CS191 – Fall 2014
Lecture 19b: Grover's Algorithm - Amplitude Amplification

Birgitta Whaley
(Dated: Wednesday November 5, 2014)

I. AMPLITUDE AMPLIFICATION IN GROVER SEARCH

The Diffusion operator D has two properties:

1. It is unitary and can be efficiently realized.
2. It can be seen as an "inversion about the mean."

We discussed the first property last time. We now analyze the second property.
For $N = 2^n$, we can explicitly evaluate

$$\begin{aligned} D &= -I + 2|\psi_0\rangle\langle\psi_0| \\ &= (H^{\overleftrightarrow{n}})^\dagger[-I + 2|0\rangle\langle 0|]H^{\overleftrightarrow{n}} \end{aligned}$$

as:

$$\begin{aligned} D &= H_N \begin{pmatrix} +1 & 0 & \cdots & 0 \\ 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 \end{pmatrix} H_N \\ &= H_N \left(\begin{pmatrix} +2 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} - I \right) H_N \\ &= H_N \begin{pmatrix} +2 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} H_N - I \\ &= \begin{pmatrix} +2/N & +2/N & \cdots & +2/N \\ +2/N & +2/N & \cdots & +2/N \\ \vdots & \vdots & \ddots & \vdots \\ +2/N & +2/N & \cdots & +2/N \end{pmatrix} - I \\ &= \begin{pmatrix} +2/N - 1 & +2/N & \cdots & +2/N \\ +2/N & +2/N - 1 & \cdots & +2/N \\ \vdots & \vdots & \ddots & \vdots \\ +2/N & +2/N & \cdots & +2/N - 1 \end{pmatrix} \end{aligned}$$

The indexing here is such that the first state (top left hand corner of the matrices) is the target state $|a\rangle$. Recall that the central matrix in D is a conditional phase shift matrix, i.e., it puts a phase shift in front of all states except the target. Now for large N, the matrix D has diagonal elements approx equal to $-(1-2/N)$ and very small, positive and constant off-diagonal elements $(2/N)$. So in each step the amplitude of every basis state contributes by a small amount to all other basis states. This is a generalization of the phenomenon of diffusion on a lattice. See the discussion of motivation and form of matrix D by Grover in his article quant-ph/0109116.

Consider the action of D on a vector $|\alpha\rangle$ to generate another vector $|\beta\rangle$:

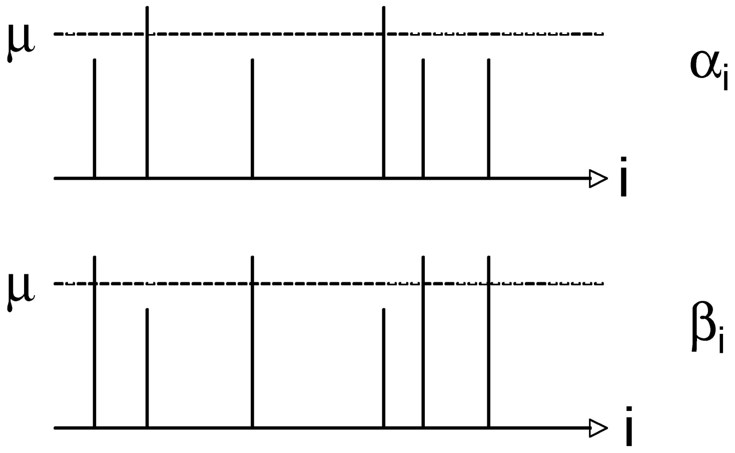

FIG. 1: Inversion of amplitudes α_i about their mean value μ.

$$D \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_i \\ \vdots \\ \alpha_N \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_i \\ \vdots \\ \beta_N \end{pmatrix}$$

Define $\mu = \sum_i \alpha_i / N$ as the mean amplitude Then

$$\begin{aligned} \beta_i &= \frac{2}{N}\sum_j \alpha_j - \alpha_i \\ &= 2(\mu - \alpha_i) \\ &= \mu + (\mu - \alpha_i) \end{aligned}$$

which corresponds to a reflection of α_i about the mean value μ. This is illustrated in Figure 1 above (note that if we start from the uniform superposition, the non-target states will have equal amplitude, we have just illustrated the principle for a general state here). Thus, the amplitude of $\beta_i = \frac{2}{N}\sum_j \alpha_j - \alpha_i = 2\mu - \alpha_i$ can be considered an "inversion about the mean" with respect to α_i. Now if we first change the sign of the amplitude of the target state, by applying the oracle as in the previous lecture, the target state is now significantly further away from the mean. The inversion about the mean further amplifies this, as shown in Figure 2 below.

This shows how quantum search algorithm iteratively improves the probability of measuring a solution by increasing the component of the target state at each iteration. The overall procedure is summarized as follows (see Figure 3 below):

1. Start state is $|\psi_0\rangle = \sum_x \frac{1}{\sqrt{N}}|x\rangle$
2. Invert the phase of $|a\rangle$ using f
3. Then invert about the mean using D
4. Repeat steps 2 and 3 $O(\sqrt{N})$ times, so in each iteration α_a increases by $\frac{2}{\sqrt{N}}$.

