Procesamiento Cuántico de Datos

Miguel Arizmendi, Gustavo Zabaleta

6 de diciembre de 2016

Sitio web: www3.fi.mdp.edu.ar/fes/ProcQ.html

ALGORITMOS CUÁNTICOS AVANZADOS

Algoritmo de Bernstein-Vazirani

Algoritmo de Bernstein-Vazirani

Objetivo: Encontrar la cadena de n bits $\mathbf{s}$

Se tiene una función de n bits

$$f : \{0,1\}^n \rightarrow \{0,1\}$$

Siendo: $f_s(\mathbf{x}) = \mathbf{x}.\mathbf{s}$

- $\mathbf{s}$ es una cadena de n bits desconocida.
- $\mathbf{x}.\mathbf{s} = x_1 s_1 + x_2 s_2 + \cdots + x_n s_n$.

Algoritmo de Bernstein-Vazirani

¿Cuál es la complejidad de este problema considerado clásicamente?

Cálculo Exacto:

- Cada consulta a la función nos puede dar 1 solo bit de información sobre **s**.

El número de consultas debe ser como mínimo n.

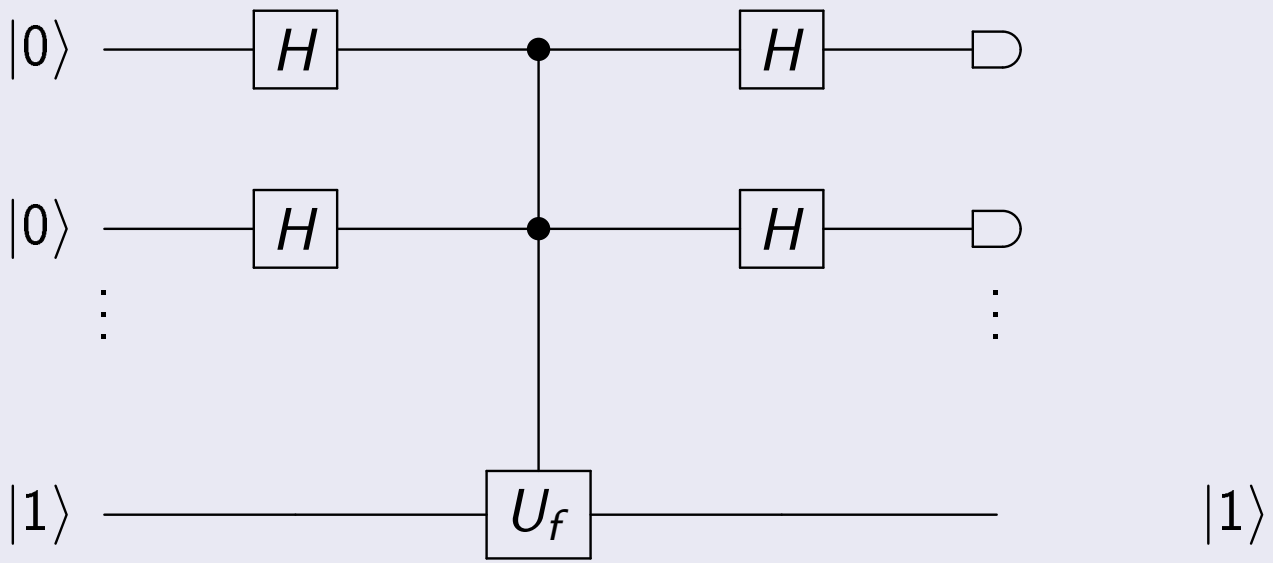
¿Es posible identificar **s** usando *una sola* consulta cuántica?

¡SI!!!

Algoritmo de Bernstein-Vazirani

¿Es posible identificar **s** usando *una sola* consulta cuántica?

- El circuito es el mismo que el del problema de Deutsch-Josza.



Problema recursivo de Bernstein-Varizani

- Un problema superpolinomial clásicamente.
- Cuánticamente se resuelve en n pasos, aplicando recursivamente n veces el algoritmo visto antes.

Nivel 1: Encontrar alguna función $g : \{0,1\}^n \to \{0,1\}$ sobre $\mathbf{s}$, $g(\mathbf{s})$.

