Cien Textos Científicos www.revista-nanociencia.ece.buap.mx ISSN 0188-6150

Inter*net* Electronic Journal
Nanociencia et Moletrónica

Octubre 2004, Vol. 2; N°2, págs. 274-281 (2004)

Álgebra en el diseño del algoritmo de búsqueda cuántico

C. Bautista

Facultad de Ciencias de la Computación
Benemérita Universidad Autónoma de Puebla
14 Sur y Av. San Claudio, Edif.. 135, Ciudad Universitaria
Puebla, Pue. 72570 México
e-mail: bautista@cs.buap.mx

recibido: agosto 2004 revisado: agosto 2004 publicado: octubre 2004

Citation of the article:
C. Bautista **"**Álgebra en el diseño del algoritmo de búsqueda cuántico". Internet Electrón. J. Nanocs. Moletrón. 2004, 2(2), 274-281:

http://www.revista-nanociencia.ece.buap.mx

Álgebra en el diseño del algoritmo de búsqueda cuántico

C. Bautista

Facultad de Ciencias de la Computación
Benemérita Universidad Autónoma de Puebla
14 Sur y Av. San Claudio, Edif.. 135, Ciudad Universitaria
Puebla, Pue. 72570 México
e-mail: bautista@cs.buap.mx

recibido: agosto 2004 revisado: agosto 2004 publicado: octubre 2004

Internet Electron. J. Nanocs. Moletrón. 2004, 2(2), pags. 274-281

Resumen Se examina el algoritmo de Grover desde el punto de vista de la teoría de grupos.

Palabras clave Computación cuántica, algoritmo de Grover, órbitas de grupos, G-conjuntos, representaciones de grupos.

1. **Introducción**

La búsqueda de varios artículos en una base de datos no estructurada se puede efectuar en una computadora cuántica con el llamado *algoritmo de Grover* [1]. Tal algoritmo ofrece una mejora cuadrática en comparación con los algoritmos de búsqueda clásicos.

El análisis usual del algoritmo de Grover se hace basado en un hecho bien conocido de la geometría plana elemental: el producto de dos reflexiones es una rotación. Sin embargo, en el presente trabajo, mostramos que el algoritmo de Grover admite un análisis puramente algebraico que usa la teoría de grupos estándar [2]. Desde éste punto de vista, la compuerta cuántica llamada matriz de *difusión*, toma la forma de la proyección canónica por promedio, que es una de las herramientas más comunes y particularmente útil en el estudio de la teoría de representaciones de grupos finitos. Por lo tanto, se revela que el algoritmo de Grover está construido alrededor de un proyector particular. Tal observación podría ser útil para el diseño de nuevos algoritmos cuánticos de búsqueda.

2. **Planteamiento del problema**

De aquí en adelante supondremos que el lector está familiarizado con las nociones elementales de la computación cuántica [2] y de la teoría de grupos [3].

El problema que nos proponemos resolver es el siguiente:

Dados: un grupo G, un subgrupo H, un G-conjunto X donde H actúa por restricción.

Compromiso: existen exactamente t elementos en la órbita, relativa al subgrupo H, de un elemento k_0 en X que podemos distinguir.

Problema: encontrar un elemento de la órbita de k_0 relativa a H.

3. **Superposiciones y el teorema órbita-estabilizador**

La base teórica de la solución del problema es lo que se conoce, en teoría de grupos, como el teorema órbita-estabilizador, que enseguida enunciamos usando la notación ket para denotar a los elementos de X. Además, en general, denotamos con $|B|$ a la cardinalidad del conjunto B.

Teorema 1 Sea $|j\rangle \in X$, $H_j = \{h \in H \mid h|j\rangle = |j\rangle\}$ el estabilizador de $|j\rangle$ y j^H la órbita de del mismo $|j\rangle$ bajo H. Entonces

$$|j^H| = \frac{|H|}{|H_j|} .$$

Se puede mostrar entonces, la siguiente igualdad en C^X (espacio vectorial complejo con base X) que

$$\sum_{h\in H} h|j\rangle = |H_j\| j^H\rangle$$

donde $|j^H\rangle = \sum_{x\in j^H} |x\rangle$. En consecuencia,

$$\sum_{g\in G} g|j^H\rangle = \frac{|H\|G_j|}{|H_j|}|j^G\rangle \quad . \qquad (2)$$

Nótese que en vista de que queremos encontrar la órbita de un elemento, es natural que aparezca la transformación $\sum_{h\in H} h$. Sin embargo ésta no es unitaria, peor aún, no es, en general invertible. Tal problema puede superarse si recordamos la serie geométrica $1/(1-z) = \sum_{n=0}^{\infty} z^n$, es decir, salvo algún radio de convergencia, los elementos $1-z$ son invertibles. Usamos tal idea para z el promedio de los elementos de H: $P = \sum_{g\in G} g/|G|$. De que $P^2 = P$ se sigue que, para $c \in C$ (C el campo complejo),

$$Id - cP \text{ es unitaria} \Leftrightarrow |1-c| = 1$$

donde Id es la transformación identidad.

