Algoritmos Cuánticos:

- The Deutsch Algorithm:

  Este algoritmo se basa en la Transformada Cuántica de Fourier, así mismo, ilustra las ideas clave del paralelismo e interferencia cuántica que se usan en todos los algoritmos útiles [An Introduction to Quantum Computing]. Por otro lado este es el primer algoritmo que explota el paralelismo cuántico utilizando solo 2 qbits, dicho algoritmo ha inspirado la construcción de varios algoritmos cuánticos que son mucho más eficientes [Basic Quantum Algorithms ].

  El problema de Deutsch fue planteado en 1985, aun sin usar el modelo de circuito cuántico. Una generalización del algoritmo de Deutsch es el algoritmo de Deutsch-Jozsa [Basic Quantum Algorithms ] tiene exactamente la misma estructura que su versión anterior y al igual que con el algoritmo de Deutsch, tenemos un circuito reversible que implementa una función desconocida f, pero esta vez f es una función de cadenas de n bits a un solo bit[An Introduction to Quantum Computing].

  en un recuadro encierras esto:
  El problema de Deutsch
  Entrada: una caja negra para calcular una función desconocida función $f : \{0, 1\} \rightarrow \{0, 1\}$.
  Problema: Determinar el valor de $f(0) \oplus f(1)$ haciendo consultas a f

  Supongamos que se tiene un circuito reversible para calcular una función desconocida de 1 bit $f:\{0,1\} \rightarrow \{0,1\}$: Tratamos al circuito reversible como una caja negra, esto quiere decir que al aplicar el circuito para obtener valores de f(x) para x entradas, no se obtendrá ninguna información del funcionamiento interno del circuito para aprender sobre la función f. Clásicamente el número de consultas que realiza para determinar $f(0) \oplus f(1)$ es 2 [An Introduction to Quantum Computing].

An Introduction to Quantum Computing
- introduction to quantum algorithm

```
@incollection{AnIntroductiontoQuantumComputing1,
   author = {Kaye, Phillip and Laflamme, Raymond and Mosca, Michele},
   title = "{Introductory Quantum Algorithms}",
   booktitle = "{An Introduction to Quantum Computing}",
   pages = {94}
   publisher = {Oxford University Press},
   year = {2006},
   month = {11}
```

Basic Quantum Algorithms

```
@incollection{BasicQuantumAlgorithms,
   author = {Renato Portugal},
   title = "{Deutsch's Algorithm}",
   booktitle = "{Basic Quantum Algorithms}",
   pages = {26}
   publisher = {National Laboratory of Scientific Computing LNCC/MCTI},
   year = {2022},
   month = {09}
```

- Quantum Transform Fourier:

  La transformada de Fourier convierte una función en el dominio del tiempo en las frecuencias que la componen en el dominio de la frecuencia, transformando una lista de muestras de funciones espaciadas uniformemente en una lista de coeficientes para una secuencia finita de sinusoides complejos, ordenados por frecuencia. En computación cuántica, la QFT es el análogo cuántico de la DFT. El QFT se puede realizar de manera eficiente en una computadora cuántica utilizando exponencialmente menos puertas de las que se requieren para calcular clásicamente. En QIP ( procesamiento de información cuántica), la QFT es una generalización de la transformada de Hadamard y ambas son bastante similares, con la excepción de que la QFT introduce una fase [A quantum Fourier transform (QFT) based note detection algorithm].

  En el procesamiento de información cuántica (QIP), la transformada cuántica de Fourier (QFT) tiene una gran cantidad de aplicaciones: el algoritmo de Shor y la estimación de fase son solo algunos ejemplos bien conocidos. El algoritmo de factorización cuántica de Shor, uno de los algoritmos cuánticos más citados, se basa en gran medida en la QFT y encuentra eficientemente factores primos enteros de grandes números en computadoras cuánticas [A quantum Fourier transform (QFT) based note detection algorithm. ].

  A quantum Fourier transform (QFT) based note detection algorithm:

```
@article{AquantumFouriertransform(QFT)basednotedetectionalgorithm,
author = { Shlomo Kashani, Maryam Alqasemi, Jacob Hammond},
year = {2022},
month = {04},
pages = {4-8},
title = {A quantum Fourier transform (QFT) based note detection algorithm},
}
```

- Grover Algorithm:

  Este algoritmo cántico brinda una aceleración polinomial sobre los algoritmos clásicos más conocidos para solucionar muchos problemas importantes .  Este algoritmo de búsqueda cuántica realiza una búsqueda genérica, por ejemplo, dado

un entero grande N, se puede reconocer eficientemente si un entero p es un factor no trivial de N. La búsqueda cuántica es una herramienta para acelerar este tipo de búsquedas genéricas[An Introduction to Quantum Computing].