- Es fácil de calcular teniendo $\mathbf{s}$.
- Si tenemos acceso al oráculo $f_s(\mathbf{x}) = \mathbf{x}.\mathbf{s}$.
- Encontramos $\mathbf{s}$ y luego $g(\mathbf{s})$

Problema recursivo de Bernstein-Varizani

Nivel 2: Encontrar alguna función $g : \{0,1\}^n \to \{0,1\}$ sobre $\mathbf{s}$, $g(\mathbf{s})$.

- No tenemos acceso al oráculo $f_s(\mathbf{x}) = \mathbf{x}.\mathbf{s}$.
- Tenemos dos cadenas de n bits: $\mathbf{x} \in \{0,1\}^n$ y $\mathbf{y} \in \{0,1\}^n$.
- La función que buscamos: $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ y está dada por $f(\mathbf{x},\mathbf{y}) = \mathbf{s}_x.\mathbf{y}$.
  - $\mathbf{s}_x$ representa 2^n cadenas diferentes de bits que satisfacen $g(\mathbf{s}_x) = \mathbf{s}.\mathbf{x}$ para algún $\mathbf{s}$.

Éste fue el primer problema en el que se encontró una separación super-polinomial entre los algoritmos clásicos (BPP) y cuánticos(BQP).

Algoritmos de aceleración super-polinomial

Estimación Cuántica de Fase

Algoritmos de aceleración Super-polinomial

- Todos estos algoritmos hacen uso de la Transformada Cuántica de Fourier **QFT**.
- La *estimación cuántica de la fase* es importante porque conduce naturalmente a la **QFT**.
- Ej. Algoritmo de Shor

Estimación Cuántica de Fase

Compuerta de Hadamard

- En el algoritmo de Deutsch como en el de Deutsch-Jozsa era usada para obtener información codificada en las fases de los estados.
- Recordemos:

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

La compuerta de Hadamard es auto-inversa:

$$H\frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) = |x\rangle$$

Estimación Cuántica de Fase

La fase es un número complejo

En general es de la forma $e^{2\pi i\omega}$, con $\omega \in (0,1)$ número real.

Problema de Estimación de Fase

- Tenemos el estado $\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i\omega y}|y\rangle$.
- El objetivo es estimar la fase ω.
  - $\omega = 0.x_1x_2x_3\ldots$ lo que significa

$$x_1 \cdot 2^{-1} + x_2 \cdot 2^{-2} + x_3 \cdot 2^{-3} + \ldots.$$

Estimación Cuántica de Fase

La fase es un número complejo

Similarmente

$$2^k\omega = x_1x_2x_3\ldots x_k.x_{k+1}x_{k+2}\ldots$$

y como $e^{2\pi ik} = 1$ para k entero, se tiene

$$e^{2\pi i2^k(\omega)} = e^{2\pi i(0.x_{k+1}x_{k+2}\ldots)}.$$

Estimación Cuántica de Fase

El caso más sencillo: 1-qubit de entrada y $\omega = 0.x_1$

El estado será:

$$\begin{aligned}
\frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{2\pi i(0.x_1)y}|y\rangle &= \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{2\pi i(\frac{x_1}{2})y}|y\rangle \\
&= \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{\pi i(x_1 y)}|y\rangle \\
&= \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{x_1 y}|y\rangle \\
&= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)
\end{aligned}$$

Podemos usar la compuerta de Hadamard de 1-qubit para determinar x_1 y por lo tanto ω.

$$H\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x}|1\rangle) = |x\rangle$$

Estimación Cuántica de Fase

Una identidad muy útil

$$\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle =$$

$$= \frac{1}{2^{n/2}} (|0\rangle + e^{2\pi i (2^{n-1}\omega)} |1\rangle) \otimes (|0\rangle + e^{2\pi i (2^{n-2}\omega)} |1\rangle) \otimes \ldots$$
$$\otimes (|0\rangle + e^{2\pi i (\omega)} |1\rangle)$$

$$= \frac{1}{2^{n/2}} (|0\rangle + e^{2\pi i (0.x_n)} |1\rangle) \otimes (|0\rangle + e^{2\pi i (0.x_{n-1}x_n)} |1\rangle) \otimes \ldots$$
$$\ldots \otimes (|0\rangle + e^{2\pi i (0.x_1 x_2 \ldots x_n)} |1\rangle)$$

