



facultade de
informática
da coruña



UNIVERSIDADE DA CORUÑA

TRABAJO FIN DE GRADO
Grao en Enxeñaría Informática

ALUMNO/A: Rodrigo Arias Mallo

NIF: 47364718J

TELÉFONO:

EMAIL: rodrigo.arias@udc.es

DIRECTOR/A: Vicente Moret Bonillo

EMAIL: vicente.moret@udc.es

Entidad a la que pertenece (departamento de la UDC / empresa): Computación

TÍTULO DEL PROYECTO:

Deseño, desenvolvemento, implementación e proba dun simulador cuántico para o algoritmo de Simon.

Diseño, desarrollo, implementación y prueba de un simulador cuántico para el algoritmo de Simon.

Design, development, implementation and testing of a quantum simulator for Simon's algorithm.

Firmado:

El Director/a/es del proyecto

El Alumno/a

Tipo

Proyecto de desarrollo en investigación

BREVE DESCRIPCIÓN

En teoría de complejidad computacional e informática cuántica, el problema de Simon es un problema computacional del modelo de complejidad de árboles de decisión o complejidad de consulta.

Simon propuso un algoritmo cuántico que soluciona el problema exponencialmente más rápido que cualquier algoritmo clásico determinista o probabilístico. El algoritmo de Simon realiza $O(n)$ consultas a una caja negra, mientras que el mejor algoritmo probabilista clásico necesariamente necesita al menos $2^{(n/2)}$ consultas. El algoritmo de Simon es óptimo en el sentido que cualquier algoritmo cuántico para solucionar este problema requiere n consultas. Este problema supone una separación de un “oráculo” entre BPP y BQP, a diferencia de la proporcionada por el algoritmo de Deutsch-Jozsa, que separa P y EQP. Este algoritmo fue propuesto por Daniel Simon en 1994.

OBJETIVOS CONCRETOS

Implementar y validar un simulador del algoritmo de Simon mediante el cual el estudiante aplique la metodología y los conceptos propios del nuevo paradigma de la computación cuántica, en un caso real.

MATERIAL Y MEDIOS NECESARIOS

- Bibliografía
- Herramienta con un lenguaje de alto nivel y un entorno interactivo para el cálculo numérico, la visualización y la programación. Por ejemplo, mediante MATLAB o Python, es posible analizar datos, desarrollar algoritmos y crear modelos o aplicaciones.

FASES PRINCIPALES DEL TRABAJO

- Implementar la arquitectura que propone Simon para resolver el problema.
- Aplicar los operadores de Hadamard al primer registro.
- Aplicar la función definida por Simon.
- Ahora añadimos un paso que no es necesario pero sí es muy útil desde el punto de vista pedagógico. Se trata de medir el segundo registro y obtener uno de los posibles valores de la función, digamos $f(x_0)$, quedando el estado colapsado.
- Aplicar de nuevo Hadamard sobre los primeros qubits.
- Medir el primer registro con diferentes casos de prueba.
- Repitiendo estos pasos del orden de n veces obtenemos n vectores y_i que nos darán un sistema lineal homogéneo de ecuaciones cuya solución no trivial nos dará las componentes deseadas.

MÉTODO DE TRABAJO

Se trata de encontrar el período de una función vectorial booleana del tipo:

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

Se puede probar que de nuevo clásicamente habría que evaluar f sobre la mitad más uno de los elementos del dominio $2^{(n-1)+1}$, es decir, el coste sería exponencial. Incluso con un algoritmo probabilista no podríamos ir más allá de las $2^{(n/2)}$ consultas. Veremos que en este caso la ganancia cuántica es clara ya que bastará evaluar U_f unas pocas veces, del orden de n , para encontrar el período con una buena cota de aproximación.

SR. PRESIDENTE DE LA COMISIÓN DE ANTEPROYECTOS DE Grao en Enxeñaría Informática