GROVER'S ALGORITHM

Searching for a Needle In a Haystack

by

Samuel J. Lomonaco, Jr.

Dept. of Comp. Sci. & Electr. Engr.

University of Maryland Baltimore County

Baltimore, MD 21250

Email: Lomonaco@UMBC.EDU

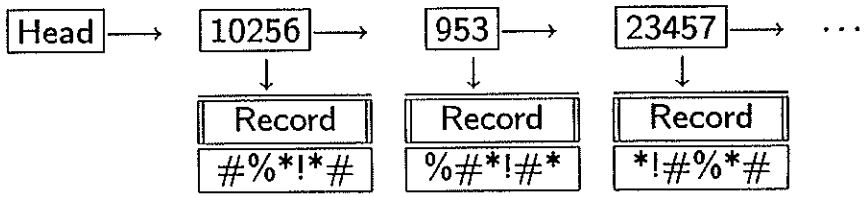
WebPage: http://www.csee.umbc.edu/~lomonaco

Grover's Algorithm
Finding a Needle in a Haystack

Consider a large unstructured database consisting of $N = 2^n$ records labelled in random order by the integers

$$0, 1, 2, \ldots, N-1$$

E.g., the database could be stored as a linked list



On average, we would have to retrieve $N/2$ labels before finding the label x_0. Hence, the average computational work would be

$$O(N)$$

computational steps

Another Example

Consider a **plaintext/ciphertext attack by brute force key search** on a message encrypted with the *Data Encryption Standard (DES)*, where the key K is a 56 bit number.

Given the plaintext/ciphertext pair

PlainText	At0500BlowUpTheEmbassyAt
CipherText	xjejpwvziderkqldievmsfkfdlqye

crack the entire cipher by encrypting the PlainText

At0500BlowUpTheEmbassyAt

with each of the keys

$$0, 1, 2, \ldots, 2^{56} - 1 \ ,$$

in turn, until the key K_0 is found that produces the CipherText

xjejpwvziderkqldievmsfkfdlqye

In other words, if

$$(P, C)$$

denotes the available plaintext/ciphertext pair, and if

$$K_0$$

denotes the key such that

$$DES\,(P, K_0) = C \ ,$$

then the **oracle** is

$$f\,(K) = \begin{cases} 1 & \text{if } K = K_0 \\ 0 & \text{otherwise} \end{cases}$$

$I_{|\psi\rangle}$ is an Inversion

Note that

$$\boxed{I_{|x_0\rangle} = I - 2\,|x_0\rangle\,\langle x_0|}\,,$$

for

$$\boxed{\begin{aligned}(I - 2\,|x_0\rangle\,\langle x_0|)\,|x\rangle &= |x\rangle - 2\,|x_0\rangle\,\langle x_0 \mid x\rangle \\ &= \begin{cases} -|x_0\rangle & \text{if } x = x_0 \\ |x\rangle & \text{otherwise} \end{cases}\end{aligned}}$$

Also please note for any unit length ket $|\psi\rangle$

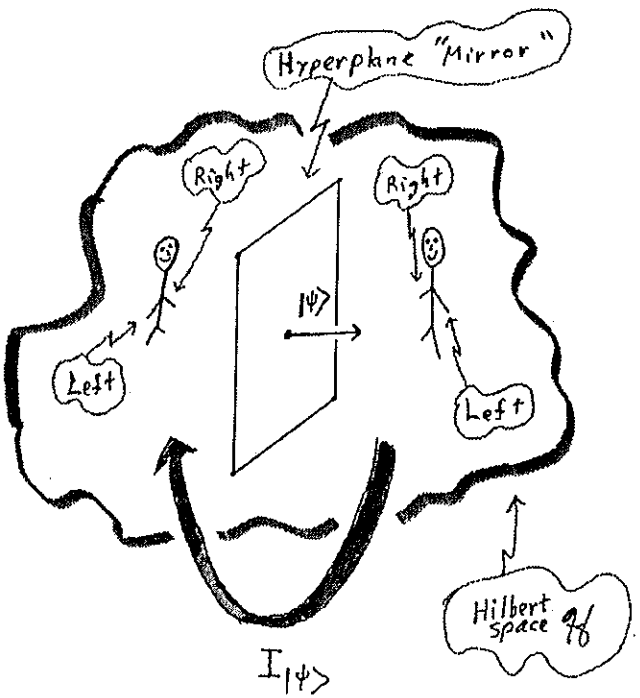
$$\boxed{I_{|\psi\rangle} = I - 2\,|\psi\rangle\,\langle\psi|}$$

is an **inversion** about the hyperplane $\perp$ to $|\psi\rangle$, i.e.,

"A Mirror Image Transformation"

"A Mirror Reflection"