Estimación Cuántica de Fase

Ejercicio: Demuestre la Identidad anterior Rta:

$$\frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle =$$
$$\frac{1}{2^{n/2}} \sum_{y_1=0}^{1} \cdots \sum_{y_n=0}^{1} e^{2\pi i \omega (\sum_{l=1}^{n} y_l 2^{-l})} |y_1 \ldots y_n\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{y_1=0}^{1} \cdots \sum_{y_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i \omega y_l 2^{-l}} |y_l\rangle$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{y_l=0}^{1} e^{2\pi i \omega y_l 2^{-l}} |y_l\rangle\right] = \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i \omega 2^{-l}} |1\rangle\right]$$

$$= \frac{1}{2^{n/2}} (|0\rangle + e^{2\pi i (0.x_n)} |1\rangle) \otimes (|0\rangle + e^{2\pi i (0.x_{n-1} x_n)} |1\rangle) \otimes \ldots$$
$$\cdots \otimes (|0\rangle + e^{2\pi i (0.x_1 x_2 \ldots x_n)} |1\rangle)$$

Estimación Cuántica de Fase

El estado de 2-qubits

- $\frac{1}{\sqrt{2^2}} \sum_{y=0}^{2^2-1} e^{2\pi i \omega y} |y\rangle$
  - $\omega = 0.x_1 x_2$
- Usando la identidad anterior

$$\frac{1}{\sqrt{2^2}} \sum_{y=0}^{2^2-1} e^{2\pi i (0.x_1 x_2) y} |y\rangle =$$

$$\frac{1}{2}(|0\rangle + e^{2\pi i (0.x_2)}|1\rangle) \otimes (|0\rangle + e^{2\pi i (0.x_1 x_2)}|1\rangle).$$

- x_2 se puede determinar del primer qubit usando una compuerta de Hadamard.
- Pero $x1$...

Estimación Cuántica de Fase

Determinación de $x1$

Consideraciones:

- Si $x_2 = 0 \Rightarrow \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(0.x_1)}|1\rangle)$
- Pero si $x_2 = 1$...

Operador rotación de fase de 1-qubit R_2

$$R_2 = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i(0,01)} \end{bmatrix},$$

- 0,01 en el exponente está escrito en base 2 o sea que es 2^{-2}

Estimación Cuántica de Fase

Determinación de $x1$

La inversa de R_2 es

$$R_2^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & e^{-2\pi i(0,01)} \end{bmatrix}.$$

- Si $x_2 = 1$ y aplicamos R_2^{-1} al segundo bit:

$$\begin{aligned} R_2^{-1}\left(\frac{|0\rangle + e^{2\pi i(0.x_1 1)}|1\rangle}{\sqrt{2}}\right) &= \frac{|0\rangle + e^{2\pi i(0.x_1 1 - 0,01)}|1\rangle}{\sqrt{2}} \\ &= \frac{|0\rangle + e^{2\pi i(0.x_1)}|1\rangle}{\sqrt{2}}. \end{aligned}$$

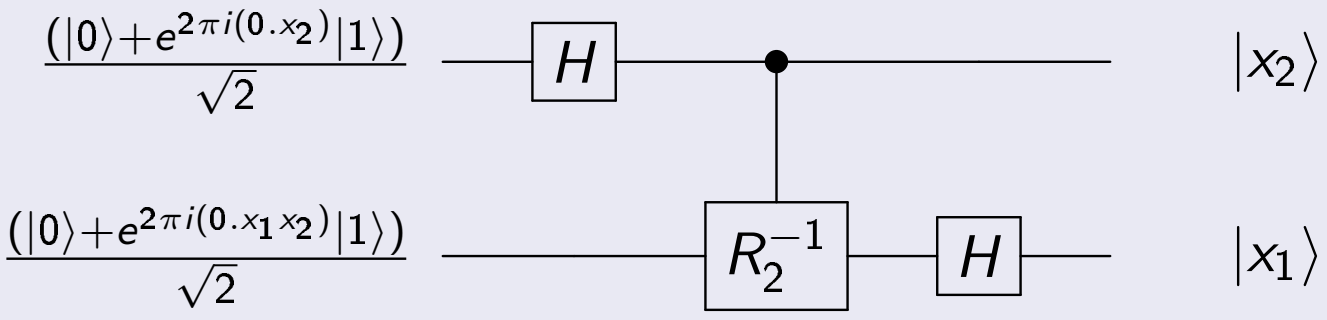
- Después de aplicar R_2^{-1} se puede obtener x_1 con una compuerta de Hadamard.

