Inter*net* Electronic Journal*

Nanociencia et Moletrónica

Diciembre 2006, Vol. 4, N°3, 743-752

Transformaciones de Moebius en Búsquedas Cuánticas

C. Bautista Ramos

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

recibido:16 de Octubre 2006 revisado: 20 de Octubre 2006 publicado: 15 de Noviembre de 2006

Citation of the article:
Transformaciones de Moebius en Búsquedas Cuánticas, Internet Electrón. J. Nanocs. Moletrón. 2006, Vol. 4, N° 3., pp. 743-752

Transformaciones de Moebius en Búsquedas Cuánticas

C. Bautista Ramos

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

recibido:16 de Octubre 2006 revisado: 20 de Octubre 2006 publicado: 15 de Noviembre de 2006

Internet Electron. J. Nanoc. Moletrón. 2006, Vol. 4, No.3, pags.743-752

Resumen

Proponemos algoritmos para computadoras cuánticas que encuentren imágenes inversas de proyectores hermitianos. El análisis de tales algoritmos se hace mediante transformaciones de Moebius. En particular, proponemos un algoritmo cuántico para el caso de transformaciones de Moebius parabólicas con probabilidad acotada, que a diferencia del conocido algoritmo de Grover, conforme se hacen más iteraciones, el algoritmo obliga al estado inicial a aproximarse cada vez más a un estado que corresponde a un punto atractor de una transformación de Moebius de tipo parabólico.

1 Introducción

La búsqueda de información es una tarea común entre las computadoras. En el presente trabajo estamos interesados en algoritmos de búsqueda no para cualquier clase de computadora, sino para las llamadas computadoras *cuánticas* [1]. Las computadoras cuánticas aprovechan las leyes de la Física del micromundo (Mecánica Cuántica) para efectuar cálculos. En consecuencia los algoritmos *cuánticos* son diferentes, en principio, a los algoritmos clásicos, puesto que las leyes del micromundo (Mecánica Cuántica) son muy diferentes a las leyes del macromundo (Mécanica Clásica); que son las que usa la computación clásica. Por ejemplo, cada paso de computación cuántica tiene que ser reversible: esto es, de la salida se puede recuperar la entrada. Esto no es así en la computación clásica (considérese el producto de dos números, si la salida resulta 0, cuáles fueron los factores? Uno fué cero, claro; pero ¿y el otro?)

Se conocen algoritmos cuánticos que resuelven problemas más rápidamente que sus contrapartes clásicas. Los más célebres son el algortimo de Shor y el algoritmo de Grover [2]. El primero factoriza números enteros exponencialmente más rápido que cualquier algoritmo de factorización conocido hasta hoy para computadoras clásicas. Mientras que el algoritmo de Grover realiza búsquedas sobre bases de datos *sin estructura* cuadráticamente más rápido que cualquier algoritmo clásico diseñado para la misma tarea.

En contraste a las bases de datos sin estructura aparecen, en computación clásica, las bases de datos *estructuradas* cuyo modelo más común es llamado *relacional* (propuesto originalmente por Codd [3]). Las bases de datos estructurados son manipuladas por piezas de software conocidas como *sistemas gestores de bases de datos* que siguen ciertas reglas algebraicas conocidas como *álgebra relacional* [4]

Uno de los operadores de las álgebras relacionales es el llamado *operador de selección.* Como su nombre lo indica tal operador de selección se encarga de elegir, de la base de datos, la información deseada. Usando matemáticas la descripción de la tarea del operador de selección es más breve: lo que hace el operador de selección es encontrar la preimagen de un proyector. Por supuesto, para lograr tal tarea se necesita de un algoritmo. El operador de selección abstrae tal algoritmo, que debe de ser un algoritmo *clásico*, esto es, usa los conceptos de la computación clásica.