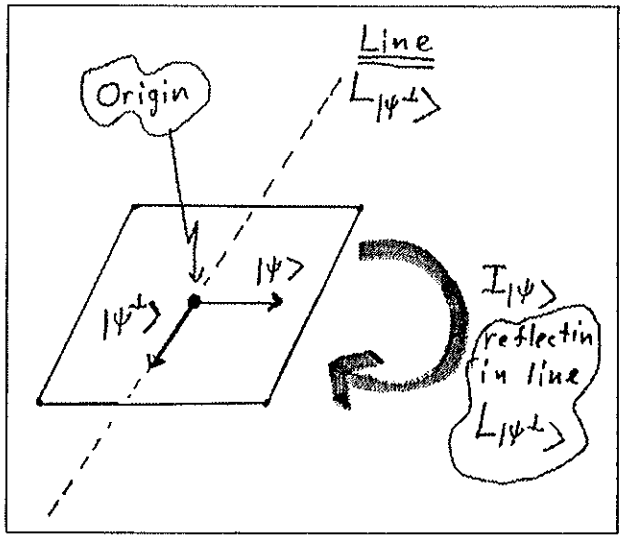
Inversion $I_{|\psi\rangle}$



Moreover, let $\left|\psi^{\perp}\right\rangle$ be be a ket in $\mathcal{S}_{\mathbb{R}} \perp |\psi\rangle$, and let $L_{\left|\psi^{\perp}\right\rangle}$ denote the line in $\mathcal{S}_{\mathbb{R}}$ passing through the origin and $\perp$ to $|\psi\rangle$. Then

$$\boxed{I_{|\psi\rangle}\Big|_{\mathcal{S}_{\mathbb{R}}} : \mathcal{S}_{\mathbb{R}} \longrightarrow \mathcal{S}_{\mathbb{R}}}$$

is a **reflection** in (**inversion** about) the line $L_{\left|\psi^{\perp}\right\rangle}$.



And moreover, if $\left|\psi^{\perp}\right\rangle$ is a unit length vector in $\mathcal{S}_{\mathbb{R}}$ which is $\perp$ to $|\psi\rangle$, then

$$\boxed{-I_{|\psi\rangle}\Big|_{\mathcal{S}_{\mathbb{R}}} \longrightarrow I_{\left|\psi^{\perp}\right\rangle}\Big|_{\mathcal{S}_{\mathbb{R}}}}$$

And finally, if $|\psi\rangle$ is a unit length ket in $\mathcal{H}$, and if $U : \mathcal{H} \longrightarrow \mathcal{H}$ is a unitary transformation, then

$$\boxed{UI_{|\psi\rangle}U^{\dagger} = I_{U|\psi\rangle}}$$

What's Going On?

The Method In Lov's "Madness"

Let

$$H : \mathcal{H} \longrightarrow \mathcal{H}$$

be the Hadamard transform given by

$$H = \bigotimes_{0}^{n-1} H^{(2)} ,$$

where

$$H^{(2)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

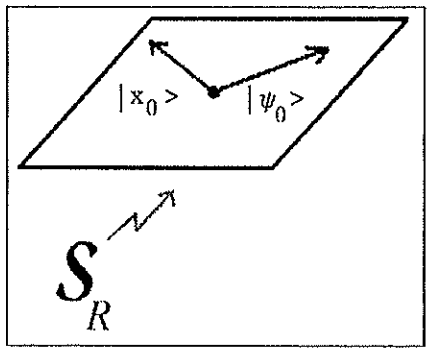
STEP 0.

This step creates a superposition of all basis states, i.e.,

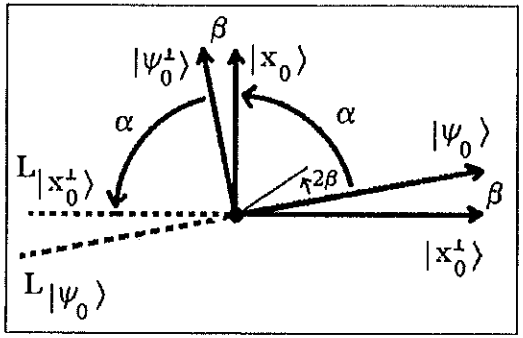
$$|0\rangle \longmapsto H|0\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle = |\psi_0\rangle$$

Thus, we now have "living" in $\mathcal{H}$ the 2-D plane

$$S_{\mathbb{R}} = Span_{\mathbb{R}} \left(|\psi_0\rangle , |x_0\rangle \right)$$



STEP 1. (Cont.)



Theorem

$L_1 \& L_2$ lines in $\mathbb{R}^2$
$L_1 \cap L_2 =$ point O
$\beta =$ Angle(L_1, L_2)

$\Longrightarrow$ $\text{Ref}_{L_2} \circ \text{Ref}_{L_1} = \text{Rot}_{2\beta}$ about O

Thus, $|\psi_0\rangle = \cos\beta \left|x_0^\perp\right\rangle + \sin\beta\,|x_0\rangle$, and

$$Q^k |\psi_0\rangle = \cos[(2k+1)\beta] \left|x_0^\perp\right\rangle + \sin[(2k+1)\beta]\,|x_0\rangle$$

STEP 1. (Cont.)

$$Q^k |\psi_0\rangle = \cos[(2k+1)\beta] \left|x_0^\perp\right\rangle + \sin[(2k+1)\beta]\,|x_0\rangle$$

Thus, we seek to iterate until

$$\sin[(2k+1)\beta]$$

is as large as possible. In other words, we seek the smallest possible positive integer $k = K$ such that

$$(2k+1)\beta$$

is as close as possible to $\pi/2$, which turns out to be

$$k = K = round\left(\frac{\pi}{4\beta} - \frac{1}{2}\right) = \left\lfloor \frac{\pi}{4\beta} \right\rfloor$$

But what is β ?

