BUSCA QUÂNTICA EM BANCOS DE DADOS XML USANDO ALGORITMO DE GROVER

PONTES, Michael Alexandre
Universidade Estadual Paulista (UNESP)
michaelpontes@terra.com.br

BORGES, Manoel Ferreira Neto
Universidade Estadual Paulista (UNESP)
borges@ibilce.unesp.br

RESUMO: Este artigo apresenta a implementação de um algoritmo de busca quântica com pequenas modificações. A idéia desse algoritmo é ser hibrido, podendo funcionar em sistemas clássicos e sistemas quânticos. São apresentados os conceitos quânticos das buscas e introduzido um pseudo-framework capaz de gerar códigos para computadores clássicos (C++) e computadores quânticos (QCL). Os algoritmos foram submetidos a simulações, que resultaram em um estudo comparativo do funcionamento do algoritmo de Grover em ambos os sistemas, realizando buscas em uma massa de dados em arquivos no formato XML. Como resultado, observa-se números muito parecidos entre sistemas clássicos e quânticos, isso gera uma expectativa de que a busca em computadores quânticos reais seja muito mais eficiente.
PALAVRAS-CHAVE: busca quântica, grover, QCL, emaranhamento, sobreposição.

ABSTRACT: *This paper presents a quantum search algorithm implementation with small modifications. The algorithm idea is to be hybrid, capable to run on classical systems and quantum systems. We present the concepts of quantum search and introduced a pseudo-framework able to generate code for classical computers (C++) and quantum computers (QCL). The algorithms were submitted to simulations, which resulted in a comparative study of the operation of Grover's algorithm on both systems, carrying out searches in a mass of data in XML format files. As a result, we see very similar numbers between classical and quantum systems, this creates an expectation that the search in real quantum computers is much more efficient.*
KEYWORDS: *quantum search, grover, qcl, entanglement, superposition.*

INTRODUÇÃO

Como todas as simples ideias na ciência, levou tempo para que se notasse a conexão entre os conceitos de computação e as características de sistemas físicos microscópicos, propriedades como emaranhamento e superposição coerentes de estados distintos estão presentes nos fundamentos da mecânica quântica e sempre foram considerados aspectos mais estranhos desta teoria (NIELSEN; CHUANG, 2005). O reconhecimento de que a informação, muito mais que um conceito matemático abstrato, é uma propriedade de sistemas físicos, levou a enormes avanços na interpretação da Mecânica Quântica.

Com a utilização da Computação Quântica, tempos impraticáveis necessários para executar certas tarefas na computação clássica, passam a ser tempos normais em computadores quânticos. Como afirma HAWKING, 2009, problemas praticamente insolúveis para computação clássica passam a ser solúveis em computação quântica.

Computadores quânticos oferecem computação mais poderosa (SIMON, 1994) do que os computadores clássicos, devido à capacidade dos computadores quânticos de terem alguns estados que não têm equivalência em um computador clássico. Características como a superposição de valores e/ou o emaranhamento de estados são aspectos que representam o "coração" do funcionamento de um sistema quântico. Isso tudo somado ao paralelismo quântico,

representa um diferencial considerável frente à computação que estamos habituados.

Visando contribuir com a área pouco explorada da Computação Quântica, este artigo propõe a implementação de um sistema híbrido de busca em bancos de dados não estruturados. Tal sistema visa realizar buscas clássicas e buscas quânticas, ambas baseadas no mesmo algoritmo de busca, o Algoritmo de Grover. Este algoritmo é conhecido na área quântica, porém sua implementação de forma híbrida é um desafio novo. A proposta de um mesmo engine capaz de realizar buscas em sistemas quânticos e clássicos é o que justifica e define a originalidade deste trabalho.

As buscas realizadas pelo algoritmo proposto poderão ser aplicadas em sistemas de computação clássica, computação quântica ou computação hibrida (SCHUBOTZ, 2007; ÖMER, 2000). Neste artigo, o algoritmo proposto utiliza um simulador quântico para testar os algoritmos em sistemas quânticos, e realiza as buscas em bancos de dados baseados em estruturas XML (eXtensible Markup Language).

1. COMPUTAÇÃO QUÂNTICA

Na computação clássica, a memória do computador é organizada em *bits*, onde cada *bit* representa um ou zero. Na computação quântica, por outro lado, existem alguns fenômenos da mecânica quântica, como superposição e emaranhamento de estados, que são utilizados para executar operações em dados (MUTIARA; REFIANTI, 1994).

Computadores Quânticos foram propostos no início dos anos 1980 (BENIOFF, 1980) e em muitos aspectos, mostraram-se tão poderosos quanto os computadores clássicos. A descrição formal dos computadores quânticos só foi realizada no final dos anos 80 e início dos anos 90 (DEUTSCH, 1985; BERTHIAUME; BRASSARD, 1994; BERNSTEIN; VAZIRANI, 1993; YAO, 1993) e os computadores quânticos, em vários problemas específicos, se mostraram mais poderosos que os computadores clássicos.

