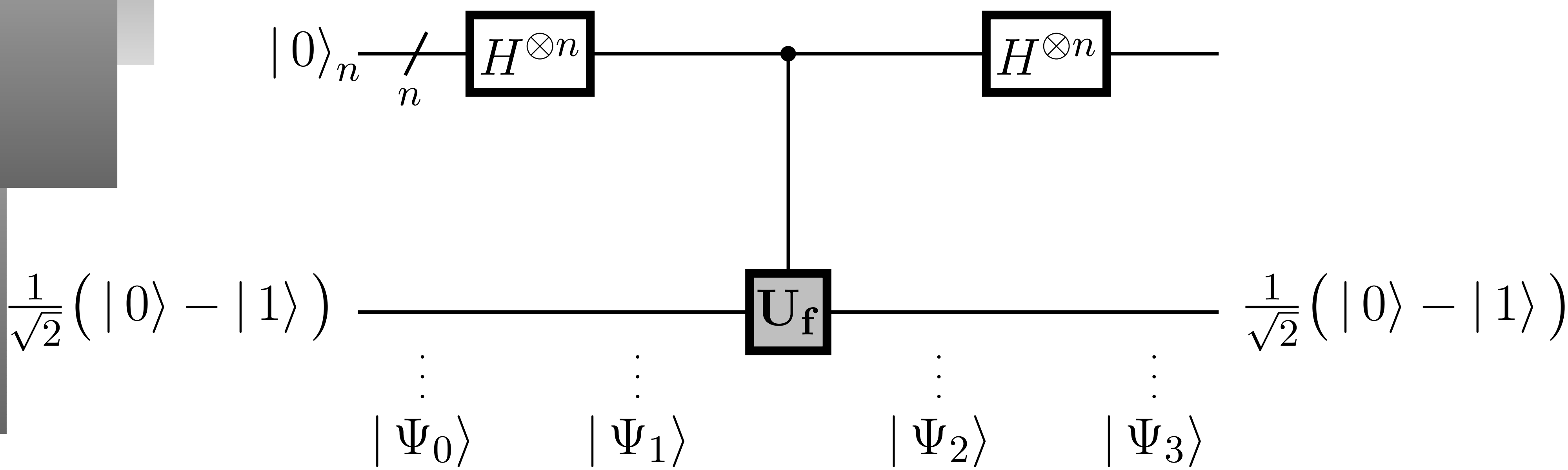
Circuito cuántico para evaluar $f(x) : \{0,1\} \to \{0,1\}$. La compuerta U_f actúa sobre un sistema *2-qubit*. Aprovecha la superposición de estados del primer qubit para evaluar paralelamente $f(0)$ y $f(1)$.

Algoritmo de Deutsch



Circuito cuántico para el Algoritmo Deutsch

Algoritmo de Deutsch-Jozsa



Circuito cuántico para el algoritmo Deutsch-Jozsa

Factorización cuántica

- Transformada cuántica de Fourier
- Estimación de fase
- El orden r de x módulo N
- Algoritmo de Shor

Transformada cuántica de Fourier

En un sistema n-qubit, la transformada cuántica de Fourier F_q sobre los elementos de su base, se define como

$$F_q\colon \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$$
$$|\,k\rangle_n \mapsto c_0\,|\,0\rangle_n + c_1\,|\,1\rangle_n + \ldots + c_{2^n-1}\,|\,2^n-1\rangle \;,$$