Hence, the number of iterations in STEP 1. is

$$O\left(\sqrt{N}\right)$$

But each iteration uses the Hadamard transform

$$H = \bigotimes_{0}^{n-1} H^{(2)}$$

at the computational cost of

$$\boxed{O\left(\lg N\right)}$$

Since STEP 1. is the computational dominant part of Grover's algorithm, it follows that the computational complexity of this algorithm is

$$\boxed{\boxed{O\left(\sqrt{N}\lg N\right)}}$$

The probabilty that the measurement performed in STEP 2. of Grover's algorithm will sucessfully retrieve the unkown label x_0 is given by

$$\boxed{Prob_{Success} = \sin^2\left[\left(2K+1\right)\beta\right] \geq \cos^2\beta = 1 - \frac{1}{N}}$$

Grover's Algorithm

STEP 0. (Initialization)

$$|\psi\rangle \longleftarrow H|0\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|j\rangle$$

$$k \longleftarrow 0$$

STEP 1. Loop until $k = round\left(\frac{\pi}{4\sin^{-1}\left(\frac{1}{\sqrt{N}}\right)} - \frac{1}{2}\right)$

$$\approx round\left(\frac{\pi}{4}\sqrt{N} - \frac{1}{2}\right)$$

$$|\psi\rangle \longleftarrow Q|\psi\rangle = -HI_{|0\rangle}HI_{|x_0\rangle}|\psi\rangle$$

$$k \longleftarrow k+1$$

STEP 2. Measure $|\psi\rangle$ with respect to the standard basis $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ to obtain the marked unknown state $|x_0\rangle$ with probability $\geq 1 - \frac{1}{N}$.

$$|psi\_1\rangle^T := \left[\frac{1}{4}\sqrt{2}\ \ \frac{1}{4}\sqrt{2}\ \ \frac{1}{4}\sqrt{2}\ \ \frac{1}{4}\sqrt{2}\ \ \frac{1}{4}\sqrt{2}\ \ \frac{1}{4}\sqrt{2}\ \ \frac{1}{4}\sqrt{2}\ \ \frac{1}{4}\sqrt{2}\right]$$

$$|psi\_1\rangle \text{ in ket notation} := \frac{1}{8}\sqrt{2}\,(|000\rangle + |001\rangle + |010\rangle + |011\rangle + 5\,|100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

```
> # Iteration 2: |psi_2>:= Q · |psi_1>
  #
        `|psi_2>`:=evalm( Q &* `|psi_1>`):
        print(`  `);
        `|psi_2>^T`:=transpose( `|psi_2>`);
        print(`  `);
        `|psi_2> in ket notation`:=factor( RKet(`|psi_2>`)  );
        print(`  `);
```

$$|psi\_2\rangle^T := \left[-\frac{1}{16}\sqrt{2}\ \ -\frac{1}{16}\sqrt{2}\ \ -\frac{1}{16}\sqrt{2}\ \ -\frac{1}{16}\sqrt{2}\ \ \frac{11}{16}\sqrt{2}\ \ -\frac{1}{16}\sqrt{2}\ \ -\frac{1}{16}\sqrt{2}\ \ -\frac{1}{16}\sqrt{2}\right]$$

$$|psi\_2\rangle \text{ in ket notation} := -\frac{1}{16}\sqrt{2}\,(|000\rangle + |001\rangle + |010\rangle + |011\rangle - 11\,|100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

```
> # We now exit because  K = 2, and measure the state of
  # our register.
  #
  # On measuring the state |psi_2> of our register, we obtain
  #
        Proj.4:=evalm( ket.1.0.0 &* My_Adjoint(ket.1.0.0));
        Intermediate_Result:=evalm(Proj.4 &* `|psi_2>`):
        Result:=evalm( (1/norm(Intermediate_Result,2) ) * Intermediate_Result):
        print(`  `);
        `Result^T`:=transpose(Result);
        print(`  `);
        `Result in ket notation`:=RKet(Result);
        print(`  `);
```

$$Proj4 := \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$Result^T := |0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0|$$

$$Result \text{ in ket notation} := |100\rangle$$

```
> # with probality  Prob_Success of sucess given by
  #
        Prob_Sucess:=(11/(8*sqrt(2)))^2;
        `Prob of Sucess in Floating Point`:=evalf(Prob_Sucess);
```


$$Prob\_Sucess = \frac{121}{128}$$

$$Prob \text{ of Sucess in Floating Point} = 9453125000$$

```
[ >
```