No início de 1994, (SHOR, 1994) demonstrou que um computador quântico poderia resolver de forma eficiente um problema bem conhecido, para o qual não havia algoritmo eficiente usando computadores clássicos. Este é o problema de fatoração, isto é, encontrando os fatores de um determinado número inteiro N, em um tempo que é polinomial em $logN$.

A pesquisa na área de computação e informação quântica ganhou um imenso interesse com os resultados apresentados para o problema de fatoração (SHOR, 1994). Na sequência, os algoritmos de busca (GROVER, 1996) também passaram a chamar bastante atenção para sua eficiência. Esses resultados comprovam o enorme poder computacional de uma máquina quântica. No entanto, a construção de computadores quânticos representa um imenso desafio tecnológico e, neste momento, o hardware quântico só está disponível em laboratórios de pesquisa. Diante desse cenário, os simuladores quânticos tornaram-se instrumentos valiosos no desenvolvimento e testes de algoritmos quânticos, bem como na simulação de modelos físicos (CARAIMAN; MANTA, 2010).

Um dos grandes atrativos na computação quântica é que no lugar de usar *bits*, são usados *qubits* (*bits* quânticos). Um único qubit pode representar um, zero, ou ambos ao mesmo tempo, o que é chamado de superposição. Com essa capacidade, a computação quântica pode realizar várias tarefas simultaneamente de forma mais rápida do que a computação clássica.

Há também outro fenômeno em computação quântica, que é chamado emaranhamento. Se dois qubits receberem uma força externa, então os qubits podem estar na condição de emaranhados. Isso significa que, mesmo à distância um do outro, qualquer influência que um dos qubits receber, irá afetar o outro também (MUTIARA; REFIANTI, 1994).

Sistemas de informação quântica, em geral, são baseados no uso de matemática intensa. Porém, o grande truque desses sistemas é a utilização de um modelo simples de construção por blocos de abstração: bits quânticos, portas e algoritmos (OSKIN; CHONG; CHUANG, 2002), o que facilita sua implementação.

Nessa pequema introdução sobre computação quântica, é possível perceber

a riqueza desse novo sistema de computação. A utilização de conceitos quânticos na computação ultrapassa fronteiras, oferecendo novas formas de processamento. Nas próximas sessões, será explorada algumas características dos sistemas quânticos, visando atingir o objetivo proposto por esse artigo.

2. Problema de busca

Encontrar um dado em um banco de dados não-estruturado é conhecido como problema de pesquisa em banco de dados não-ordenados (UDS – *unsorted database search*), este problema é muito comum e difícil de ser solucionado. Muitos problemas científicos podem ser reduzidos a problemas de UDS e esta tem larga aplicação em ciência e tecnologia (LONG; LIU, 2007; HU; ZHANG; LU, 2009).

Mesmo em ciência da computação teórica, são bastante comuns problemas em que seja necessário examinar uma série de possibilidades diferentes para ver se uma delas satisfaz dada condição. Esta situação é análoga ao problema de busca descrito acima, e o ponto de observação mais crítico em problemas de busca é sempre o desempenho e eficiência do algoritmo utilizado (GROVER, 1996).

2.1. Busca quântica

Os algoritmos quânticos são probabilísticos, isso oferece um ótimo ponto de partida para se pensar em suas possíveis aplicações (BERNSTEIN; VAZIRANI, 1993).

Nestes algoritmos, o sistema não está em um estado especificado, ao contrário disso, está em uma distribuição de vários estados com certa probabilidade de ser cada um deles. Em cada etapa, há uma probabilidade de acontecer uma transição de um estado para o outro. A evolução do sistema é obtida através da pré-multiplicação do vetor de probabilidades pelo estado de transição da matriz (GROVER, 1996).

Suponha que se tenha um mapa contendo muitas cidades, e que se deseje encontrar o menor caminho entre elas. Um algoritmo simples para resolver esse problema consiste em encontrar todas as rotas possíveis, mantendo gravada a de menor comprimento. Em um computador clássico, se existirem *N* rotas, serão obviamente necessárias $O(N)$ operações para se determinar o menor caminho (NIELSEN; CHUANG, 2005; LONG; LIU, 2007).

O algoritmo quântico de Grover aumenta significativamente a velocidade dessa busca, necessitando apenas de $O(\sqrt{N})$ operações. Além disso, o algoritmo quântico de busca é geral, no sentido de que ele pode ser aplicado para acelerar diversos algoritmos clássicos que usam rotinas de busca (GROVER, 1996).

Tais algoritmos representam papéis muito importantes nos campos da informação e computação. Tomando como exemplo a tarefa de encontrar o proprietário de um número telefônico decifrando um código como DES (BRASSARD, 1997), resolvendo o problema de Simon (BRASSARD; HOYER, 1997), solucionando o problema de contagem quântica (BRASSARD; HOYER; TAPP, 1998). O espaço pode ser vasculhado de forma altamente eficiente por um robô quântico usando o algoritmo de busca (BENIOFF, 2000). Esses algoritmos também podem acelerar a resolução de problemas de raiz quadradas considerados difíceis, como o problema do deslocamento oculto (TWAMLEY, 2000), o problema do circuito hamiltoniano (DESURVIRE, 2009) e problemas NP-completos em geral (GUO; LONG; LI, 2002).