En el presente trabajo proponemos algoritmos *cuánticos* para resolver problemas de selección, es decir, para encontrar preimágenes de proyectores. La idea es generalizar el ya mencionado algoritmo de Grover haciendo uso de *puntos atractores* que aparecen en la llamada *linea proyectiva* relacionados a *transformaciones de Moebius* [5,6]

Resulta que la computación cuántica es más estructurada que la computación clásica: el estado de la computadora cuántica es un vector complejo, la forma de cambiar los estados es mediante la aplicación sucesiva de matrices unitarias y el cálculo se termina al aplicar una matriz que corresponde a una mediación (usualmente matrices de proyección). Las matrices forman lo que en Álgebra se conoce como un *grupo*, los vectores forman lo que en Análisis Matemático se llama *un espacio de Hilbert* y entonces podemos usar los resultados de tales áreas de las Matemáticas y tratar de interpretarlos en computación cuántica. En particular el algoritmo de Grover hace uso de espacios invariantes de dimensión 2, que es un plano complejo sobre el que actúan matrices de orden 2×2 . Luego se puede hacer uso del epimorfismo que existe de las matrices al grupo de las tranformaciones de Moebius [5,6] que en particular lleva el plano complejo al espacio proyectivo de dimensión 1.

Por lo tanto el análisis de nuestros algoritmos que proponemos aquí, se puede hacer mediante transformaciones de Moebius. Aprovechamos la bien conocida clasificación de tales transformaciones en *elípticas, parabólicas, hiperbólicas y loxodrómicas* y su relación con puntos atractores.

Recientemente, Grover *et al* [7,8] han propuesto algorimos cuánticos de búsqueda usando puntos fijos. Pero su análisis y la clase de búsquedas que él propone son diferentes a los del presente trabajo.

2 Definición del problema y primeros resultados

Esta sección definimos nuestro problema principal y establecemos nuestras suposiciones.

Dados: dado P un proyector hermitiano ($P^{\dagger}=P$, $P^2=P$ donde $P^{\dagger}$ es la matriz conjugada transpuesta de P) y un par de vectores ortogonales en la imagen de P : $|v_0\rangle \in \mathrm{Im}\ P$, $|v_1\rangle \in \mathrm{Im}\ P$ producidos por un algoritmo cuántico Q sin medición:

$$Q|0\rangle = |v_0\rangle + |v_1\rangle \in \mathrm{Im}\ P$$

donde la probabilidad de obtener $|v_0\rangle$ es $\langle v_0|v_0\rangle$.

Problema: encontrar una preimagen $|u\rangle$ de $|v_0\rangle$, esto es

$$P|u\rangle = |v_0\rangle$$

y además tal que

$$\langle u|v_0\rangle = q \quad \text{y} \quad \langle u|v_1\rangle = 0 \ .$$

Es natural tratar de usar la misma proyección P para resolver el problema. En computación cuántica sólo se permite usar matrices unitarias. En particular una matriz unitaria tiene que ser invertible. Una matriz invertible relacionada de manera cercana con P está dada por la serie geométrica

$$(Id - cP)^{-1} = \sum_{j=0}^{\infty} c^j P^j$$

donde el escalar complejo c ha sido introducido para controlar la convergencia de tal serie.

Es fácil mostrar que

$$Id - c\,P \quad \text{es unitaria si y sólo si} \quad |1-c| = 1 \ .$$

A las matrices de la forma $D(c) = Id - cP$ con $c \in \mathbb{C}$ tal que $|1-c| = 1$ les llamamos *matrices de difusión.* Si $P \neq Id$ entonces tales matrices de difusión tienen un subespacio invariante de dimensión 2. Para explicar cómo es ésto posible consideremos $|v\rangle$ el vector normalizado de $|v_0\rangle$. Entonces $P|u\rangle = \lambda|v\rangle$ donde λ es la norma de $|v_0\rangle$.

