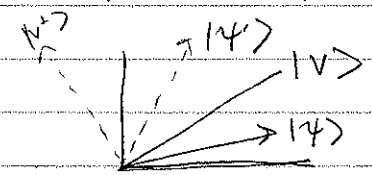
$\boxed{\text{Ph 452}}$ Lecture 14

101 Quick Review

- Gottesman-Knill Theorem
- Magic states
- Grover's algorithm: algebraic analysis

Grover's algorithm: geometric analysis

2 reflections = 1 rotation



$$|\psi\rangle = \alpha|v\rangle + \beta|v^\perp\rangle$$

$$\xrightarrow{\text{refl.}} \alpha|v\rangle - \beta|v^\perp\rangle$$

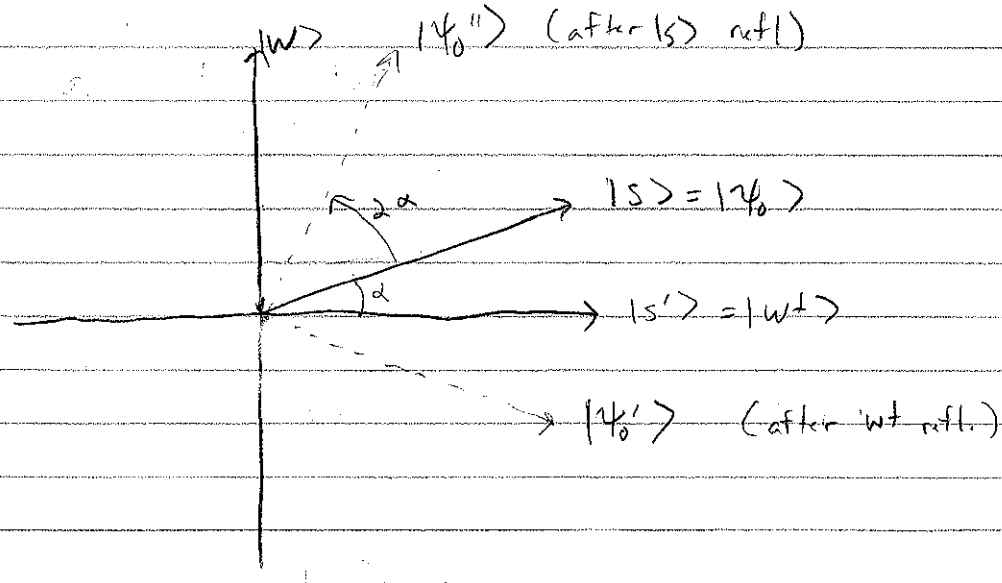
$$= \left(I - 2|v^\perp\rangle\langle v^\perp|\right)(|\psi\rangle)$$

$$= \left(2|v\rangle\langle v| - I\right)|\psi\rangle$$

Grover alg:

$$\Big[\underbrace{\overset{\text{invert}}{-}\underbrace{(I - 2|s\rangle\langle s|)}_{|s^\perp\rangle \text{ refl.}}}_{|s\rangle \text{ refl}}\underbrace{(I - 2|w\rangle\langle w|)}_{|w^\perp\rangle \text{ refl}}\Big]^k \underbrace{H^{\otimes n}|0\rangle^{\otimes n}}_{|\psi_0\rangle}$$

Note: last time I used $\cos\alpha$ for $\sin\alpha$



$\boxed{\text{Ph 432}}$ Lecture 14

$$G^k H^{\otimes n} |0\rangle^{\otimes n} = \cos((2k+1)\alpha)|s'\rangle + \sin((2k+1)\alpha)|w\rangle$$

$$\sin((2k+1)\alpha) = 1$$

$$(2k+1)\alpha = \pi/2$$

$$k = \frac{\pi}{4\alpha} - \frac{1}{2}$$

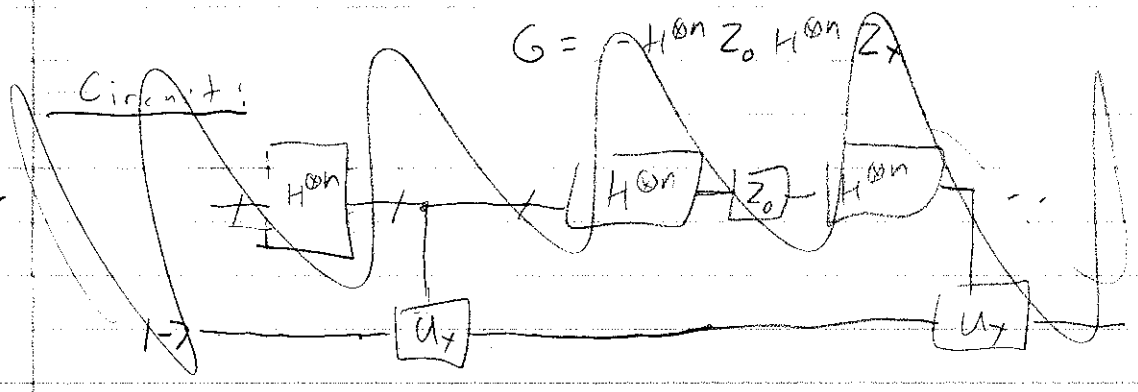
$$\alpha = \sin^{-1}\left(\sqrt{\frac{1}{N}}\right) \approx \frac{1}{\sqrt{N}}$$

$$\Rightarrow \boxed{k = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor}$$

$$G = -H^{\otimes n} Z_0 H^{\otimes n} Z_x$$

Circuit:

