Implementación del algoritmo de Grover utilizando un modelo de computación cuántico discreto.

L. Gatti[1], A. Fonseca de Oliveira[2], E. Buksman[1], J. García-López

Introducción

Los estados resultantes de la aplicación del algoritmo de Grover son un subconjunto de estados que se enmarcan dentro de un modelo de computación cuántica discreto. Estudiando este modelo es posible extraer algunas conclusiones del conocido algoritmo.

Modelo de computación cuántica discreta.

En [1] se presenta un modelo de computación cuántica discreta que permite mantener las principales fortalezas de la computación cuántica: la superposición y el entrelazamiento. El conjunto E (de estados discretos) consiste en todos los estados que se pueden obtener utilizando únicamente el conjunto C de compuertas cuánticas X_i (negación), H_i (Hadamard), V_i (fase $V|0\rangle = |0\rangle$ y $V|1\rangle = i|1\rangle$), $C_{i,j}$ (CNOT) y $T_{i,j,k}$ (Toffoli) partiendo de la base computacional.

Este conjunto, para sistemas de más de 2 qubits $(n_q \geq 3)$, es denso en la esfera unitaria y permite interpretarlo como la acumulación de distintos grados de refinamiento F_k :

$$F_k = \left\{ \varphi \in \mathrm{H}^{2^n} : \left(\sqrt{2}\right)^k \varphi \in (\mathrm{Z}[i])^{2^n} \text{ y } \left(\sqrt{2}\right)^{k-2} \varphi \notin (\mathrm{Z}[i])^{2^n} \right\} \quad \text{y} \quad E_K = \bigcup_{k=0}^{K} F_k \tag{1}$$

donde H^{2^n} nota al espacio de Hilbert correspondiente a un sistema de n qubits y $(\mathrm{Z}[i])^{2^n}$ a un vector complejo 2^n dimensional cuya parte real e imaginaria tienen todas sus entradas enteras.

Se prueba que F_k es un conjunto finito de estados, con $F_k \cap F_{k'} = \varnothing$ si $k \neq k'$. Por tanto $E_{k_1} \subset E_{k_2}$ (estrictamente) si $k_1 < k_2$ y $E = \lim_{K \to \infty} E_K$.

De los trabajos [2] y [3] se deduce que el conjunto de compuertas C es estrictamente universal para las matrices unitarias actuando sobre estados de $n_q \geq 3$ qubits.

Algoritmo de búsqueda Grover.

Este algoritmo [4] emplea como estado inicial la superposición uniforme de todos los $N = 2^{n_q}$ elementos de la base computacional al que llamaremos $|s\rangle$. El objetivo del algoritmo es encontrar alguno de los N estados de la base al que llamaremos $|t\rangle$. Para esto aplica sucesivamente el operador $O = 2|t\rangle\langle t| - I_d$ y el operador $G = 2|s\rangle\langle s| - I_d$.

El operador O (ó G) tiene como vector propio al vector $|t\rangle$ (ó $|s\rangle$) asociado al valor propio 1. El resto de los valores propios son -1 y corresponden a una base de vectores ortogonales a $|t\rangle$

(ó a $|s\rangle$). Por tanto el operador de Grover $U_G = G.O$ no es más que una reflexión sobre el sub-espacio generado por $|t\rangle$ y $|s\rangle$. Luego de aplicar $\Theta\left\lfloor\sqrt{N}\right\rfloor$ pasos se obtiene un estado muy cercano a $|t\rangle$.

Algoritmo de Grover sobre el conjunto discreto *E*

En el caso de las compuertas utilizadas en el algoritmo de Grover, se prueba que estas se pueden construir sin error utilizando únicamente una cantidad polinómica, en la cantidad de qubits, de compuertas del conjunto C y una cantidad lineal de ancillas. Por tanto los estados resultantes de la evolución de estados en el algoritmo son estados del conjunto E.