Estimación Cuántica de Fase

compuerta controlada R_2^{-1}

- Sólo es necesario aplicar R_2^{-1} si $x_2 = 1$

Estimación de Fase para un estado de 2-qubits con $\omega = 0.x_1x_2$.



Estimación Cuántica de Fase

Estimación de Fase para un estado de 3-qubits con $\omega = 0.x_1x_2x_3$

De acuerdo al desarrollo demostrado antes este estado se puede expresar como:

$$\left(\frac{(|0\rangle + e^{2\pi i(0.x_3)}|1\rangle)}{\sqrt{2}}\right) \otimes \left(\frac{(|0\rangle + e^{2\pi i(0.x_2x_3)}|1\rangle)}{\sqrt{2}}\right) \otimes \left(\frac{(|0\rangle + e^{2\pi i(0.x_1x_2x_3)}|1\rangle)}{\sqrt{2}}\right).$$

Definimos una compuerta general de rotación de fase de 1-qubit R_k

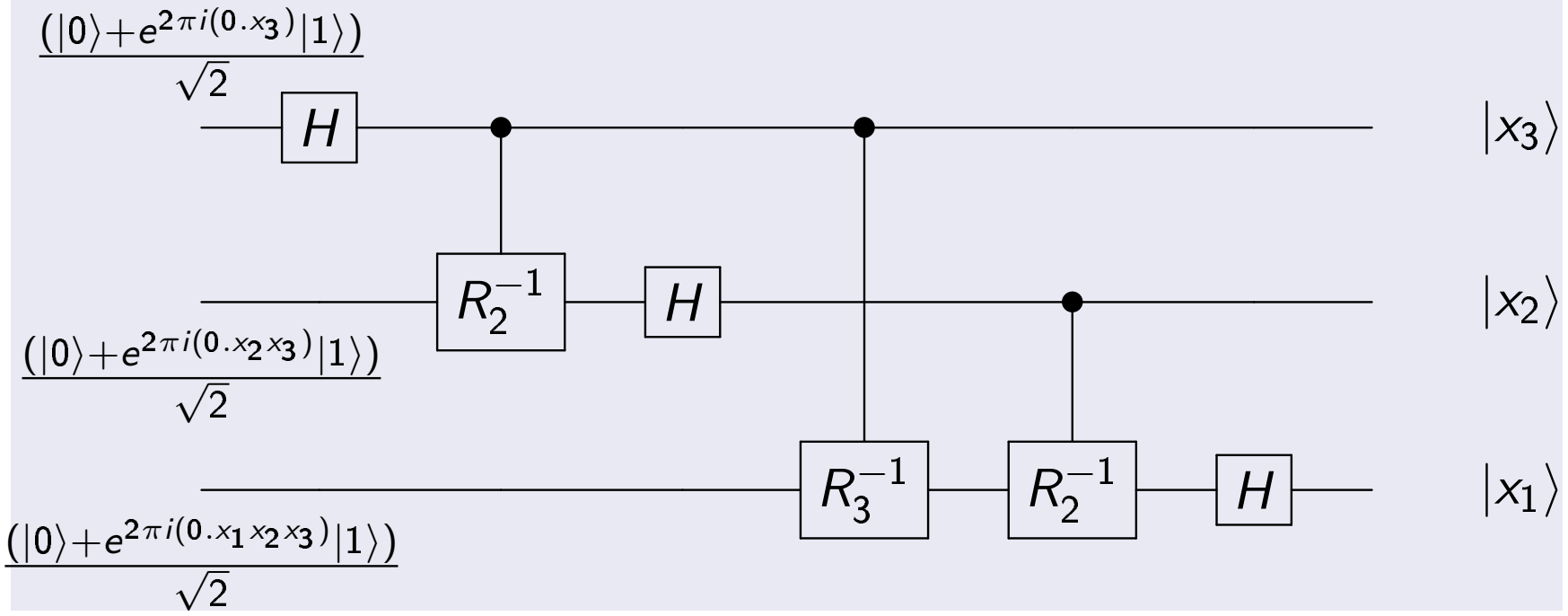
$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i(0,0\ldots1)} \end{bmatrix},$$

donde el 1 en el exponente está en la posición k.