OMIT



PH 432 Lecture 14

Number Theory warmup

$\gcd(a,b)$ = "greatest common divisor" of $a, b \in \mathbb{N} = \{1, 2, \ldots\}$

$:= \max\{q \in \mathbb{N} \mid q \text{ divides both } a \text{ and } b \text{ without remainder}\}$

2300+ year old algorithm [Euclid's original algorithm]

Input: $a, b \in \mathbb{N}$

Output: $\gcd(a,b)$

① If $a > b$ $\quad a := a - b$

② If $b > a$ $\quad b := b - a$

③ If $a = b$ $\quad$ return a else, goto ①

n-digit number $\rightarrow$ $O(n 2^n)$ steps.

Can be sped up!

$\mathrm{Mod}(a,b) \Leftrightarrow a \bmod b$ = "remainder when dividing $a \in \mathbb{N}$ by $b \in \mathbb{N}$"

$a \equiv b \bmod c \Leftrightarrow c$ divides $a-b$ $\quad (c \mid a-b)$

"a and b have the same remainder when divided by c"

Euclidean algorithm

```
function gcd(a,b)
    if b=0, return a
    else return gcd(b, a mod b)
```

$O(n^2)$ steps (each recursive call divides input bits in half or more)

Worst-case input: Fibonacci pairs

Ph 45a Lecture 14

from NC pg. 33

5-Step factoring algorithm [Miller, 1976] (1-sided error)

Input: $N \in \mathbb{N}$ (n-digit integer)

Output: A factor a of N if N is composite (not prime)

$O(1)$ ① Check: Is N even? If yes, return $a=2$, else

NC Ex. 5.17 $O(n^3)$ ② Check: Is $N = s^t$ for integers s, t? If yes, return $a=s$, else

$O(n^6)$ exact.

$O(1)$ ③ Select $x \in \{2, \dots, N-1\}$ uniformly at random.

$O(n^2)$ Compute $y = \gcd(x, N)$.

$O(1)$ Check: Is $y > 1$? If yes, return $a = y$, else

$O(n^3)$ Quantum. ④ Compute the order of x in N, i.e., compute

$$\min \{ r \mid x^r \equiv 1 \bmod N \}.$$

$O(1)$ Check: Is r odd? If yes, return $a=1$, else (algorithm fails)

$O(n^2)$ ⑤ Compute $d = \gcd(x^{r/2} - 1, N)$.

$O(1)$ Check: Is $d > 1$? If yes, return $a = d$, else return 1. (algorithm fails)

Analysis:

$$x^r \equiv 1 \bmod N \iff N \mid x^r - 1$$

$$x^r - 1 = (x^{r/2} - 1)(x^{r/2} + 1) \quad \text{if } r \text{ is even}$$

But $N \nmid (x^{r/2} - 1)$ because r is minimum order of x in N

$\rightarrow$ Factors of N split between $(x^{r/2}+1)$, $(x^{r/2}-1)$.

If at least one factor in $(x^{r/2}-1)$, then

$\gcd(x^{r/2}-1, N)$ is a factor of N

Otherwise, $N \mid (x^{r/2}+1)$ and $\gcd(x^{r/2}-1, N) = 1$ $\rightarrow$ fails

$\gcd(x^{r/2}+1, N) = N$

Ph452 Lecture 14

Let $N = p_1^{a_1} \cdots p_k^{a_k}$

$\Pr[r \text{ is odd or } r \text{ is even and } d=1] \leq \left(\frac{1}{2}\right)^{k-1}$

$\leq \frac{1}{2}$

("This is why we had to test if $N = m^k$ because then $k=1$

[Go back and analyze runtimes of each step]

<u>Example:</u> $N=15$

① N even? No

② $N = m^k$? No

③ $y = \gcd(x, N)$ $\quad x \in \underbrace{\{2, 4, , 7, 8, 11, 13, 14\}}_{y=1} \cup \underbrace{\{3, 5, 6, 9, 10, 12\}}_{y>1}$

$y > 1$? Yes if

④ $x^r \equiv 1 \bmod N$ $\quad x^r \in \{2^4, 4^2, 7^4, 8^4, 11^2, 13^4, 14^2\}$

r odd? No,

⑤

$d = \gcd(x^{r/2} - 1, N) = \{3, 3, 3, 3, 5, 3, 1\}$

only 1/7 of possibilities cause alg to fail.

Got this far