donde

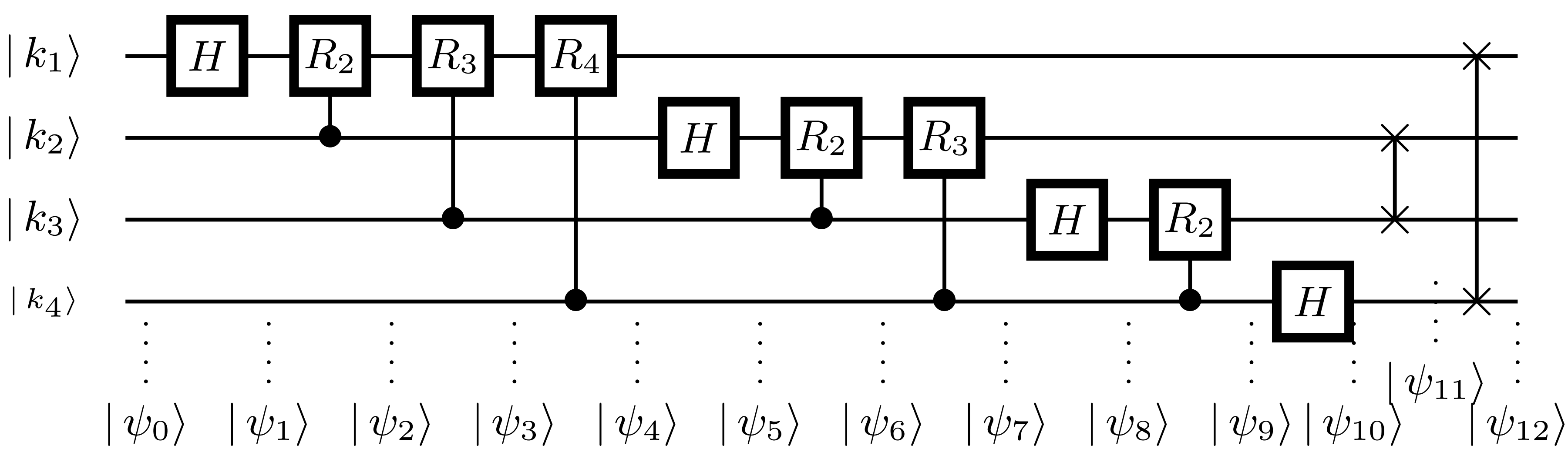
$$F_q\,|\,k\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{\frac{2\pi ijk}{2^n}}\,|\,j\rangle_n \;, \quad \text{para } 0 \leqslant k < 2^n \,.$$

Debido a la *linealidad* de F_q, la transformada de Fourier cuántica sobre un sistema superpuesto $|\,\Psi\rangle = \alpha_0\,|\,0\rangle_n + \alpha_1\,|\,1\rangle_n + \ldots + \alpha_{2^n-1}\,|\,2^n-1\rangle_n$ es

$$\begin{aligned} F_q\,|\,\Psi\rangle &= F_q\left(\alpha_0\,|\,0\rangle_n + \alpha_1\,|\,1\rangle_n + \cdots + \alpha_{2^n-1}\,|\,2^n-1\rangle_n\right) \\ &= \alpha_0 F_q\,|\,0\rangle_n + \alpha_1 F_q\,|\,1\rangle_n + \cdots + \alpha_{2^n-1} F_q\,|\,2^n-1\rangle_n \;. \end{aligned}$$

La F_q para un estado base $|\,k\rangle_n = |\,k_1 k_2 \ldots k_n\rangle$ se puede representar mediante

$$F_q|\,k\rangle_n = \frac{1}{\sqrt{2^n}}\Big(|\,0\rangle + e^{2\pi i 0.k_n}|\,1\rangle\Big)\otimes\Big(|\,0\rangle + e^{2\pi i 0.k_{n-1}k_n}|\,1\rangle\Big)\otimes\cdots\otimes\Big(|\,0\rangle + e^{2\pi i 0.k_1 k_2\ldots k_n}|\,1\rangle\Big).$$



En un sistema n-qubit, la inversa de F_q sobre los elementos de su base, se define como

$$\begin{aligned} F_q^{-1} \colon \mathbb{C}^{2^n} &\to \mathbb{C}^{2^n} \\ |\, k\rangle_n &\mapsto c_0 \,|\, 0\rangle_n + c_1 \,|\, 1\rangle_n + \ldots + c_{2^n-1} \,|\, 2^n - 1\rangle \ , \end{aligned}$$

donde

$$F_q^{-1} \,|\, k\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{-\frac{2\pi i j k}{2^n}} \,|\, j\rangle_n \ , \quad \text{para } 0 \leqslant k < 2^n \, .$$

Estimación de fase

Problema: Suponga un operador unitario U con un autovector $|\,u\rangle$ y un autovalor asociado $e^{2\pi i\varphi}$, es decir, $U\,|\,u\rangle = e^{2\pi i\varphi}\,|\,u\rangle$. El problema de la estimación de fase es determinar φ, con $\varphi \in [0,1)$.

Se define la compuerta V de tal forma que

$$\begin{aligned} V(|\,j\rangle_t\,|\,u\rangle_m) &= |\,j\rangle\,U^j\,|\,u\rangle \\ &= |\,j\rangle\,e^{2\pi i\varphi j}\,|\,u\rangle \\ &= e^{2\pi i\varphi j}\,|\,j\rangle\,|\,u\rangle\ . \end{aligned}$$

Algoritmo para la estimación de fase

1. Estado inicial del sistema $(t+n)$-*qubit*

$$|\,\Psi_0\rangle = |\,0\rangle_t\,|\,u\rangle_m\ .$$

2. Creación de una superposición de estados al aplicar $H^{\otimes t}$ sobre el primer registro

$$|\,\Psi_1\rangle = \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|\,j\rangle_t\,|\,u\rangle_m\ .$$