O algoritmo de Grover, utilizando as propriedades quânticas da superposição e do emaranhamento, também pode ser usado para procurar um elemento em uma lista não estruturada de elementos N quadrática com velocidade superior aos algoritmos clássicos (BRICKMAN; et al, 2005).

3. Algoritmo de Grover

Na seção anterior, superposição e emaranhamento de estados quânticos foram apontados como os fatores essenciais para a obtenção do desempenho dos sistemas quânticos. O algoritmo de busca de Grover (BUGAJSKI, 2001; GROVER, 1996; KLAMKA, 2002) faz uso desses fenômenos. A complexidade da pesquisa clássica de uma coleção não ordenada de N itens é

de $O(N)$. Usando o algoritmo quântico, podemos reduzir esse fator para $O(\sqrt{N})$.

O algoritmo utiliza um quregister único de 2^n qubits, onde $2^n \geq N$. Para simplificar, assumimos que N é uma potência de 2 e $2^n = N$. Como segue:

1. No primeiro passo, uma superposição de todos estados é gerado.
2. Uma transformação é realizada para fazer com que a amplitude da probabilidade do estado se diferencie das outras (Oráculo Quântico).
3. Outra transformação (difusão) é realizada para ampliar a probabilidade deste estado.
4. Os passos (2) e (3) são iterados quantas vezes forem necessárias.
5. O algoritmo termina quanto a probabilidade do estado desejado está próxima de 1. Na sequência, uma medição é realizada.

A superposição é uma operação realizada através do operador quântico Hadamard, que resulta no mesmo valor para todas as amplitudes possíveis. Na Figura 1a está situação está representada por um registro de 4-*qubit*, que contém 16 valores diferentes. A soma dos quadrados de todas as amplitudes é 1, o valor de cada amplitude a_i é demonstrado na sequência em (1):

$$\forall i \in (0..N-1) \quad a_i := \frac{1}{\sqrt{N}} = \frac{1}{\sqrt{2^n}} = 2^{-n/2} \quad (1)$$

O Oráculo Quântico é o segundo passo do algoritmo, esse é o ponto em que o item procurado é identificado. O Oráculo decide se o argumento é o item que está sendo procurado, e é simultaneamente chamado para cada item presente na lista de estados. A operação tem que ser reversível, portanto nenhuma informação pode ser perdida. Isto é obtido através da negação da amplitude do item procurado (Figura 1b). Dado que x é o estado que está sendo pesquisado, temos em (2):

$$\forall i \in (0..N-1) \quad a_i := (i == x)? -a_i : a_i \quad (2)$$

A medida da amplitude é complexa, a operação de negação é descrita antes como a rotação do estado marcado por uma fase de π. De qualquer modo, esta operação não irá afetar a possibilidade de detecção deste estado em uma medição feita nesse ponto.

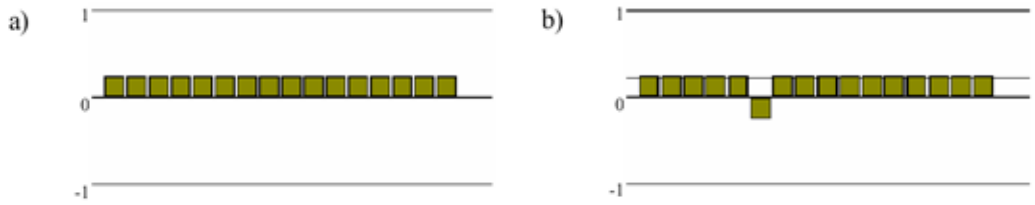

Figura 1: Etapas iniciais do Algoritmo de Grover.
Fonte: Adaptado de: FRANCIK, 2002.

O operador de difusão é o próximo passo do algoritmo, nessa etapa, é feita a operação de interferência. Esta operação é muitas vezes referenciada como inversão sobre a média, como é dado a seguir em (3):

$$\forall i \in (0..N-1) \quad a_i := -a_i + 2\bar{a} = -a_i + \frac{2}{N}\sum_{j=0}^{N-1} a_j \quad (3)$$

onde $\bar{a}$ é a média de todas as amplitudes. Esta operação é aplicada sobre um vetor no qual todos os componentes, exceto um, são iguais a um valor, como α; o componente *um*, que é diferente, é negativo (Figura 1b). A média $\bar{a}$ é aproximadamente igual a α, então $N-1$ componentes não alteram de forma significativa o resultado da inversão sobre a média. O componente *um*, que estava negativo, torna-se positivo e aumenta cerca de 2α (Figura 2c).