Tomemos ahora un par de números complejos x,y tales que $x/y = -\langle u|v\rangle$. Definimos

$$|\delta\rangle = x\,|u\rangle + y|v\rangle$$

y $|\Delta\rangle$ su vector normalizado. Entonces el subespacio $W = \mathbb{C}|u\rangle + \mathbb{C}|\Delta\rangle$ generado por $|u\rangle$ y $|\Delta\rangle$ es un subespacio invariante de $D(c)$. De hecho la representación matricial de la matriz de difusión $D(c)$ es

$$\begin{pmatrix} 1-c\,q & c\,\alpha(1-q) \\ -\lambda\, c/\beta & 1-c+c\,q \end{pmatrix}$$

donde $q = \lambda\langle u|v\rangle$ y $|\Delta\rangle = \alpha|u\rangle + \beta|\Delta\rangle$.

También el subespacio $\mathbb{C}|v_1\rangle$ es invariante de $D(c)$, de hecho si n es un entero no negativo entonces $D(c)^n|v_1\rangle = (1-c)^n|v_1\rangle$.

El marco teórico del cociente x/y es el siguiente: el espacio proyectivo complejo de dimensión 1 denotado $\mathbb{C}P^1$ es el conjunto $\mathbb{C}\times\mathbb{C} - (0,0)$ módulo la relación de equivalencia $(a,b) \sim (b,c)$ si y sólo si existe $\mu \in \mathbb{C}$ tal que $(a,b) = \mu(c,d)$. La clase de equivalencia de una pareja (a,b) se denota $[a:b]$. La función $X : \mathbb{C}P^1 \to \mathbb{C}\cup\{\infty\}$, $X[x:y] = x/y$ se llama coordenada afín. Luego $[x:y]$ *es un punto de la linea proyectiva con coordenada afín* $-\langle u|v\rangle$.

2 Oráculos cuánticos y transformaciones de Moebius

Un *oráculo cuántico* es una simplificación de un problema o mejor dicho, es la suposición de un algoritmo eficiente que resuelve un problema. En nuestro caso usaremos oráculos U_θ con $0<\theta<2\pi$ que son matrices unitarias que se comportan de la siguiente forma: $U_\theta|u\rangle=e^{i\theta}|u\rangle$, $U_\theta|\Delta\rangle=|\Delta\rangle$, $U_\theta|v_1\rangle=|v_1\rangle$. Como puede notarse la tarea del oráculo U_θ es marcar el estado buscado $|u\rangle$ con un cambio de fase por $e^{i\theta}$.

Un cálculo directo muestra que la representacion matricial de la restricción de la composición $D(1-e^{i\psi})\circ U_\theta$ al subspacio W es

$$R_{\theta,\psi}=\begin{pmatrix} q e^{i(\theta+\psi)}-q e^{i\theta}+e^{i\theta} & \alpha q e^{i\psi}-\alpha e^{i\psi}-\alpha q+\alpha \\ \frac{\lambda}{\beta}(e^{i(\theta+\psi)}-e^{i\theta}) & q-e^{i\psi}q+e^{i\psi} \end{pmatrix}$$

la cual tiene determinante $e^{i(\theta+\psi)}$.

El algoritmo cuántico que proponemos para resolver el problema planteando tiene la siguiente forma:

(1)

para algún $n\in\mathbb{N}$. Esto es, primero se aplica Q el algoritmo cuántico dado y entonces se itera un número n conviente de veces la transformación $D(1-e^{i\psi})\circ U_\theta$. En lo que sigue estableceremos cómo tomar los ángulos θ y ψ y además estimaremos n .

Según la discusión anterior, el análisis del algoritmo cuántico propuesto se reduce a estudiar las potencias de la matriz $R_{\theta,\psi}$. A su vez, podemos estudiar tales potencias mediante el morfismo de grupos canónico φ que existe entre Mob que es el grupo de las tranformaciones de Moebius y GL(2) el grupo lineal general:

$$\varphi: GL(2)\to Mob, \begin{pmatrix} a & b \\ c & d \end{pmatrix}\to \frac{az+b}{cz+d}$$