3. Se aplica V al sistema $(t+m)$-*qubit*

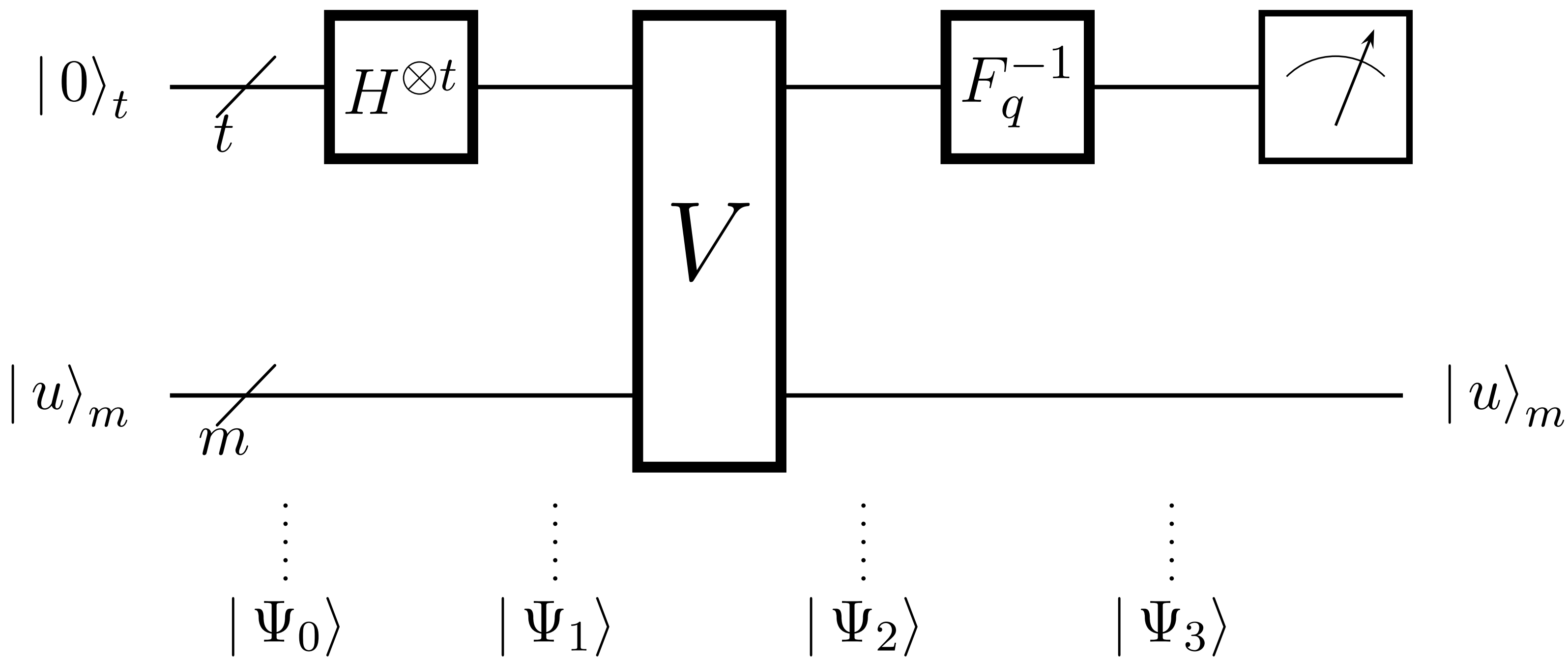
$$
\begin{aligned}
|\,\Psi_2\rangle &= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} V(|\,j\rangle_t\,|\,u\rangle_m) \\
&= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |\,j\rangle_t\, U^j\,|\,u\rangle_m \\
&= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i \varphi j}\,|\,j\rangle_t\,|\,u\rangle_m \ .
\end{aligned}
$$

4. Se aplica F_q^{-1} al primer registro

$$
\begin{aligned}
|\,\Psi_3\rangle &= \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1} e^{2\pi i\varphi j}\,\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1} e^{\frac{-2\pi ijk}{2^t}}\;|\,k\rangle_t\,|\,u\rangle_m \\
&= \sum_{k=0}^{2^t-1}\frac{1}{2^t}\sum_{j=0}^{2^t-1} e^{2\pi i\left(\varphi-\frac{k}{2^t}\right)j}\;|\,k\rangle_t\,|\,u\rangle_m \\
&= \left|\,\widetilde{\varphi}\times 2^t\right\rangle_t |\,u\rangle_m \;.
\end{aligned}
$$

5. Se mide el primer registro y se divide por 2^t para obtener $\widetilde{\varphi}$.

Circuito para la estimación de fase



El orden r de x módulo N

Sean x, N dos enteros positivos coprimos con $x < N$. El orden de x módulo N es el menor entero positivo r, tal que $x^r \bmod N = 1$.