Este resultado permite re-interpretar los resultados del algoritmo en función del modelo de computación de cuántica discreta. La cantidad de pasos que se da en el algoritmo está directamente relacionada con el nivel de refinamiento F_k que se alcanza en los estados. Asumiendo un sistema de n_q, por cada aplicación del operador de Grover, si el estado inicial está en el nivel F_k, el estado resultante estará en el nivel F_{k+2n_q-4}. Una aplicación de Grover aumenta el refinamiento del modelo discreto una cantidad $2n_q - 4$. Como se muestra en la figura 1, k crece linealmente con la cantidad de iteraciones.

Por otro lado, es interesante analizar qué pasa cuando se toma la cantidad de iteraciones óptima de Grover, $p_o = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$. Para p_o iteraciones el nivel de refinamiento varía según la cantidad de qubits que se utilice. De hecho se puede obtener de forma exacta como $k = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor (2n_q - 4) + n_q$. Resultado que se ilustra en la figura 2.

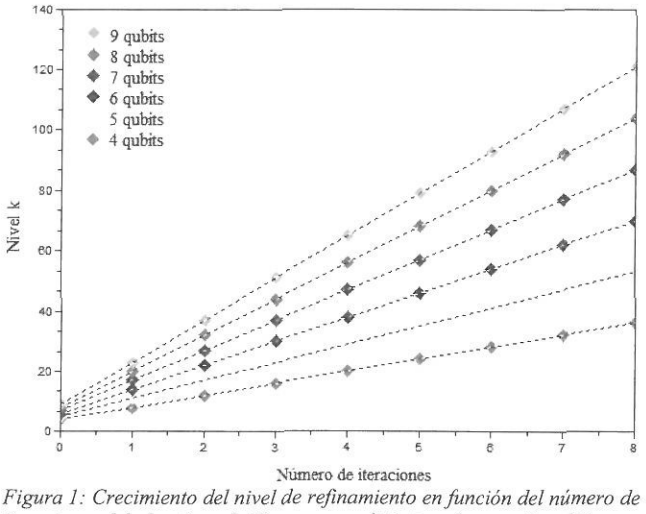

Figura 1: Crecimiento del nivel de refinamiento en función del número de iteraciones del algoritmo de Grover para distintos números de qubits.

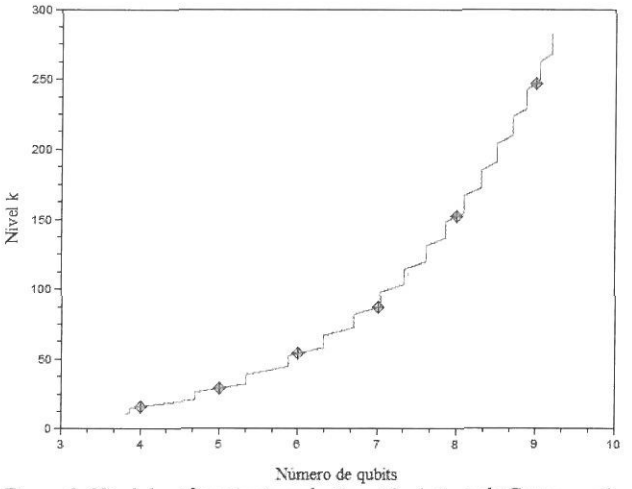

Figura 2: Nivel de refinamiento en la iteración óptima de Grover según la cantidad de qubits utilizados.

Referencias

[1] J. J. Carreño y J. García-López, CONJUNTOS DE ESTADOS PARA COMPUTACIÓN CUÁNTICA DISCRETA, XXXI Reunión Bienal de La Real Sociedad Española de Física, pág. 291, 2007, Granada.

[2] D.Aharanov, *"A Simple Proof that Toffoli and Hadamard are Quantum Universal"*, arXiv:quant-ph/0301040, (2003).

[3]Y Shi, *Quantum Information & Computation* **3**(1): 84-92 (2003)

[4] L.K. Grover, Proceedings, "A fast quantum mechanical algorithm for database search", *28th Annual ACM Symposium on the Theory of Computing*, (1996), 212.