Tal morfismo transforma la valuación de matrices en vectores por la coordenada afín correspodiente. Formalmente si $p(a,b)=[a:b]$ entonces, el siguiente diagrama conmuta:

$$\begin{array}{ccccc} \mathbb{C}\times\mathbb{C}-\{(0,0)\} & \xrightarrow{p} & \mathbb{C}P^1 & \xrightarrow{X} & \mathbb{C}\cup\{\infty\} \\ M\downarrow & \nearrow & \downarrow & \nearrow & \downarrow\varphi(M) \\ \mathbb{C}\times\mathbb{C}-\{(0,0)\} & \xrightarrow{p} & \mathbb{C}P^1 & \xrightarrow{X} & \mathbb{C}\cup\{\infty\} \end{array}$$

donde X es la coordenada afín descrita anteriormente. Lo que implica, en nuestro caso que $(D(1-e^{i\psi})^{-1}\circ U_\theta)^n\circ U_\theta|0\rangle$ se convierte en $\varphi(R_{\theta,\psi})^n(-\alpha)$. Para estudiar éstas potencias

normalizamos la transformación de Moebius $\varphi(R_{\theta,\psi})^n$. Esto es, la dividimos por la raíz cuadrada de su determinante y resulta en

$$N_{\theta,\psi}=\frac{1}{e^{i(\theta+\psi)/2}}\varphi(R_{\theta,\psi})=\begin{pmatrix} f(\theta,\psi)+ig(\theta,\psi) & -2i\alpha e^{-i\theta/2}\sin\left(\frac{\psi}{2}\right) \\ 2i\frac{\lambda}{\beta}e^{i\theta/2}\sin\left(\frac{\psi}{2}\right) & f(\theta,\psi)-ig(\theta,\psi) \end{pmatrix}$$

donde

$$f(\theta,\psi)=q\cos\left(\frac{\theta+\psi}{2}\right)+(1-q)\cos\left(\frac{\theta-\psi}{2}\right)$$

y

$$g(\theta,\psi)=q\sin\left(\frac{\theta+\psi}{2}\right)+(1-q)\sin\left(\frac{\theta-\psi}{2}\right)$$

Las transformaciones de Moebius (normalizadas) se pueden clasificar según su traza [6]. La traza de $N_{\theta,\psi}$ nos dice qué clase de transformación es $\varphi(R_{\theta,\psi})$. El resultado lo formalizamos en el siguiente Teorema.

Teorema Sea $q=\lambda\langle u|v\rangle$ fijo.

1. Si $0<q<1$ entonces $\varphi(R_{\theta,\psi})$ es elíptica para cualesquiera $0<\theta<2\pi$, $0<\psi<2\pi$.
2. Si $q<0$ ó $q>1$ entonces existen ángulos $0<\theta_1,\theta_2,\theta_3<2\pi$, $0<\psi_1,\psi_2,\psi_2<2\pi$ tales que $\varphi(R_{\theta_1,\psi_1})$ es elíptica, $\varphi(R_{\theta_2,\psi_2})$ es parabólica y $\varphi(R_{\theta_3,\psi_3})$ es hiperbólica.
3. Si $q=0$ ó $q=1$ entonces existen ángulos $0<\theta_1,\theta_2<2\pi$, $0<\psi_1,\psi_2<2\pi$ tales que $\varphi(R_{\theta_1,\psi_1})$ es elíptica y $\varphi(R_{\theta_2,\psi_2})$ es parabólica.
4. Si $q\in\mathbb{C}-\mathbb{R}$ entonces $\varphi(R_{\theta,\psi})$ es loxodrómica para cualesquiera $0<\theta<2\pi$, $0<\psi<2\pi$.

Demostración. La traza de $\varphi(N_{\theta,\psi})$ es $2f(\theta,\psi)$. Luego si $q\in\mathbb{C}-\mathbb{R}$ entonces $f(\theta,\psi)\in\mathbb{C}-\mathbb{R}$ y así $\varphi(R_{\theta,\psi})$ es loxodrómica. Por otra parte si $q\in\mathbb{R}$ entonces podemos calcular los puntos críticos de $f(\theta,\psi)$ que se encuentran en el centro y las esquinas del cuadrado $0\leqslant\theta\leqslant2\pi, 0\leqslant\psi\leqslant2\pi$. En las esquinas f toma los valores 0, ±1 y en en centro tenemos que $f(\pi,\pi)=1-2q$.