Ejemplo: Sean $x = 5$ y $N = 21$, el orden r de 5 módulo 21 es 6, pues

$$
\begin{aligned}
5^1 \bmod 21 &= 5\,,\\
5^2 \bmod 21 &= 4\,,\\
5^3 \bmod 21 &= 20\,,\\
5^4 \bmod 21 &= 16\,,\\
5^5 \bmod 21 &= 17\,,\\
5^6 \bmod 21 &= 1\,.
\end{aligned}
$$

Algoritmo para hallar el orden r de x módulo N

1. Estado inicial

$$|\,\Psi_0\rangle = |\,0\rangle_t\,|\,1\rangle_n\ .$$

2. Empleando $H^{\otimes t}$ se crea una *superposición uniforme* de todos los estados de la base del sistema *t-qubit* sobre el primer registro

$$|\,\Psi_1\rangle = \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|\,j\rangle_t\,|\,1\rangle_n$$

3. Se aplica la compuerta $V_{(x,N)}$ a todo el sistema

$$| \Psi_2\rangle = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} V_{(x,N)} \left(| j\rangle_t \, | 1\rangle_n\right)$$

$$= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} | j\rangle_t \left| x^j \bmod N \right\rangle_n \, .$$

Suponga que r es potencia de dos de esta forma

$$| \Psi_2\rangle = \frac{1}{\sqrt{2^t}} \sum_{b=0}^{r-1} \sum_{a=0}^{\frac{2^t}{r}-1} | ar + b\rangle_t \left| x^b \bmod N \right\rangle_n \, .$$

4. Se mide el segundo registro y, con probabilidad $1/r$, se obtiene un estado $\left|\, x^{b'} \bmod N \right\rangle$ de los r posibles

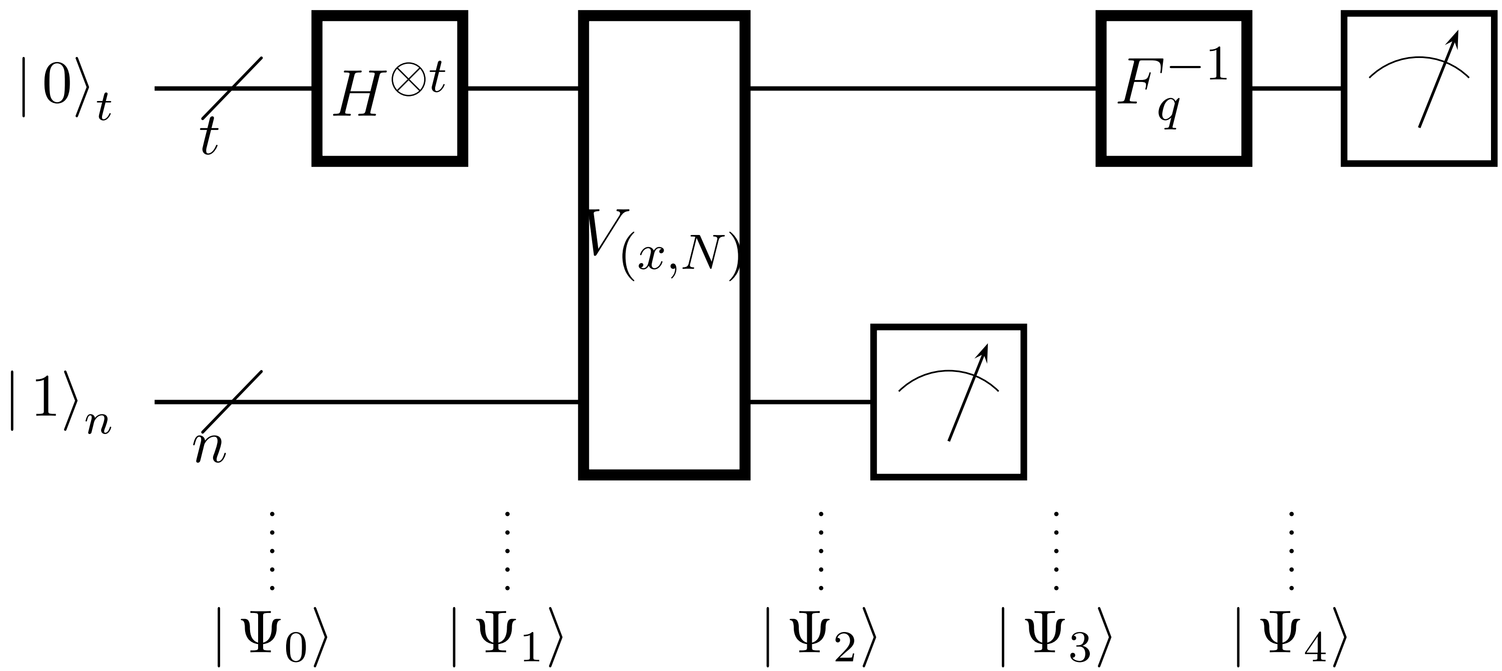
$$| \Psi_3 \rangle = \frac{1}{\sqrt{2^t/r}} \sum_{a=0}^{\frac{2^t}{r}-1} \left|\, ar + b' \right\rangle_t \left|\, x^{b'} \bmod N \right\rangle_n .$$