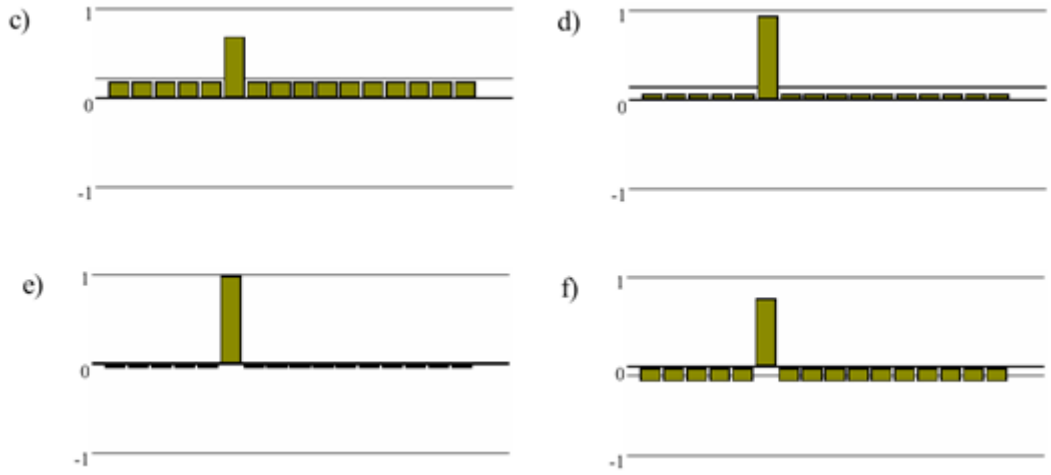

Figura 2: Iterações do Algoritmo de Grover.
Fonte: FRANCIK, 2002.

Iteração: o ganho efetivo obtido por uma inversão única sobre a média não é o suficiente, especialmente se for notado que mais estados possuem ganhos menores. Após certo número de iterações, possivelmente a amplitude se aproximará de 1.

Porém a amplitude nunca será igual a 1, pelo fato do algoritmo de Grover ser probabilístico: o resultado mais adequado é obtido com uma alta probabilidade, mas não é garantido totalmente.

Iterações consecutivas são mostradas da Figura 2c até Figura 2f. Na terceira iteração (Figura 2e) a amplitude do estado desejado atingiu o máximo (para o caso de 16 estados); após isso, diminui (Figura 2f). O valor do componente $N-1$, denotado α, lentamente diminui uma vez que se aproxima de zero, e o ganho efetivo inverte. Na verdade, ambos os valores são quantificados em uma função periódica (a amplitude desejada cresce novamente depois das iterações 9, 15 e assim por diante).

O problema é: quantas vezes devemos iterar para obter o resultado ideal? Vamos denotar α, sendo o valor de todas as amplitudes acrescido de um, e β é a amplitude do estado iniciando a pesquisa em a_x. Então, a média é dada por (4):

$$\bar{a} = \frac{1}{N}((N-1)\alpha - \beta) \quad (4)$$

Usando (3), (2) e (1), temos:

$$\alpha_{k+1} = -\alpha_k + \frac{2}{N}\left((N-1)\alpha_k - \beta_k\right) = \left(1 - \frac{2}{N}\right)\alpha_k - \frac{2}{N}\beta_k$$

$$\beta_{k+1} = -(-\beta_k) + \frac{2}{N}\left((N-1)\alpha_k - \beta_k\right) = \left(1 - \frac{2}{N}\right)\beta_k + \frac{2(N-1)}{N}\alpha_k \quad (5)$$

$$\alpha_0 = \beta_0 = 2^{-n/2}$$

onde α_k e β_k são os estados anteriores, e α_{k+1} e β_{k+1} são os próxmos estados de α e β.

A solução (5) leva a uma equação quadrática com raízes complexas. A abordagem analítica pode ser complicada, mas observa-se que, depois de uma substituição $\chi = \alpha\sqrt{N} - 1$, a equação (5) torna-se uma equação de rotação de um ponto (χ, β) ao redor do centro das coordenadas do sistema por um ângulo $\Delta x, \sin\Delta x = \frac{2\sqrt{N-1}}{N}$. O melhor resultado é alcançado quando o ângulo atinge $\pi/2$, então o número de iterações é apresentado em (6):

$$k_{max} = \frac{\pi/2}{\Delta x} \approx \frac{\pi/2}{\frac{2\sqrt{N-1}}{N}} \approx \frac{\pi\sqrt{N}}{4} \quad (6)$$

Após a última iteração, a medição final é executada.

3.1. Grover sem emaranhamento quântico

A propriedade de emaranhamento quântico é considerada necessária para que os algoritmos quânticos superem os

clássicos. Porém, diversos autores, dentre eles LLOYD (1999) e MEYER (2000) observaram em suas pesquisas que o algoritmo de busca quântico de Grover pode ser implementado sem o emaranhamento quântico. Isso só é possível com a realização de substituições de partículas múltiplas (características quânticas) por uma partícula única, porém com muitos estados exponencialmente associados a ela.

Segundo LLOYD (1999), qualquer algoritmo quântico pode ser reescrito sem o uso de emaranhamento. Para tal, basta simplesmente desconsidedar a estrutura do produto tensorial do espaço de Hilbert. Fazendo isso, naturalmente, haverá um custo extra de utilização do sistema, já que a computação quântica estará sendo subjulgada.