Suppose we just want to find a with probability $\frac{1}{2}$. Until this point, the rest of the basis vectors will have amplitude at least $\frac{1}{\sqrt{2N}}$. In each iteration of the algorithm, α_a increases by at least $\frac{2}{\sqrt{2N}} = \sqrt{\frac{2}{N}}$. Eventually, $\alpha_a = \frac{1}{\sqrt{2}}$. The number of iterations to get to this α_a is $\leq \sqrt{N}$.

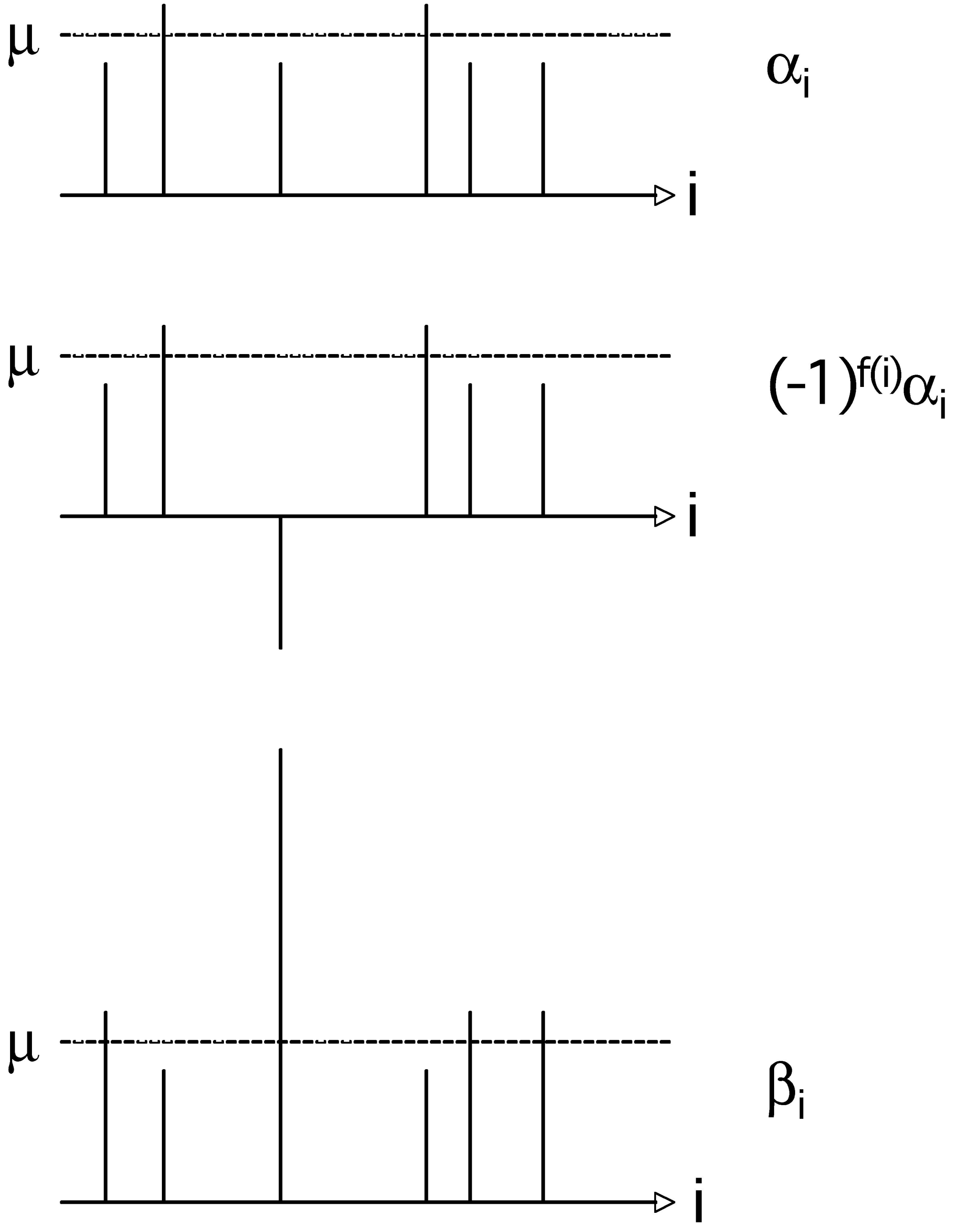

FIG. 2: Application of oracle to invert sign of target state followed by inversion of amplitudes α_i about their mean value μ gives rise to amplification of the target component.

A. Applications of quantum search

Grover's algorithm is often called a "database" search algorithm, where you can query in superposition. Requirements for this are discussed in Nielsen and Chuang, Ch. 6/5 and discussed in Zalka, quant-ph/9901068.