5. Se aplica F_q^{-1} al primer registro

$$
\begin{aligned}
|\,\Psi_4\rangle &= \frac{1}{\sqrt{2^t/r}} \sum_{a=0}^{\frac{2^t}{r}-1} \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{\frac{-2\pi i k(ar+b')}{2^t}} \,|\,k\rangle_t \left| x^{b'} \text{ mód } N \right\rangle_n \\
&= \frac{1}{\sqrt{r}} \sum_{k=0}^{2^t-1} \frac{1}{2^t/r} \sum_{a=0}^{\frac{2^t}{r}-1} e^{-2\pi i\left(\frac{k}{2^t/r}\right)a} e^{-2\pi i\left(\frac{k}{2^t}\right)b'} \,|\,k\rangle_t \left| x^{b'} \text{ mód } N \right\rangle_n \\
&= \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i\left(\frac{s}{r}\right)b'} \left| s \cdot \frac{2^t}{r} \right\rangle_t \left| x^{b'} \text{ mód } N \right\rangle_n .
\end{aligned}
$$

6. Se mide el primer registro y se obtiene $s' \cdot \frac{2^t}{r}$, donde s' toma cualquier valor entre cero y $(r-1)$. Luego se divide por 2^t y se aplica el algoritmo de fracciones continuas para obtener r o un r' factor de r.

Circuito para hallar el orden r de x módulo N



Problema: Dado un entero N, determinar sus factores primos no triviales.

1. Mientras que N sea par divida N por dos y retorne el factor 2.
2. Verifique que N sea compuesto. Mediante el algoritmo de *Manindra* esto es posible en tiempo polinomial.
3. Determine si N es de la forma a^b, con $a > 2$ y $b \geqslant 2$, pues el método para *encontrar el orden* puede fallar si N es de esta forma con a primo impar. Si $N = a^b$, retorne b veces el factor a. Si N no es de la forma a^b vaya al paso (4).

4. Aleatoriamente elija un x, tal que $1 < x < N - 1$. Mediante el algoritmo de Euclides encuentre el máximo común divisor entre x y N. Mientras que $\mathrm{m.c.d.}(x, N) > 1$, retorne el factor $\mathrm{m.c.d.}(x, N)$ y a N asígnele N dividido por $\mathrm{m.c.d.}(x, N)$.
   Si ahora N es un número primo termine el algoritmo. De lo contrario evalúe si es necesario encontrar los otros factores de N cuánticamente. En caso afirmativo vaya al paso (5), sino, encuentre los otros factores clásicamente.
5. Ejecute el algoritmo cuántico para encontrar el orden r de x módulo N.

6. Si r es impar hay que ejecutar nuevamente la parte cuántica del algoritmo con un nuevo x, vaya al paso (4). Si r es par se define y como

$$x^{r/2} \bmod N = y\,, \tag{1}$$

donde $0 \leqslant y < N$. De (1) se tiene que $x^{r/2} = k_1 N + y$, al elevar al cuadrado a ambos lados se obtiene

$$\begin{aligned} x^r &= k_1^2 N^2 + 2k_1 N y + y^2 \\ x^r &= \left(k_1^2 N + 2k_1 y\right) N + y^2 \\ x^r &= k_2 N + y^2\,. \end{aligned} \tag{2}$$

Ahora, como $x^r \bmod N = 1$ entonces

$$x^r = k_3 N + 1 \,. \tag{3}$$

De la diferencia entre (2) y (3) se encuentra que $(y-1)(y+1) = (k_3 - k_2)N$, es decir, N divide a $(y-1)(y+1)$.
Luego, si $1 < y < N-1$ entonces $0 < y-1 < y+1 < N$, lo cual implica que N no divide a $y-1$ ó a $y+1$ separadamente. Se concluye que $y-1$ y $y+1$ contienen factores de N por el *teorema fundamental de la aritmética*. Así, el $\mathrm{m.c.d.}(y-1, N)$ y el $\mathrm{m.c.d.}(y+1, N)$ son factores no triviales de N.