Gracias a la ecuación (2) es posible encontrar un subespacio invariante bajo $Id - cP$. Definimos el subespacio $W_j = C\left| j^H \right\rangle + C\left|\Delta_j\right\rangle$, donde $\left|\Delta_j\right\rangle = \left| j^G \right\rangle - \left| j^H \right\rangle$. Cálculos directos muestran que

Teorema 2 Para $c \in C$ definimos $D(c) = Id - cP$. Si $\left| j^H \right\rangle \neq \left| j^G \right\rangle$ entonces el siguiente diagrama conmuta

$$\begin{array}{ccc} W_j & \xrightarrow{D(c)} & W_j \\ T\downarrow & & \downarrow T \\ C^2 & \xrightarrow[M]{} & C^2 \end{array}$$

donde $\left| j^H \right\rangle \xrightarrow{T} |0\rangle$, $\left|\Delta_j\right\rangle \xrightarrow{T} |1\rangle$,

$$M = \begin{pmatrix} 1-cq & c \\ cq & c(q-1)+1 \end{pmatrix}$$

y $q = \left|j^H\right| / \left|j^G\right|$. Además, si $\left| j^H \right\rangle = \left| j^G \right\rangle$ entonces $D(c)\big|_{W_j}$ es una homotecia (múltiplo de Id).

La forma de marcar (reconocer) los elementos buscados es con la matriz unitaria $U_{k_0}{}^{\theta}$ definida por

$$U_{k_0}{}^{\theta}\left| j\right\rangle = \begin{cases} e^{i\theta}\left| j\right\rangle, & si \quad j \in k_0{}^H \\ \left| j\right\rangle, & otro \quad caso \end{cases}$$

Ésta matriz es un ejemplo de lo que se conoce como oráculo (cuántico). El análisis que haremos del algoritmo que presentamos se hará en base al número de llamadas que se haga a tal oráculo.

También el siguiente diagrama conmuta

$$\begin{array}{ccccc} W_j & \xrightarrow{U_{k_0}{}^{\theta}} & W_j & \xrightarrow{D(1-e^{i\theta})} & W_j \\ T\downarrow & & T\downarrow & & \downarrow T \\ C^2 & \xrightarrow[M']{} & C^2 & \xrightarrow[M]{} & C^2 \\ T'\downarrow & & & & \downarrow T' \\ C^2 & & \xrightarrow{-R} & & C^2 \end{array}$$

donde

$$M'=\begin{pmatrix} e^{i\theta} & 0 \\ 0 & 1 \end{pmatrix} \qquad T'=\begin{pmatrix} \sqrt{Nq} & 0 \\ 0 & \sqrt{N(1-q)} \end{pmatrix} \qquad N=2^n=|X|$$

y

$$R=\begin{pmatrix} (e^{i\theta}-1)q-e^{i\theta} & (1-e^{-i\theta})\sqrt{1-q}\sqrt{q} \\ (e^{i\theta}-1)\sqrt{q}\sqrt{1-q} & (e^{-i\theta}-1)q-e^{-i\theta} \end{pmatrix}.$$

Es realmente notable que R resulte una matriz en $SU(2)$ el grupo lineal especial de matrices 2×2 y que en particular cuando se pone $\theta=\pi$, la matriz R sea una matriz de rotación. Aún más, si se restringen coeficientes al campo real **R** se obtiene que el siguiente diagrama conmuta:

$$\begin{array}{ccccccc} W_j & \xrightarrow{T'T} & C & \xrightarrow{-i} & C & \xrightarrow{*} & C \\ D(2)U_{k_0}{}^{\pi}\downarrow & & & & & & \downarrow -e^{i\alpha} \\ W_j & \xrightarrow[T'T]{} & C & \xrightarrow[*]{} & C & \xrightarrow[i]{} & C \end{array} \qquad (3)$$

donde $R=e^{i\alpha}$, $\alpha=\arccos(1-2q)$ y además $C\xrightarrow{i}C$, $C\xrightarrow{-i}C$, $C\xrightarrow{-e^{i\alpha}}C$ son las multiplicaciones por i, $-i$, $-e^{i\alpha}$ respectivamente; mientras que $C\xrightarrow{*}C$ es la conjugación compleja.

4. **El algoritmo**

Que al diagrama anterior conmute significa que la transformación unitaria $D(2)U_{k_0}{}^{\pi}$ es, salvo un cambio de base una rotación. Ahora la idea es rotar varias veces hasta obtener probabilidad máxima en el estado que marca a los elementos buscados. Tal número de rotaciones resulta ser $r=\mathbf{round}\left(\pi/(2\alpha)-1/2\right)$, como explicaremos más abajo.