Other things you can do with a similar approach:

1. Find the minimum.

2. Approximately count elements, or generate random ones. Kaye et al., Ch. 8.3, Nielsen/Chuang Ch. 6.3.

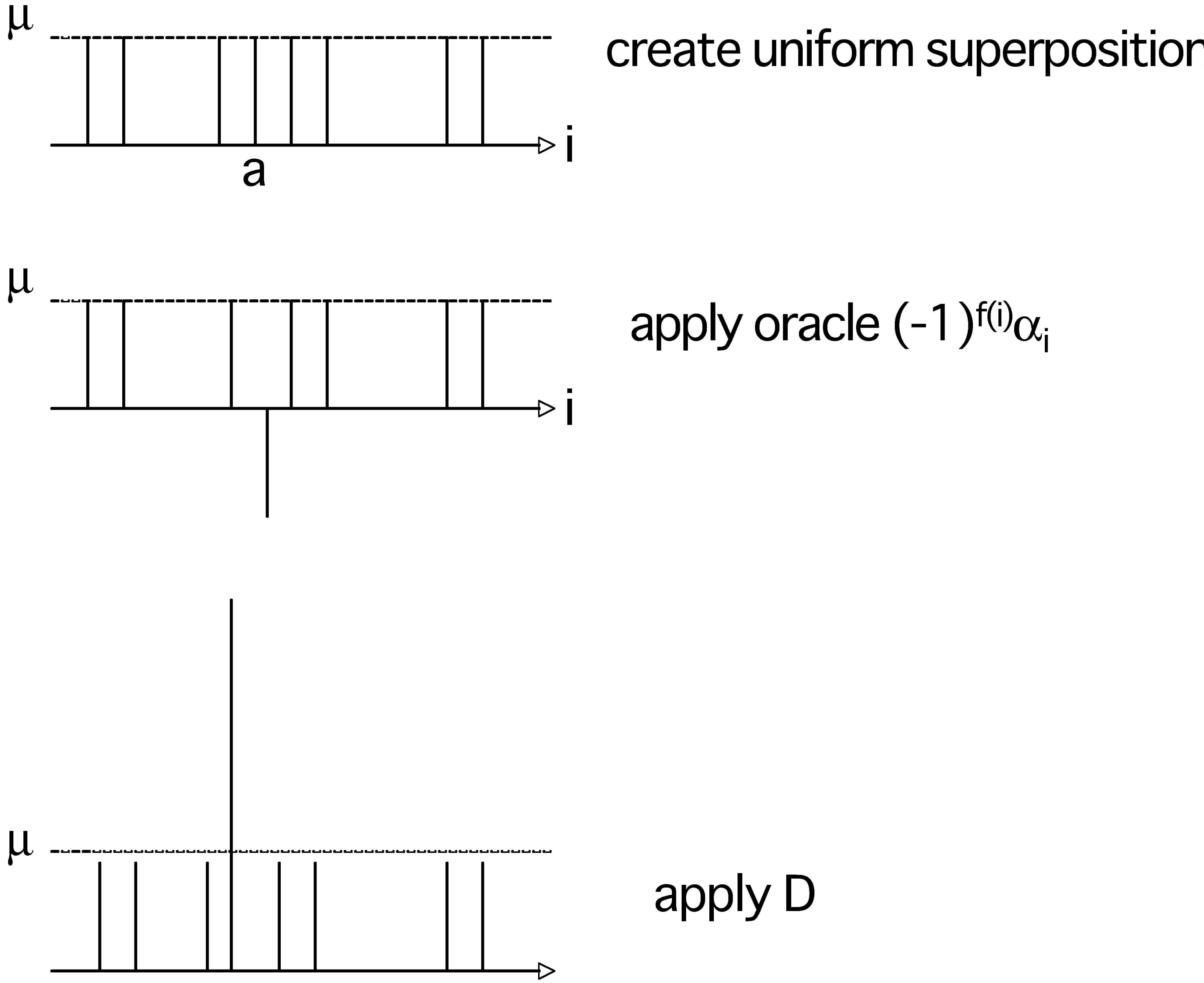
μ
create uniform superposition
i
a
μ
apply oracle $(-1)^{f(i)}\alpha_i$
i
μ
apply D

FIG. 3: The first three steps of Grover's algorithm. We start with a uniform superposition of all basis vectors in the top panel. In the middle panel we have used the function f to invert the phase of α_k. After running the diffusion operator D in the bottom panel, we have amplified α_k while decreasing all other amplitudes.

3. Speed up the collision problem.

4. Speed up the test for matrix multiplication. In this problem we are given three matrices, A, B, and C, and are told that the product of the first two equals the third. We wish to verify that this is indeed true. An efficient (randomized) way of doing this is picking a random array r, and checking to see whether $Cr = ABr = A(Br)$. Classically, we can do the check in $O(n^2)$ time, but using a similar approach to Grover's algorithm we can speed it up to $O(n^{1.75})$ time.

5. Speedup exhaustive search in NP-complete problems, although this alone is not enough to provide efficient solution. See Ambainis, quant-ph/0504012 for a review of applications to NP-complete problems, and also an example in Nielsen/Chuang Ch. 6.4.

II. REFERENCES AND FURTHER READING

1. Grover's algorithm and amplitude amplification: quant-ph/9605043

2. Diffusion transform and other motivations from physics: Grover, quant-ph/0109116