Simuladores cuánticos

En computación, la simulación es la ejecución de un algoritmo que finge un sistema de tal forma que *dadas unas condiciones iniciales*, se pretende determinar *cuáles serán las condiciones finales de éste*.

- **En el presente:** software clásico ejecutable en un computador clásico que sólo alcanza a simular sistemas cuánticos pequeños.

- **En el futuro:** software cuántico ejecutable en un computador cuántico que tendrá el potencial de simular sistemas cuánticos grandes.

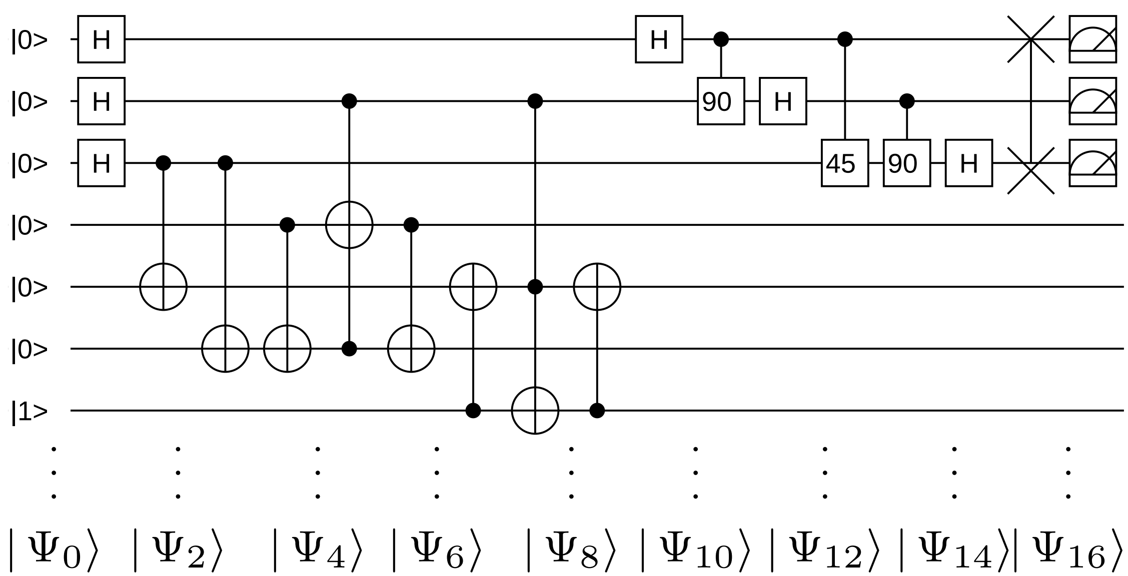
En `www.vcpc.univie.ac.at/~ian/hotlist/qc/programming.shtml` hay una lista de enlaces a simuladores y lenguajes de computación cuántica. Dos de ellos que permiten la construcción y simulación de circuitos cuánticos son:

- **qcad**
- **QuaSi**

- **Ventajas:**
  - ✓ Su *GUI* es amigable.
  - ✓ La contrucción de los circuitos es fácil.
  - ✓ Resultados en forma gráfica, además de la notación de *Dirac*.

- **Desventajas:**
  - ✓ Compuertas de medición ignoradas.
  - ✓ No permite la realización de la simulación paso a paso.
  - ✓ Para mostrar los resultados representa los qubits de derecha a izquierda así $|\, x_n x_{n-1} \ldots x_2 x_1 \rangle$, es decir, el primer qubit es el del extremo derecho y el último es el del extremo izquierdo. Esto es contrario a la forma usual.
  - ✓ El usuario no puede definir sus propias compuertas. Está limitado a las predefinidas.

El siguiente circuito fue construido y simulado utilizando **quasi**. Este circuito es una implementación optimizada del algoritmo de *Shor* para factorizar el número 15 con $x = 7$.



Resultado simulación

$$
\begin{aligned}
|\,\Psi\rangle = \frac{1}{4}\Big(& |\,0010\rangle\,|\,000\rangle + |\,0010\rangle\,|\,001\rangle - \\
& |\,0010\rangle\,|\,010\rangle - |\,0010\rangle\,|\,011\rangle + \\
& |\,1000\rangle\,|\,000\rangle + |\,1000\rangle\,|\,001\rangle + \\
& |\,1000\rangle\,|\,010\rangle + |\,1000\rangle\,|\,011\rangle + \\
& |\,1011\rangle\,|\,000\rangle - |\,1011\rangle\,|\,001\rangle - \\
& i\,|\,1011\rangle\,|\,010\rangle + i\,|\,1011\rangle\,|\,011\rangle + \\
& |\,1110\rangle\,|\,000\rangle - |\,1110\rangle\,|\,001\rangle + \\
& i\,|\,1110\rangle\,|\,010\rangle - i\,|\,1110\rangle\,|\,011\rangle\,\Big).
\end{aligned}
$$

- **Ventajas:**
  - ✓ Simulación paso a paso.
  - ✓ Solamente los resultados con amplitudes diferentes de cero son mostrados.
  - ✓ Demostraciones del algoritmo de *Shor*, del algoritmo de *Deutsch-Jozsa* y del algoritmo de *Grover*.