El siguiente es el algoritmo que resuelve el problema planteado, cuando la cardinalidad de X es una potencia de 2: $|X| = 2^n$. Denotamos con H la matriz de Hadamard de orden 2×2.

qSearch (G, H)
1. $|\xi_0\rangle = |0 \ldots 0\rangle$
2. $|\xi_1\rangle = H^{\otimes n} |\xi_0\rangle$
3. **for** $i = 1$ **to** r
4. $\quad |\xi_1\rangle = U_{k_0}{}^{\pi} |\xi_1\rangle$
5. $\quad |\xi_1\rangle = D(2) |\xi_1\rangle$
6. $|\xi_1\rangle =$ **measurement** $|\xi_1\rangle$
7. **if** $|\xi_2\rangle \neq |k_0\rangle$ **then** repetir la secuencia anterior
8. $\quad$ **else return** $|k_0\rangle$

donde la medición se hace con respecto a la base del cálculo.

5. **Análisis del algoritmo**

El análisis de tal algoritmo es el siguiente. Supóngase que $i_1{}^G, \ldots, i_l{}^G$ corresponden a las diferentes órbitas en X. Entonces la primera evolución en la línea 2 del algoritmo **qSearch** es

$$|\xi_1\rangle = \frac{1}{\sqrt{N}} \left(|i_1{}^H\rangle + |\Delta_1\rangle + \cdots + |i_l{}^H\rangle + |\Delta_l\rangle \right).$$

Debido a que el diagrama (3) conmuta se obtiene que

$$\left(D(2)U_{k_0}{}^{\pi}\right)^r \left(|k_0{}^H\rangle + |\Delta_{k_0}\rangle \right) = (-1)^r \frac{\sin(r+1/2)\alpha}{\sqrt{Nq}} |k_0{}^H\rangle + (-1)^r \frac{\cos(r+1/2)\alpha}{\sqrt{N(1-q)}} |\Delta_{k_0}\rangle .$$

Después del ciclo **for** se obtiene que $(r+1/2)\alpha \approx \pi/2$, por lo que el coeficiente (amplitud) de $|k_0{}^H\rangle$ es máximo. Es entonces que la probabilidad de obtener $|k_0{}^H\rangle$ en la línea 9 de **qSearch** es $|k_0{}^H\rangle/(Nq)$. Por lo que tenemos que la repetición de la secuencia se hace, en promedio, $Nq/\left\| k_0{}^H \right\rangle|$-veces.

Resulta entonces que el número de veces que se consulta al oráculo $U_{k_0}{}^{\pi}$ es $Nqr/\left|k_0{}^{H}\right| \in O(N/(\sqrt{\left|k_0{}^{H}\right|}\sqrt{\left|k_0{}^{H}\right|}))$.

Se puede mostrar que para $G = S_N$ el grupo simétrico de orden $N!$ y $H = \langle \rho \rangle$ el subgrupo generado por un ciclo ρ de orden t, **qSearch** $\left(S_N, \langle \rho \rangle\right)$ es el famoso algoritmo de Grover para la búsqueda de t elementos de entre $N = 2^n$.

6. **Sobre generalizaciones**

Se ha mostrado que el elemento central en el algoritmo de Grover es la proyección por promedio que hemos llamado P. Tal proyección es un caso particular de las proyecciones canónicas en las llamadas representaciones irreducibles de un grupo G. Éstas están definidas como

$$P_k = \frac{\chi_k(e)}{|G|} \sum_{g \in G} \chi_k{}^{*}(g) \quad g$$

para cada χ_k carácter irreducible de G (ver [4]). Nuestra P se obtiene del carácter trivial $\chi_0(g) \equiv 1$. La utilidad de los caracteres no triviales en el diseño de nuevos algoritmos de búsqueda es un asunto pendiente pero prometedor.

Por otra parte, que la base de datos X tenga tantos elementos como una potencia de 2 no es esencial. El uso de sistemas híbridos [5], con obvias modificaciones, nos permite usar el algoritmo **qSearch** sobre bases de datos con un número arbitrario de elementos.

7. **Conclusiones**

Una fuente de transformaciones unitarias es el conjunto de transformaciones idempotentes. Un ejemplo es la proyección por promedio que resulta del carácter trivial de un grupo. Tal proyección por promedio da lugar al famoso algoritmo de Grover.

En vista de que las representaciones irreducible de un grupo tienen asociadas proyecciones, nuestro punto de vista podría ser útil para el diseño de nuevos algoritmos de búsqueda que usen el conjunto de caracteres irreducible de un grupo.

Referencias

[1] L.K. Grover, "A fast quantum mechanical algorithm for database search", Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 212-219, 1996.
[2] J. J. Rotman, "An Introduction to the Theory of Groups", Springer-Verlag, Nueva York, 1995.

[3] M. A. Nielsen y I. L. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press, Cambridge, 2002.
[4] J. P. Serre, "Linear Representations of Finite Groups", Springer-Verlag, Nueva York, 1977.
[5] J. Daboul, X. Wang y B. C. Sanders, "Quantum gates on hybrid qudits", *J. Phys. A: Math. Gen.* **36** 2525-2536, 2003.