Não se deve concluir que o emaranhamento é desnecessário. Para algoritmos iterativos, pode haver redução do número de consultas necessárias, reduzindo o caminho até a solução. Já nos algoritmos de contagens (funções locais), há perda de desempenho e aumento no uso dos recursos para sua execução. Simon (1994) demonstrou em seu algoritmo que a implementação da fatoração de Shor (1994) sem o emaranhamento não apresentavam resultados satisfatórios.

Concluímos que alguns algoritmos quânticos podem ter seus equivalentes clássicos, abrindo mão de propriedades quânticas, em especial, o emaranhamento. Por outro lado, nem todos os algoritmos respondem bem a esse tipo de adaptação. Para o contexto desse artigo, as pesquisas de LLOYD (1999) e MEYER (2000) mostram que o algoritmo de busca quântico de Grover não sofre perdas ao retirar a propriedade de emaranhamento quântico, sendo assim, será conceitualizado o algoritmo de Grover em sistemas clássicos, visto que o objetivo do artigo é a criação de um sistema híbrido de buscas.

3.2. Implementação híbrida do algoritmo de Grover

Conforme a sessão 3.1, o algoritmo de Grover pode ser implementado sem utilizar algumas propriedades que são exclusivamente quânticas. Diante disso, é possível a criação de um modelo de algoritmo que seja híbrido, e possa ser executado tanto em sistemas clássicos quanto em sistemas quânticos.

YAMASHITA (2006) propõe em seu trabalho, a criação de um framework com o objetivo de permitir que algoritmos sejam ajustados de forma automática, dependendo do modelo clássico ou modelo quântico.

Com relação ao algoritmo de Grover (1996), que pode ser considerado de uso geral, a adaptação de seu funcionamento em diversos modelos computacionais oferece notável flexibilidade em sua utilização.

Para a modelagem híbrida proposta por esse artigo, os conceitos propostos por YAMASHITA (2006) foram utilizados, onde o algoritmo de Grover foi implementado usando uma linguagem Clássica (C++) e uma linguagem Quântica (QCL).

O framework capaz de compatibilizar essa dupla implementação, funciona analisando o código e gerando novos códigos baseados nas plataformas específicas. Neste artigo, utilizamos o modelo, conceitos e implementamos uma versão própria do framework proposto por YAMASHITA (2006), mais simples com o objetivo apenas de gerar a versão híbrida do algoritmo de Grover.

Na Figura 3, podemos observar o fluxo da informação dentro do pseudo-framework criado para esse artigo. O código desenvolvido é aplicado no framework, que faz uma pré-análise e gera os circuitos e códigos baseados no tipo de sistema a ser aplicado.

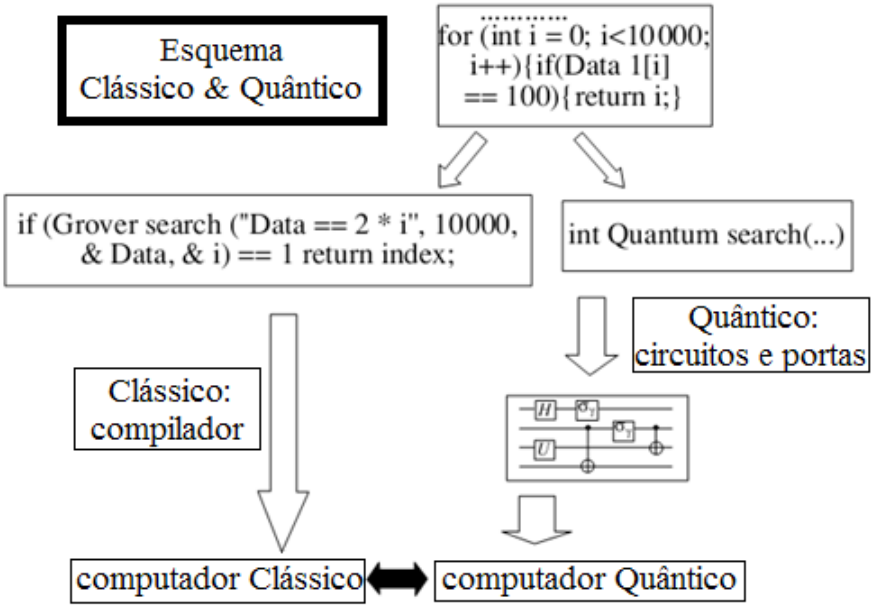

Figura 2: Framework para geração de código híbrido.
Fonte: YAMASHITA, 2006.

No Quadro 1, podemos observar um trecho do código fonte do algoritmo de Grover em linguagem C++. Para fins de comparação, apenas a função Grover() está sendo apresentada.

Quadro 1. Função Grover em C++.

```
void grover(int target, quantum_reg *reg)
{
   int i;

   oracle(target, reg);

   for(i=0;i<reg->width;i++)
      quantum_hadamard(i, reg);

   inversion(reg);

   for(i=0;i<reg->width;i++)
      quantum_hadamard(i, reg);
}
```

Por outro lado, no Quadro 2, notamos um trecho do código fonte do algoritmo de Grover em linguagem QCL. Para fins de comparação, apenas a função Grover() está sendo apresentada.