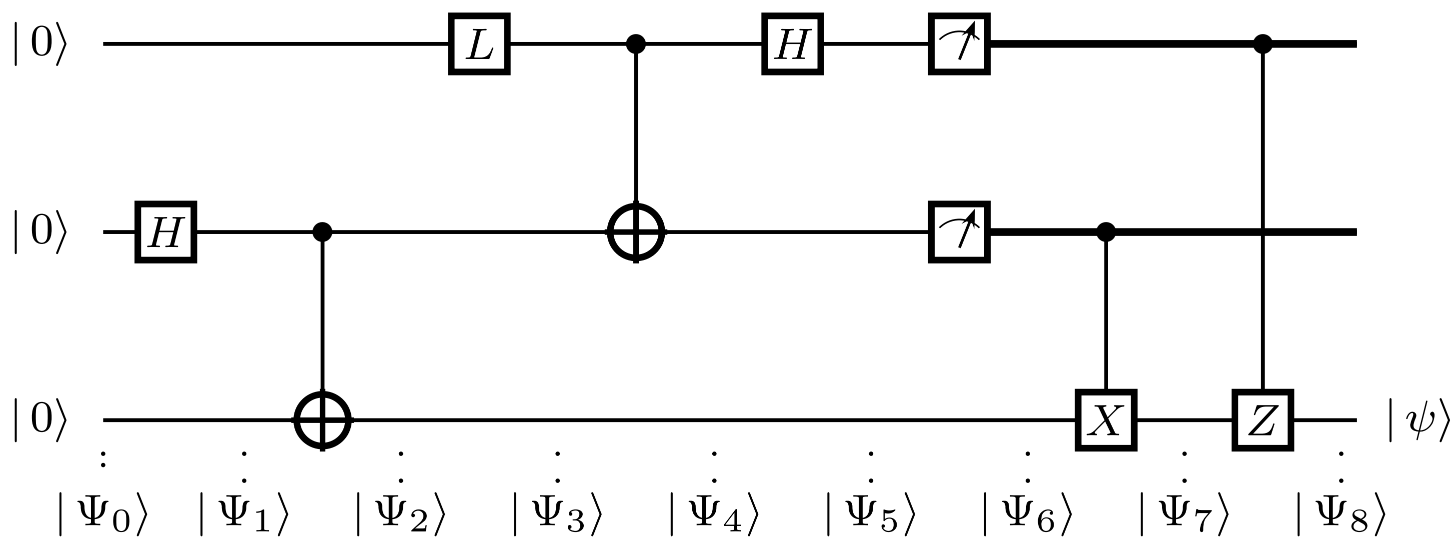
QuaSi

- ✓ Su *GUI* consta de cuatro ventanas: en la primera se construye el circuito; en la segunda se observa la evolución de la simulación en la notación de *Dirac*; en la tercera se grafica el valor absoluto de cada amplitud y su desplazamiento de fase relativo y en la cuarta ventana las amplitudes son mostradas divididas en su parte real (azul) e imaginaria (roja).
- ✓ Permite la creación de compuertas definidas por el usuario, definir funciones y cargar archivos *XML* que contienen instrucciones para la creación de circuitos cuánticos.

- **Desventajas:**
  - ✓ Algunas veces se bloquea durante la construcción del circuito.
  - ✓ Es tedioso a la hora de hacer modificaciones a los circuitos.
  - ✓ Al repetir la simulación de un circuito n veces los datos obtenidos no corresponden con los esperados estadísticamente.

Ejemplo: teleportación cuántica

Circuito cuántico para transportar un qubit de un espacio físico a otro en ausencia de un canal físico de comunicación.