El problema de búsqueda
Entrada: Una caja negra Uf para calcular una función desconocida f : {0, 1}n → {0, 1}.
Problema: Encuentra una entrada x ∈ {0, 1}n tal que f(x)=1

Si la función f sólo se proporciona como una caja negra, entonces son necesarias Ω(√2^n) aplicaciones de la caja negra para resolver el problema de búsqueda con alta probabilidad para cualquier entrada. Por lo tanto, los algoritmos cuánticos pueden proporcionar, como máximo, una aceleración cuadrática sobre la búsqueda exhaustiva clásica.  El algoritmo de Grover realiza la búsqueda cuadráticamente más rápido de lo que se puede hacer de forma clásica. Si hay exactamente una solución, una búsqueda de fuerza bruta determinista clásica toma 2^n − 1 consultas en el peor de los casos. De hecho, cualquier algoritmo clásico, que para cualquier función encuentra una solución con una probabilidad de al menos 2/3 , debe realizar consultas Ω(2^n) en el peor de los casos. El algoritmo de búsqueda cuántica de Grover solo toma O(√2^n) = O(2^n/2) consultas [An Introduction to Quantum Computing].

En particular, el algoritmo de Grover proporciona una aceleración cuadrática en la solución de problemas NP-completos , que explican muchos de los problemas difíciles importantes en informática [An Introduction to Quantum Computing]. Por otro lado, el poder de los algoritmos cuánticos, tal como lo descubrió Lov Grover, es que N/2 se puede mejorar a O(N1/2). En comparación con un algoritmo clásico de búsqueda aleatoria, el factor 1/2 entra en el exponente, lo que es una gran mejora. Ahora explicaremos cómo y por qué funciona el algoritmo [QUANTUM ALGORITHMS VIA LINEAR ALGEBRA].

An Introduction to Quantum Computing

```
@article{AnIntroductiontoQuantumComputing2,
   author = {Kaye, Phillip and Laflamme, Raymond and Mosca, Michele},
   title = "{ALGORITHMS BASED ON AMPLITUDE AMPLIFICATION}",
   booktitle = "{An Introduction to Quantum Computing}",
   pages = {152-163},
   publisher = {Oxford University Press},
   year = {2006},
   month = {11}
}
```

QUANTUM ALGORITHMS VIA LINEAR ALGEBRA

```
@INBOOK{QuantumAgorithmsviaLinearAlgebraGrover,
  author={Lipton, Richard J. and Regan, Kenneth W.},
  booktitle={Quantum Algorithms via Linear Algebra: A Primer},
```

```
  title={Grover's Algorithm},
  year={2014},
  volume={},
  number={},
  pages={115-128}
}
```

- Shor’s Algorithm:

El algoritmo de Shor se presentó en 1994 en una conferencia, este describe dos algoritmos cuánticos para la factorización de enteros y logaritmos discretos que se ejecutan en tiempo polinomial. Shor explota no solo el paralelismo cuántico sino también el entrelazamiento [Basic Quantum Algorithms].

a) Idea general:

En el algoritmo de factorización de Shor (SFA), el objetivo es encontrar un factor no trivial de un número entero compuesto N. Dicho brevemente, SFA funciona de la siguiente manera. Elige aleatoriamente un número entero y < N y comprueba si y y N son coprimos. Si y es coprimo con N, entonces SFA ejecuta una subrutina cuántica especial para obtener el orden 2r de N con cierta probabilidad (2r es aquí un número entero). En el SFA original y en todos los SFA anteriores, si 2r era un número entero par y y^r ≡ −1(mod N), entonces SFA usa y y 2r para obtener un factor no trivial de N. Sin embargo, si el resultado r obtenido por la subrutina de búsqueda de orden cuántico no era 2r, o 2r no era un número entero par, o y^r ≡ −1 (mod N), entonces la subrutina cuántica tendría que ejecutarse nuevamente [Reversibility and Universality].

b) Explicación detallada del algoritmo Shor [Probabilistic and]:

– Elige un número d con factores primos pequeños tal que 2n^2 ≤ d ≤ 3n^2.
– Elija un número entero aleatorio x que sea coprimo de n.
– Repita los siguientes pasos, registre d veces usando la misma x cada vez:
  – Cree un registro de memoria cuántica de 2d enteros no negativos módulo n y divídelo en dos mitades llamadas reg1 y reg2. Para el estado de todo el registro escribimos el vector ket |reg1,reg2](quantum symbol).
  –

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a, 0\rangle.$$

  – Realice la transformación x → x^a(mod.n) (usando paralelismo cuántico) en cada número (no normalizado) en reg1 y coloque los resultados en los lugares correspondientes en reg2. Denote por r el

período de la transformación anterior. Entonces el estado del registro completo (normalizado) se vuelve

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a, x^a (mod.n)\rangle.$$

– Medir el contenido de reg2 mediante el operador hermitiano A. Entonces esto colapsa a algún k y tiene el efecto de proyectar el estado de reg1 para que sea una superposición de exactamente aquellos valores de a para los cuales x^a = k(mod.n). Por tanto, el estado del registro completo es

$$|\psi\rangle = \frac{1}{\#M} \sum_{a' \in M} |a', k\rangle,$$

$$\text{where } M := \{a' : x^{a'} = k(mod.n)\}.$$

– Calcule la transformada de Fourier discreta (rápida) del estado proyectado en reg1 y devuelva este resultado a reg1. Esto mapea el estado proyectado en reg1 en una superposición

$$|\psi\rangle = \frac{1}{\#M} \sum_{a' \in M} \frac{1}{\sqrt{d}} \sum_{h=0}^{d-1} e^{2\pi i a' h/d} |h, k\rangle.$$

– Ahora, la transformada de Fourier en reg1 es una función periódica con un pico en múltiplos del período inverso 1/r. Los estados correspondientes a múltiplos enteros de 1/r y los cercanos a ellos aparecen con mayores amplitudes de probabilidad que los que no corresponden a múltiplos enteros del periodo inverso. Entonces, en cada paso, obtenemos un número h' tal que h'/d está cerca del múltiplo λ/r del período inverso del mapa exponencial para algún λ ∈ IN. Para estimar λ, se puede calcular la expansión de fracción continua de h'/d siempre que el denominador sea menor que n y luego retener la fracción más cercana como λ/r . Si esto se hace con suficiente frecuencia, tenemos suficientes muestras de λ_i que conducen a una conjetura del verdadero λ y, por lo tanto, de r.

– Ahora que conocemos r, podemos determinar los factores de n con alta probabilidad[Probabilistic and].

Observamos que, por supuesto (con una probabilidad bastante baja), el algoritmo de Shor puede fallar. Tales contraejemplos se construyen fácilmente. Pero representan casos bastante atípicos. Además, en lugar de utilizar la transformada clásica (rápida) de Fourier, también hay algoritmos cuánticos para la transformada de Fourier, que hacen que el algoritmo de Shor funcione aún más rápido en la práctica, pero no hasta el punto de mejorar el orden lineal de complejidad [Probabilistic and].

Basic Quantum Algorithms

@article{BasicQuantumAlgorithmsShor,
author = {Renato Portugal},
title = "{Shor’s Algorithm for Factoring Integers }",
booktitle = "{Basic Quantum Algorithms}",
pages = {56-74},
publisher = {National Laboratory of Scientific Computing LNCC/MCTI},
year = {2022},
month = {09}
}

Reversibility and Universality

@Inbook{ProbabilisticandStatisticalShor,
author="Xu, Guoliang
and Qiu, Daowen
and Zou, Xiangfu
and Gruska, Jozef",
editor="Adamatzky, Andrew",
title="Improving the Success Probability for Shor's Factorization Algorithm",
bookTitle="Reversibility and Universality: Essays Presented to Kenichi Morita on the Occasion of his 70th Birthday",
year="2018",
publisher="Springer International Publishing",
address="Cham",
pages="447--462",
}

Probabilistic and

@Inbook{ReversalyShor,
author="Neuenschwander, Daniel",
title="3 Factorization with Quantum Computers: Shor's Algorithm",
bookTitle="Probabilistic and Statistical Methods in Cryptology: An Introduction by Selected Topics",
year="2004",
publisher="Springer Berlin Heidelberg",
address="Berlin, Heidelberg",
pages="37--45",
}