Quadro 2. Função Grover em QCL.

```
int qufunction Grover(int x)
{
   const N = 16;
   quregister A[sqrt(N)];
   int i, j;

   qufor (<i>=<0..N-1>)  A<i> = 1 / sqrt(N);
   for (j = 0; j < pi*sqrt(N) / 4; j++)
   {
      qufor (<i>=<0..N-1>)  A<i> = (i == x) ? –A<i> : A<i>;
      qufor (<i>=<0..N-1>)  A<i> = -A<i> + 2 *
         qsum(i = 0 to N-1) { return A<i>;}
   }
   return measure(A);
}
```

4. Simulações

Com o objetivo de validar os conceitos apresentados nesse artigo, um ambiente de simulação foi estruturado com o desafio de realizar testes de carga nos algoritmos construídos.

Para realização dos testes, foi gerado um banco de dados em XML com uma massa de dados não-estruturada de cerca de 5.000 registros. O objetivo foi realizar buscas com os algoritmos de Grover nessa massa de dados, e analisar três fatores importantes:

(i) Compatibilidade dos algoritmos, ou seja, se o algoritmo clássico e o quântico executam de formas semelhantes, sem a necessidade de realizar ajustes nos dados ou nos códigos fontes. Esse item avalia a portabilidade de códigos diferentes acessando o mesmo banco de dados.

(ii) Desempenho da execução, um comparativo simples de tempos decorridos, para gerar informações sobre os tempos gastos por cada um dos algoritmos, considerando as mesmas condições.

(iii) Número de iterações, como o algoritmo de Grover é iterativo, quanto menor o número de iterações, com a mesma eficiência, melhor os resultados da execução dos algoritmos.

4.1. Simuladores

Para realizar as simulações, foram utilizadas duas ferramentas. Para o desenho e avaliação do Circuito Quântico, foi utilizada a ferramenta *Wolfram Demonstrations* (http://demonstrations.wolfram.com/). Essa ferramenta permitiu a construção de um código dinâmico para gerar o circuito quântico que foi implementado no simulador quântico para execução das buscas.

Já para execução do código quântico, foi utilizada a biblioteca *libquantum* (http://www.enyo.de/libquantum/). Tal biblioteca foi apresentada no trabalho de SCHUBOTZ (2007), onde o autor realiza um estudo comparativo entre três simuladores, e a libquantum mostra-se melhor em todos os critérios.

A *libquantum* é uma biblioteca em C específica para computação quântica. Ela usa o modelo QRAM, e fornece registradores quânticos, operações unitárias e funções de medição. A biblioteca vem com uma interface para codificar registros quânticos, controle de correção de erro quântico (QEC) e oferece flexibilidade no uso. Seu principal objetivo é uma precisa simulação física de um computador quântico com alto desempenho (SCHUBOTZ, 2007).

Apesar da biblioteca já incluir a implementação do algoritmo de Grover, para as simulações, utilizamos os algoritmos e circuitos gerados no decorrer da pesquisa.

4.2. Resultados

Os testes em sistemas clássicos foram realizados em ambiente de computação clássica tradicional, onde o arquivo XML com os dados estava armazenado em disco e as rotinas em C++ foram executadas e os indicadores analisados.

Já os testes em sistemas quânticos, foram realizados no simulador *libquantum* apresentado na sessão 4.1. O arquivo XML foi armazenado dentro da estrutura do simulador e os testes foram realizados e os devidos indicadores foram analisados.

Na Figura 4, observa-se o circuito quântico construído dentro da ferramenta *libquantum*, notem que o circuito sugere pelo menos 4 iterações, porém devido ao tamanho da massa de dados, a execução do circuito completo é interativa até que a massa de dados seja completamente analisada.

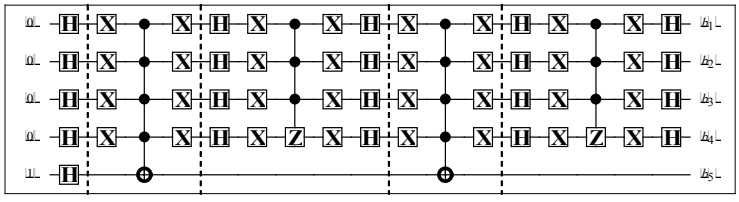

Figura 4: Cirtuito Quântico iterativo aplicado na libquantum (gerado na ferramenta Wolfram).

Na Tabela 1, temos os resultados das análises de cada um dos algoritmos, executados e analisados nos sistemas propostos, baseado em uma massa de dados com 5.000 registros em formato XML.

Podemos notar que o sistema Quântico, apesar de rodar sobre um simulador, apresentou uma quantidade menor de iterações até convergir para o melhor resultado.

Apresentam-se as três iterações do sistema Quântico no momento em que a convergência ocorreu, e sua precisão chegou aos 100% com 55 iterações, mesma precisão atingida pelo sistema Clássico em 72 iterações. Essa diferença de precisão e número de iterações é esperada, já que o sistema Clássico é determinístico e o sistema Quântico é probabilístico.

Tabela 1. Grover Clássico X Grover Quântico.