Estimación Cuántica de Fase

Aplicamos R_3^{-1} y R_2^{-1} para obtener x_1.

El circuito:



Estimación Cuántica de Fase

Últimas consideraciones

- Vimos estimación de fase para $\omega = 0.x_1 x_2 \ldots x_n$ o, dicho de otra forma, cuando ω es de la forma $\frac{x}{2^n}$ para algún entero n.
- Para ω arbitrario se usa el mismo circuito de estimación de fase que resultará en una **aproximación** x tal que $\frac{x}{2^n}$ es cercano a ω con alta probabilidad dada por n.
- El circuito que estima una fase de la forma $0.x_1 x_2 \ldots x_n$ realiza la transformación

$$\frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x}{2^n} y} |y\rangle \rightarrow |x\rangle.$$

  - siendo la salida el estado $|x\rangle = |x_n \ldots x_2 x_1\rangle$

Estimación Cuántica de Fase

Transformada cuántica de Fourier

- La inversa de esta transformación es:

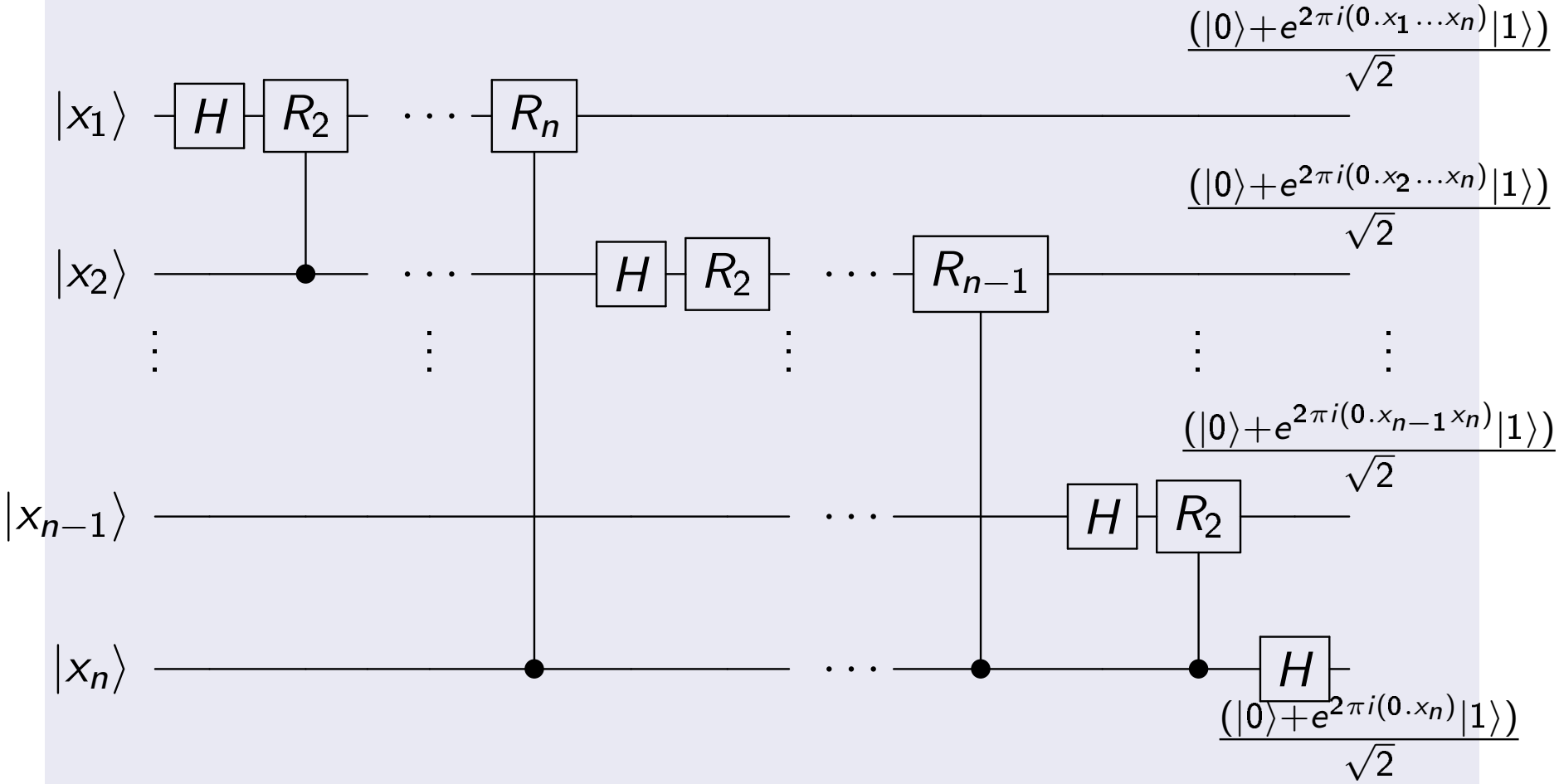
$$|x\rangle \rightarrow \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x}{2^n} y} |y\rangle.$$