Si $0<q<1$ entonces $|1-2q|<1$ lo que implica que los máximos y minimos de f se encuentran en las esquinas del cuadrado ya mencionado. Por lo tanto, para cualesquiera $0<\theta,\psi<2\pi$ se tiene que $-1<f(\theta,\psi)<1$ lo que implica que $\varphi(R_{\theta,\psi})$ es elíptica.

Los demás casos se examinan similarmente.

3 El caso parabólico

Por simplicidad sólo examinaremos el caso parabólico. Como veremos más abajo, en este caso el comportamiento de nuestro algoritmo cuántico es lineal. Sin embargo se puede mostrar que los casos loxodrómico y hiperbólico se tiene un comportamiento de avance exponencial.

El caso parabólico es posible debido a que para $q \leqslant 0$ las soluciones a la ecuación $f(\theta,\psi)=1$ estan dadas por

$$\sec\left(\frac{\theta}{2}\right)=\frac{-2\cos(\psi/2)\pm\sqrt{q(q-1)(1-2q)^2(\cos(2\psi)-4\cos(\psi)+3)/2}}{2(1-q)^2\sin^2(\psi/2)-2} \tag{2}$$

Supongamos que $Sz=(az+b)/(cz+d)$ es una transformación de Moebius parabólica y γ un punto fijo. Entonces, para

$$T=\begin{pmatrix} 0 & \frac{a-c\gamma}{c} \\ \frac{c}{a-c\gamma} & \frac{c\gamma}{c\gamma-a} \end{pmatrix}$$

obtenemos que $Sz=\varphi(T^{-1})\circ(z+1)\circ\varphi(T)$. De donde nuestro algoritmo cuántico (1) se transforma en

$$S^n(-\alpha)=\varphi(T^{-1})\circ(z+n)\circ\varphi(T)(-\alpha)$$

Luego si $n\to\infty$ entonces $S^n(-\alpha)\to\varphi(T^{-1})(\infty)=\gamma$. Este hecho nos dice cuál es el comportamiento del algoritmo cuántico dado en (1).

Teorema Sea $q \leqslant 0$. Si

$$\psi=2\arcsin\left(\frac{1}{2\sqrt{\langle u|v\rangle+1}}\right)$$

y θ satisface la ecuación (2) entonces, para $g=g(\theta,\psi)$ y

$$n\geqslant\lambda^{-2}\left(\frac{2}{|g|}+\frac{1}{||\alpha|-|g||}\right)$$

en el algoritmo cuántico (1), la probabilidad de obtener la preimagen $|u\rangle$ es, al menos,

$$\frac{\langle v_0|v_0\rangle}{\frac{2}{\lambda|g|}+1}$$

Agradecimientos

A la memoria de mi maestro Jesús García Fernández.

Referencias

[1] Nielsen, M. A; Chuang, I. L.: Quantum Computation and Quantum Information. Cambridge: Cambridge Univ. Press 2001
[2] Grover, L. K.: Quantum Mechanics helps in searching a needle in a haystack, Phys. Rev. Lett. 79, 325 (1997), quant-ph/9706033
[3] Codd, E. F.: A relational model of data for large shared data banks, Comm. ACM 13, 377 (1970)
[4] Abiteboul, S; Hull, R; Vianu, V: Foundations of Databases. Reading Mass: Addison-Wesley 1995
[5] Ahlfors, L. V: Complex Analysis. Tokyo: McGraw-Hill 1979
[6] Schwerdtfeger, Geometry of Complex Numbers. Nueva York: Dover 1979
[7] Grover, L.K; Patel, A; Tulsi, T: Quantum algorithms with fixed points: the case of database search, quant-ph/0603132
[8] Tulsi, T.; Grover, L. K.; Patel, P.: A new algorithm for fixed point quantum search, Quantum Computation and Information 6, 483 (2006) quant-ph/0505007.