	Grover			
	Clássico	Quântico	Quântico	Quântico
Iterações	72	54	55	56
Tempo decorrido	23s	30s	32s	34s
Precisão	100%	99,8%	100%	99,8%
Compatibilidade	Total	Total	Total	Total

Em termos de tempo decorrido, notamos uma diferença considerável onde o Grover clássico (23s) é cerca de 39% mais rápido que o Grover quântico (32s), porém isso se justifica pois o sistema quântico está rodando sobre um simulador, e a documentação da libquantum afirma perdas de até 45% pelo fato de ser um ambiente simulado. Além disso, não existem sistemas quânticos consistentes disponíveis para conseguirmos uma simulação com valores reais.

Observamos também, que os códigos são perfeitamente portáveis, ou seja, ambos os códigos funcionaram na mesma massa de dados, sem quaisquer modificações ou necessidades de ajustes em nenhuma das partes.

CONSIDERAÇÕES FINAIS

A busca em bancos de dados não-estruturados é muito importante para ciência e tecnologia. Ela serve como comparativo de algoritmos para demonstrar o poder de computadores quânticos. Curiosamente, um algoritmo totalmente quântico é relativamente simples de ser implementado, o que traz vantagens para essa área.

Neste artigo, foram apresentados de forma breve alguns conceitos quânticos básicos. Também foi apresentado com mais detalhes a busca quântica, com especial atenção para o algoritmo de busca de Grover, e demonstra seu funcionamento em sistemas clássicos e quânticos.

Seguindo as implementações sobre o algoritmo de Grover, o artigo apresenta um pseudo-framework capaz de tornar híbrido o algoritmo de busca, permitindo uma flexibilidade em seu uso.

Após a criação dos algoritmos, simulações foram feitas, com o objetivo de comparar o funcionamento do algoritmo de Grover em sistemas clássicos (normais) e em sistemas quânticos (simulados). Os resultados foram apresentados na sessão 4.2, onde podemos observar poucas variações entre os modelos.

O objetivo de implementar um sistema hibrido de busca, foi cumprido. Os algoritmos gerados conseguiram realizar buscas com eficiência em bases em formato XML, tanto para sistemas clássicos quanto para quânticos (simulados).

O aspecto mais importante implícito nesse trabalho é que, gerenciar um banco de dados não-estruturado em um computador quântico é possível e eficiente.

TRABALHOS FUTUROS

Os resultados obtidos com essa pesquisa serão diretamente aplicados no projeto de mestrado do autor deste artigo, cujo tema é Busca Quântica em Bancos de Dados Relacionais. Este artigo apresenta os resultados da primeira fase, que se trata de buscas em arquivos XML, a próxima

fase envolverá a integração com bancos de dados relacionais e acesso aos dados em baixo nível.

REFERÊNCIAS BIBLIOGRÁFICAS

BENIOFF, P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. **Journal of Statistical Physics**, 22, 1980, pp. 563-591.

BENIOFF, P. **Spaces searches with a quantum robot**. In Quantum computation and information. Washington DC: AMS Series on Contemporary Mathematics, 2000, 305: 1-12. Disponível em: quant-ph/0003006.

BERNSTEIN, E.; VAZIRANI, U. **Quantum Complexity Theory**. In Proceedings 25th ACM Symposium on Theory of Computing, 1993, pp. 11-20.

BERTHIAUME, A.; BRASSARD, G. Oracle quantum computing. **Journal of Modern Optics**, vol.41, n. 12. December, 1994, pp. 2521-2535.

BRASSARD, G. Searching a quantum phone book. **Science**, 1997, 275(5300): 627-628.

BRASSARD, G.; HOYER, P. **An exact quantum polynomial-time algorithm for Simon´s problem**. In: Proceedings of 35th Annual Symposium on the Foundations of Computer Science. 1997, 116-123.

BRASSARD, G.; HOYER, P.; TAPP, A. **Quantum counting**. Lectures Notes in Computer Science, 1998, 1443: 820-831.

BRICKMAN, K. A.; HALJAN , P. C.; LEE, P. J.; ACTON, M.; DESLAURIERS, L.; MONROE, C. **Implementation of Grover's quantum search algorithm in a scalable system**. FOCUS Center and Department of Physics, University of Michigan. In Proceedings of The American Physical Society, Physical Review A 72, 050306-1(4). Michigan, USA:2005.

BUGAJSKI, S. **Quantum Search**. Archiwum Informatyki Teoretycznej i Stosowanej, vol 13 No 2/2001, pp. 143-150.

CARAIMAN, S.; MANTA, V. **Parallel Simulation of Quantum Search**. "Gheorghe Asachi" Technical University of Iasi. In Proceedings Journal of Computers, Communications & Control, V(5), pp.634-641. Romania, 2010.

DESURVIRE, E. **Classical and Quantum Information.** eBook (EBL), New York, Cambridge University Press, 2009.

DEUTSCH, D. **Quantum Theory, the Church-Turing principle and the universal quantum computer**. In Proceedings Royal Society London Series A, 400, 1985, pp. 96-117.

FRANCIK, J. **Quantum Software**. Studia Informatica. Vol 23, n. 2A (48). Redakcji, 2002.