$$
\begin{aligned}
|\,\Psi_0\rangle &= |\,0\rangle\,|\,0\rangle\,|\,0\rangle\ , \\
|\,\Psi_1\rangle &= |\,0\rangle\,\tfrac{1}{\sqrt{2}}\big(\,|\,0\rangle + |\,1\rangle\,\big)\,|\,0\rangle \\
&= |\,0\rangle\,\tfrac{1}{\sqrt{2}}\big(\,|\,00\rangle + |\,10\rangle\,\big)\,, \\
|\,\Psi_2\rangle &= |\,0\rangle\,\tfrac{1}{\sqrt{2}}\big(\,|\,00\rangle + |\,11\rangle\,\big)\,, \\
|\,\Psi_3\rangle &= \big(\alpha\,|\,0\rangle + \beta\,|\,1\rangle\,\big)\,\tfrac{1}{\sqrt{2}}\big(\,|\,00\rangle + |\,11\rangle\,\big) \\
&= \tfrac{\alpha}{\sqrt{2}}\big(\,|\,000\rangle + |\,011\rangle\,\big) + \tfrac{\beta}{\sqrt{2}}\big(\,|\,100\rangle + |\,111\rangle\,\big)\,, \\
|\,\Psi_4\rangle &= \tfrac{\alpha}{\sqrt{2}}\big(\,|\,000\rangle + |\,011\rangle\,\big) + \tfrac{\beta}{\sqrt{2}}\big(\,|\,110\rangle + |\,101\rangle\,\big) \\
&= \tfrac{\alpha}{\sqrt{2}}\,|\,0\rangle\,\big(\,|\,00\rangle + |\,11\rangle\,\big) + \tfrac{\beta}{\sqrt{2}}\,|\,1\rangle\,\big(\,|\,10\rangle + |\,01\rangle\,\big)\,, \\
|\,\Psi_5\rangle &= \tfrac{\alpha}{2}\big(\,|\,0\rangle + |\,1\rangle\,\big)\big(\,|\,00\rangle + |\,11\rangle\,\big) + \tfrac{\beta}{2}\big(\,|\,0\rangle - |\,1\rangle\,\big)\big(\,|\,10\rangle + |\,01\rangle\,\big) \\
&= \tfrac{\alpha}{2}\big(\,|\,000\rangle + |\,011\rangle + |\,100\rangle + |\,111\rangle\,\big) + \tfrac{\beta}{2}\big(\,|\,010\rangle + |\,001\rangle - |\,110\rangle - |\,101\rangle\,\big)\,,
\end{aligned}
$$

- Si al medir los primeros dos qubits se obtiene el estado $|\,00\rangle$ entonces

$$
\begin{aligned}
|\,\Psi_6\rangle &= \alpha\,|\,000\rangle + \beta\,|\,001\rangle \\
&= |\,00\rangle\,\big(\alpha\,|\,0\rangle + \beta\,|\,1\rangle\,\big)\,, \\
|\,\Psi_8\rangle &= |\,\Psi_7\rangle = |\,\Psi_6\rangle\ .
\end{aligned}
$$

- Si al medir los primeros dos qubits se obtiene el estado $|\,01\rangle$ entonces

$$
\begin{aligned}
|\,\Psi_6\rangle &= \alpha\,|\,011\rangle + \beta\,|\,010\rangle \\
&= |\,01\rangle\,\big(\alpha\,|\,1\rangle + \beta\,|\,0\rangle\,\big)\,, \\
|\,\Psi_7\rangle &= |\,01\rangle\,\big(\alpha\,|\,0\rangle + \beta\,|\,1\rangle\,\big)\,, \\
|\,\Psi_8\rangle &= |\,\Psi_7\rangle\ .
\end{aligned}
$$

- Si al medir los primeros dos qubits se obtiene el estado $|\,10\rangle$ entonces

$$
\begin{aligned}
|\,\Psi_6\rangle &= \alpha\,|\,100\rangle - \beta\,|\,101\rangle \\
&= |\,10\rangle\,\big(\alpha\,|\,0\rangle - \beta\,|\,1\rangle\,\big)\,, \\
|\,\Psi_7\rangle &= |\,\Psi_6\rangle\ , \\
|\,\Psi_8\rangle &= |\,10\rangle\,\big(\alpha\,|\,0\rangle + \beta\,|\,1\rangle\,\big)\,.
\end{aligned}
$$

- Si al medir los primeros dos qubits se obtiene el estado $|\,11\rangle$ entonces

$$
\begin{aligned}
|\,\Psi_6\rangle &= \alpha\,|\,111\rangle - \beta\,|\,110\rangle \\
&= |\,11\rangle\,\big(\alpha\,|\,1\rangle - \beta\,|\,0\rangle\,\big)\,, \\
|\,\Psi_7\rangle &= |\,11\rangle\,\big(\alpha\,|\,0\rangle - \beta\,|\,1\rangle\,\big)\,, \\
|\,\Psi_8\rangle &= |\,11\rangle\,\big(\alpha\,|\,0\rangle + \beta\,|\,1\rangle\,\big)\,.
\end{aligned}
$$

Realización física

- Resonancia nuclear magnética (NMR)
- Implementación NMR con fase geométrica
- Computador cuántico atómico
- Iones atrapados
- Implementación óptica