- Esta transformación se llama *Transformada Cuántica de Fourier* (QFT_{2^n}) o directamente *QFT*

Es importante señalar que la QFT_{2^n} se realiza simplemente aplicando el circuito de estimación de fase a la inversa (orden y compuertas inversas)

Transformada cuántica de Fourier

Circuito



Transformada cuántica de Fourier

Estados Periódicos

- Una superposición de estados periódicos es de la forma:

$$|\phi_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} |zr + b\rangle.$$

- Decimos que este estado es periódico con *período* r, *desplazamiento* b y m repeticiones del período.

Transformada cuántica de Fourier

Problema: Hallar el Período r de un Estado Periódico, Dado mr

Entrada:

- Entero mr
- Oráculo generador de estados cuánticos

$$|\phi_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} |zr + b\rangle,$$

- donde $b \in \{0, 1, \ldots, r-1\}$ es elegido aleatoriamente con distribución uniforme.

Transformada cuántica de Fourier: Estados Periódicos

Problema: Encontrar r.

- ¿Qué sucede Si se mide directamente $|\phi_{r,b}\rangle$ en la base computacional?
- $P(x \in \{0, 1, \ldots, mr-1\}) = \frac{1}{mr}$

En cambio si usamos QFT^{-1} a $|\phi_{r,b}\rangle$ se obtiene:

$$QFT_{mr}^{-1}|\phi_{r,b}\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i \frac{b}{r} k} |mk\rangle$$

- Medimos este estado y obtenemos un valor $x = mk$ con k entre 0 y $r-1$.
- Sabemos mr, entonces podemos calcular $\frac{x}{mr} = \frac{k}{r}$.

Transformada cuántica de Fourier: Estados Periódicos

Expresando $\frac{x}{mr}$ como fracción reducida podemos obtener r.

Tenemos un problem si k y r tienen algún factor común

- El denominador no será r sino algún divisor de r.
- Ejemplo: Supongamos $m = 3, r = 20, x = 24$.
  Inicialmente conocemos $mr = 60$ y midiendo $QFT_{60}^{-1}|\phi_{r,b}\rangle$ nos dió el número $x = 24$
  - $\frac{24}{60} = \frac{8}{20}$ y $k = 8$
  - Al reducir la fracción obtendremos $\frac{24}{60} = \frac{2}{5}$
  - Perdimos el factor 4 porque es también factor de 24

Transformada cuántica de Fourier: Estados Periódicos

Para resolver este problema

1. Se repite el procedimiento para obtener dos resultados x_1 y x_2, que cumplen $\frac{x_1}{mr} = \frac{k_1}{r}$ y $\frac{x_2}{mr} = \frac{k_2}{r}$, con k_1 y k_2 enteros entre 0 y $r-1$.
2. Por medio del *Algoritmo Extendido de Euclides* se puede encontrar los enteros c_1, c_2, r_1, r_2 tal que $MCD(c_1, r_1) = MCD(c_2, r_2) = 1$ y $\frac{k_1}{r} = \frac{c_1}{r_1}$ y $\frac{k_2}{r} = \frac{c_2}{r_2}$.

Ésto significa que r_1 y r_2 son divisores de r, o sea que es múltiplo común de r_1 y r_2. De hecho, es el mínimo común múltiplo de ambos con probabilidad $\frac{6}{\pi^2}$.

Transformada cuántica de Fourier: Otras aplicaciones

- Estimación de autovalores
- Logaritmo discreto
- Encontrar orden
- Factorización