8 October 2002

QUANTUM LEARNING SEMINAR
LECTURE 2: GROVER'S ALGORITHM

David A. Meyer

Project in Geometry and Physics, Department of Mathematics
University of California/San Diego, La Jolla, CA 92093-0112
`http://math.ucsd.edu/~dmeyer/`; `dmeyer@math.ucsd.edu`

Introduction

Grover's algorithm [1] is a quantum analogue of a Markovian version of Algorithm P. As we will see in this lecture, it requires only $O(\sqrt{N})$ membership queries. This is a quantum improvement in *sample complexity* for this problem of concept learning from membership queries. The geometrical description of Grover's algorithm presented here was originally noticed by several people, independently [2].

The query state

Rather than preparing the obvious quantum analogue of the initial probability vector (1.1) in Algorithm P, namely

$$\sum_x \frac{1}{\sqrt{N}}|x,0\rangle$$

(recall that quantum states have unit ℓ_2-norm), Grover's algorithm works by preparing a more subtle quantum state:

$$\sum_x\Big(\frac{1}{\sqrt{2N}}|x,0\rangle - \frac{1}{\sqrt{2N}}|x,1\rangle\Big) = \sum_x \frac{1}{\sqrt{N}}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{2.1}$$

The notation here takes advantage of the fact that $\mathbb{C}^{2N} = \mathbb{C}^N \otimes \mathbb{C}^2$, so the basis vectors $|x,b\rangle = |x\rangle \otimes |b\rangle$, where $\{|x\rangle \mid x \in \mathbb{Z}_N\}$ and $\{|b\rangle \mid b \in \mathbb{Z}_2\}$ are orthogonal bases for the tensor factors $\mathbb{C}^N$ and $\mathbb{C}^2$, respectively. We use the additional notational simplification that $|x\rangle|b\rangle = |x\rangle \otimes |b\rangle$; *i.e.*, we will often omit the tensor product symbol when writing vectors.

Membership oracle geometry

Querying the membership oracle with the quantum computer in the state (2.1) transforms the state to

$$\sum_x \frac{1}{\sqrt{N}}|x\rangle\frac{1}{\sqrt{2}}(|0+g_a(x)\rangle - |1+g_a(x)\rangle) = \sum_x \frac{1}{\sqrt{N}}|x\rangle(-1)^{g_a(x)}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$= \Big(\sum_x \frac{1}{\sqrt{N}}|x\rangle(-1)^{g_a(x)}\Big)\otimes\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

since $|0\rangle - |1\rangle$ goes to $|0\rangle - |1\rangle$ when $g_a(x) = 0$ and to $|1\rangle - |0\rangle = -(|0\rangle - |1\rangle)$ when $g_a(x) = 1$. Grover's algorithm is organized so that the last tensor factor is unchanged by the evolution. Thus we can understand the action of querying the membership oracle as a reflection of the first tensor factor of the state vector in the hyperplane orthogonal to the basis vector $|a\rangle \in \mathbb{C}^N$—the only change is to the component of $|a\rangle$, which is negated.

Figure 2 shows the (real) subspace of $\mathbb{C}^N$ spanned by $|a\rangle$ and $\sum_x |x\rangle/\sqrt{N}$. The intersection of the hyperplane orthogonal to $|a\rangle$ with this plane is the red line; the angle θ between it and the initial state satisfies $\sin\theta = 1/\sqrt{N}$. Querying the membership oracle reflects the state vector in this plane, as shown.

Geometry of Grover's algorithm

Just as in Algorithms D and P of Lecture 1, after the membership oracle responds, the state of the computer should be adjusted, before being returned to the oracle. In a quantum computer, this adjustment must be unitary, as well as independent of the oracle. As shown in Figure 2, a natural choice is to reflect in the hyperplane orthogonal to $\sum_x |x\rangle/\sqrt{N}$, the intersection of which with the subspace shown is the green line. Reflecting the post-query state in this hyperplane produces the vector shown; the angle between (the negative of) this vector and the initial vector is 2θ since the product of two reflections is a rotation by twice the angle between the hyperplanes.

A second iteration: sending the state vector to the membership oracle—equivalently, reflecting in the red hyperplane—and then reflecting in the green hyperplane, rotates the state vector by another 2θ towards $|a\rangle$. Grover's algorithm works by repeating this pair of reflections k times, where k is the smallest positive integer approximate solution to

$$\theta + k\cdot 2\theta = \frac{\pi}{2}$$

since the state vector then is close to $|a\rangle$. That is,

$$k = \Big\lfloor \frac{\pi}{4\theta} - \frac{1}{2}\Big\rceil \sim \frac{\pi}{4}\sqrt{N} \quad \text{as} \quad N\to\infty.$$

Here $\lfloor\cdot\rceil$ denotes "closest integer to".