GROVER, L. K. **A fast quantum mechanical algorithm for database search**. In Proceedings of 28th ACM Annual STOC, pp. 212-219. ACM Press New York. Philadelphia-PA/USA:1996.

GUO, H.; LONG, G.L.; LI, F. **Quantum algorithms for some well-known NP problems**. Communications in Theoretical Physics, 2002, 37(4): 424-426.

HAWKING, S. **O Universo numa Casca de Noz**. Rio de Janeiro: Nova Fronteira, 2009, 216p.

HU, H.; ZHANG, Y.; LU, Z. **An efficient quantum search engine on unsorted database**. Huazhong University of Science and Technology, 2009. Disponível em: cs.DB/0904.3060v1.

KLAMKA, J. **Quantum search algorithm**. Seminarium Sieci Komputerowe, Zakopane, 2002.

LLOYD, S. **Quantum search without entanglement**. Physical Reviews A61 (1999) 010301.

LONG, G.L.; LIU, Y. **Search an unsorted database with quantum mechanics**. Frontiers of Computer Science in China, 2007, 1(3): 247-271.

MEYER, D. A. **Sophisticated Quantum Search Without Entanglement**. Project in Geometry and Physics. Department of Mathematics. Institute for Physical Sciences. University of California/San Diego. Disponível em quant-ph/0007070. 2000.

MUTIARA, A. B.; REFIANTI, R. **Simulation of Grover's Algorithm Quantum Search in a Classical Computer**. In Proceedings of the International Journal of Computer Science and Information Security. Indonesia, 8(9)261–269,1994.

NIELSEN, M. A.; CHUANG, I. L. **Computação Quântica e Informação Quântica**. Rio de Janeiro, Brasil, Bookman/Artmed, 2005.

ÖMER, B. **Quantum Programming in QCL**. Institute of Information Systems. Technical University of Vienna, pp 42-45. Vienna, 2000.

OSKIN, M.; CHONG, F. T.; CHUANG, I. L. **A Pratical Architecture for Reliable Quantum Computers**. Universidade de Toronto. IEEE Computer Society. 2002.

SCHUBOTZ, R. **Programming and Simulation of Quantum Agents**. Department of Computer Science. Faculty of Natural Sciences and Technology I. Saarland University, pp. 31-36. Saarbrücken, 2007.

SHOR, P. W. **Algorithms for quantum computation**: discrete logarithms and factoring. In Proceedings 35th Annual Symposium of Fundamentals of Computer

Science (FOCS). S. Goldwasser, Santa Fe, NM. pp. 124-134. IEEE Computer Society, Los Alamitos. 20-22 Novembro 1994.

SIMON, D. R. **On the power of quantum computation**. In Proceedings of the 35th Annual Symposium of Foundations of Computer Science. S. Goldwasser, Santa Fe, NM. pp. 116-123. 20-22 Novembro 1994.

TWAMLEY, J. J. **A hidden shift quantum algorithm**. Journal on Physics A, 2000, 33: 8973-8979.

YAMASHITA, S. **How to Utilize a Grove Search in General Programming**. Scholl of Information Science, Nara Institute of Science and Technology. In Proceedings Laser Physics, vol 16, n. 4, pp 730-734. Ikoma, Nara, Japan, 2006.

YAO, A. **Quantum circuit complexity**. In Proceedings 34th Annual Symposium of Foundations of Computer Science (FOCS), 1993, pp. 352-361.

Michael Alexandre Pontes é bacharel em Ciência da Computação pela UNiRP, Pós-graduado em Desenvolvimento Cliente/Servidor e Internet pela UNiRP, Pós-graduado em Engenharia de Sistemas pela Faculdade Modelo. Detentor de diversas certificações importantes, como Microsoft, Oracle, Progress, Novell, Citrix. Atualmente é professor nas seguintes instituições: Universidade Paulista, FATEC Rio Preto e Kees Informática. Também é líder de unidade de negócio da empresa Dual Software Ltda. Tem experiência com Governança de TI e Administração de Banco de Dados. Atua diretamente na área de Sistemas de Informação com ênfase em Engenharia de Sistemas. Possui vários projetos de pesquisa e desenvolvimento, tendo sido reconhecido e premiado em vários deles.

Manoel Ferreira Borges Neto é graduado em Física pela Universidade de Brasília (UnB), Doutorado em Matemática pelo “Kings College - University of London” e Pós-doutorado pelo “Department of Mathematics and Applied Mathematics - University of Cape Town (UCT)”. Professor titular da Universidade Estadual Paulista (UNESP). Membro da “International Association of Mathematical Physics (IAMP)”. Membro e revisor da “American Mathematical Society (AMS)”. Membro da “European Society of Computational Methods in Sciences and Engineering (ESCMSE)”. Co-fundador e membro permanente do “World Peace and Diplomacy Forum (WPDF)”, Cambridge. Vasta experiência na área de matemática e matemática aplicada atuando principalmente nos temas: i) Geometrias Hipercomplexas; ii) Aspectos geométricos da Física-Matemática, notadamente das Teorias Alternativas da Gravitação, e suas relações com Variedades Topológicas; iii) Criptografia e Computação Quântica.