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

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

1 Facultad de Ingeniería, Universidad ORT Uruguay, Montevideo, Uruguay.

2 ETSI de Sistemas Informáticos, UPM, Madrid, España.

*lgatti@uni.ort.edu.uy

## Introducción

■ En el marco de la computación cuántica el algoritmo de Grover es uno de los algoritmos de busqueda más importante. Permite encontrar, con alta probabilidad, un elemento en una secuencia no ordenada de $N$ datos en un tiempo $O(\sqrt{N})$.

■ En este trabajo se muestra que 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 presentado en [1] que se explicará brevemente. Estudiando este modelo es posible tener interesantes conclusiones del ya conocido algoritmo.

## Modelo discreto

El modelo de computación cuántica discreta sobre el que se trabaja está construido a partir de los estados que lo conforman. Para un sistema de $n$ qubits ($n_q$) el conjunto de estados discretos $E$ se obtiene operando los estados de la base computacional utilizando únicamente el conjunto de compuertas $C = \{X_j; V_j; H_j; C_{j,k}; T_{j,k,l}\}$ tantas veces como se desee.

**Propiedades:**

Si se definen los conjuntos $F_k$ y $E_k$:

$$F_k = \left\{\psi \in \mathcal{H}^{2^n} | (\sqrt{2})^k \psi \in (\mathbb{Z}[i])^{2^n} \text{ y } (\sqrt{2})^{k-2}\psi \notin (\mathbb{Z}[i])^{2^n}\right\}$$

$$E_k = \bigcup_{0 \le j \le k} F_j$$

donde $(\mathbb{Z}[i])^{2^n}$ es un vector de entradas complejas $2^{n_q}$ dimensional cuya parte real e imaginaria son números enteros.

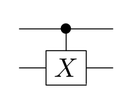
Se prueba que:

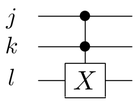
1. $F_k$ es finito y no vacío para todo $k \geq 0$,
2. $F_k$ y $F'_k$ son disjuntos si $k \neq k'$,
3. El conjunto de estados discretos $E$ es el límite de $E_k$ cuando $k \to \infty$, esto es: $E = \bigcup_{j=0}^{\infty} F_j$.

Estados de partida (Base computacional):
$\{|0\rangle, |1\rangle, ..., |2^{n_q} - 1\rangle\}$
Compuertas de un qubit:

$$V_l : \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad X_l : \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad H_l : \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Compuertas controladas:

$C_{j,k}$ : 


$T_{j,k,l}$ : 

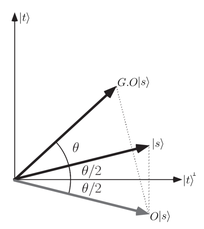

$\forall\, j,k,l$ entre 1 y $n_q$

- Las propiedades anteriores permiten interpretar al conjunto de estados $E$ como la acumulación de distintos niveles de discretización representados por $E_k$.
- De los resultados de [2] y [3] se tiene que el conjunto de compuertas $C$ es un conjunto universal, o sea, es capaz de aproximar cualquier operador unitario con un error arbitrario.

## Algoritmo de Grover

- El objetivo del algoritmo [4] es encontrar uno estado marcado ($|t\rangle$) en un conjunto desordenado, representado por un elemento de la base canónica.
- 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 algoritmo se basa en aplicar 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 $|s\rangle$ ).

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 $\Theta = \lfloor\sqrt{N}\rfloor$ 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, 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 son estados del conjunto $E$.
Este resultado permite interpretar el algoritmo en función del modelo de computación de cuántica discreta. La cantidad de pasos que se da en el algoritmo está directamente relacionado con el nivel de discretización $F_k$ que se alcanza en los estados.

Asumiendo un sistema de $n_q$, si el estado inicial está en el nivel $F_k$, por cada aplicación del operador de Grover el estado resultante estará en el nivel $F_{x+2n_q-4}$. Una aplicación de Grover aumenta la discretización del modelo en 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 estudiar qué pasa cuando se toma la cantidad de iteraciones óptima de Grover, $p_0 = \lfloor\frac{\pi}{4}\sqrt{N}\rfloor_q$. Para $p_0$ iteraciones el nivel de discretización varía según la cantidad de qubits que se utilice. De hecho se puede obtener de forma exacta como $k = \lfloor\frac{\pi}{4}\sqrt{N}\rfloor(2n_q - 4) = n$. El resultado se ilustra en la figura 2.

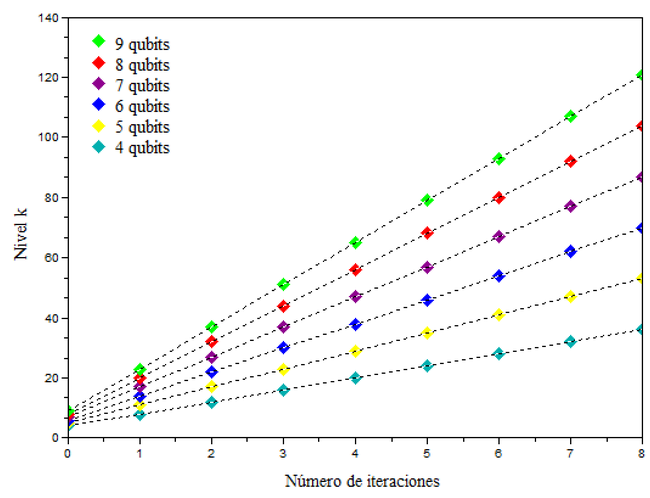



Fig. 1: Crecimiento del nivel de discretización en función del número de iteraciones del algoritmo de Grover para distintos números de qubits.

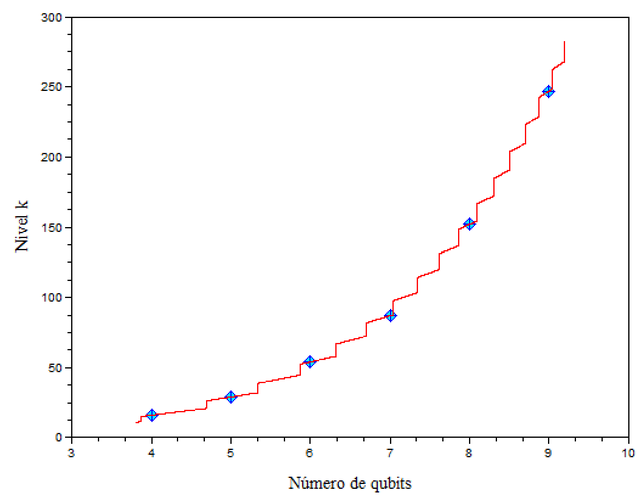



Fig. 2: Nivel de discretización en la iteración óptima de Grover según la cantidad de qubits utilizados.

## 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, 291 (2007).
[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, 212 (1996).

**XXXV** REUNIÓN BIENAL DE LA REAL SOCIEDAD ESPAÑOLA DE FÍSICA, 13-17 Julio 2015, Gijón, España