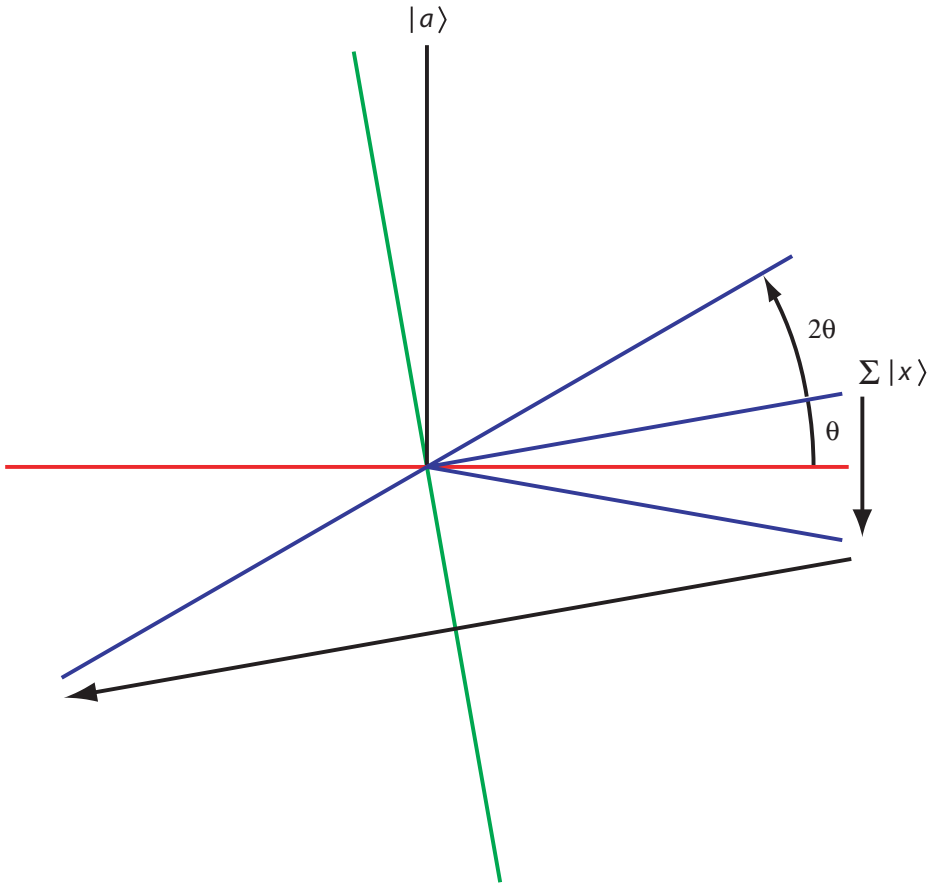

Figure 2. The first iteration of Grover's algorithm consists of reflecting the initial equal superposition vector in the (red) hyperplane orthogonal to $|a\rangle$ and then reflecting it in the (green) hyperplane orthogonal to the equal superposition vector. Each subsequent iteration consists of the same two reflections, and each rotates the state by 2θ towards $|a\rangle$, where $\sin\theta = 1/\sqrt{N}$.

Measurement

The last stage of Grover's algorithm is to measure the state vector. Let us not worry about how to implement a measurement; we'll just take the following definition as a correct description of quantum mechanics.

DEFINITION. A *projective* (or *von Neumann* [3]) *measurement* on $\mathbb{C}^N$ is defined by a choice of orthonormal basis $\{|\phi_j\rangle \mid j \in \mathbb{Z}_N\}$. The outcome of each measurement is probabilistic: when the state is $|\psi\rangle \in \mathbb{C}^N$, it is $|\phi_j\rangle$ with probability $|\langle\phi_j|\psi\rangle|^2$.

Since after k iterations the state vector is within an angle θ of $|a\rangle$, the probability that the outcome of measurement in a basis including $|a\rangle$ is $|a\rangle$, is

$$|\langle a|\psi\rangle|^2 \geq 1 - \sin^2\theta = 1 - \frac{1}{N},$$

which is asymptotically 1. Thus Grover's algorithm learns g_a with probability close to 1

using $O(\frac{\pi}{4}\sqrt{N})$ membership queries, quadratically fewer than the classical algorithms D and P, and in fact, quadratically fewer than is possible classically.

References

[1] L. K. Grover, "A fast quantum mechanical algorithm for database search", in *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, Philadelphia, PA, 22–24 May 1996 (New York: ACM 1996) 212–219;
L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack", *Phys. Rev. Lett.* **79** (1997) 325–328.

[2] R. Jozsa, "Searching in Grover's algorithm", `quant-ph/9901021`.

[3] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik* (Berlin: Springer-Verlag 1932); transl. by R. T. Beyer as *Mathematical Foundations of Quantum Mechanics* (Princeton: Princeton University Press 1955).