

Recap around Grover's algorithm

given $f: \{0,1\}^n \rightarrow \{0,1\}$

- if there is unique x^* s.t. $f(x^*) = 1$:

$$(DU_f)^k H^{\otimes n} |0 \dots 0\rangle \sim |x^*\rangle \quad \text{at } k \sim \frac{\pi\sqrt{N}}{4}, N=2^n$$

$\uparrow$ phase query
 $\uparrow$ Grover's diffusion op

- if we don't know the number of x^* s.t. $f(x^*) = 1$:

random choice of $0 \leq k \leq \frac{\pi\sqrt{N}}{4}$, then

measurement of $(DU_f)^k H^{\otimes n} |0 \dots 0\rangle$ in the

$(|x\rangle)_{x \in \{0,1\}^n}$ basis gives a x^* s.t. $f(x^*) = 1$

with prob. $\sim \frac{1}{2}$

- such speed ($\sqrt{N}$ steps) is optimal for general unordered search of functions with N inputs.

Application of Grover's algorithm: OR of ANDs §23.2

Setup. $n = 2n_0$ even, $f: \underbrace{\{0,1\}^{n_0} \times \{0,1\}^{n_0}}_{N=2^n \text{ inputs}} \rightarrow \{0,1\}$

We want to find: if there is any $y \in \{0,1\}^{n_0}$ such that $f(y, x) = 1$ for all x .

i.e. $\text{OR}_{y \in \{0,1\}^{n_0}} \text{AND}_{x \in \{0,1\}^{n_0}} (f(y, x) = 1)$.

Classically: $\sim N = 2^n$ steps

- each row (y fixed) takes $\sim \sqrt{N} = 2^{n_0}$ steps to check if there is any 0 in it.

- checking all rows takes $\sim \sqrt{N}$ times this.

y	0	0	0	0
	1	1	0	0
	1	1	1	1
	0	1	0	1
	x			

One way to speedup: use Grover's algo. for each row to find if there is any 0.

(work with $1 - f(y, x)$, or phase query $(-1)^{1+f(y, x)} |x\rangle$)

cont.) then each row takes $\sim N^{\frac{1}{4}}$ steps.

with $\frac{1}{2}$ prob. of error.

repeating this k times, we get $\frac{1}{2^k}$ prob. error.

$\Rightarrow$ with $k = \log N$, each row takes $N^{\frac{1}{4}} \log N$ steps, $\sim \frac{1}{N}$ prob. error.

Then use a classical algo. to tally the results of all rows $\Rightarrow N^{\frac{3}{4}} \log N$ steps, $\frac{1}{\sqrt{N}}$ prob. error

More Speedup (Buhrman-Cleve-Wigderson '98)

Use Grover (-like) algo for both

- search of x s.t. $f(y, x) = 0$ in each row

- tallying the results of all rows

- Consider $g(y) = \bigwedge_{x \in \{0,1\}^{n_0}} f(y, x)$

- Construct an approximation of XOR query

$$U_g^{\text{XOR}} : |y\rangle \mapsto |y(z \oplus g(y))\rangle \text{ on } (\mathbb{C}^2)^{n_0+1}$$

with $\sim n_0 \sqrt{2^{n_0}}$ query to f (without measurement)

- Then use this to approx. the phase query

- Then use Grover's algo. to see if there is

y s.t. $g(y) = 1 \iff f(y, x) = 1 \text{ for all } x$

Application 2: finding collision pairs

(§ 24.1.1)

Setup : $f : \{0, \dots, N-1\} \rightarrow \{0, \dots, N-1\}$

Want to find $x, y \in \{0, \dots, N-1\}$ $x \neq y$ - $f(x) = f(y)$

Classically : "birthday attack" $\sim \sqrt{N}$ steps ($N = 2^n$)
to go through N pairs

cont.) Quantum algorithm.

- pick $k \sim \sqrt[3]{N}$ random inputs $x^0, \dots, x^{k-1}$,
compute $y^i = f(x^i)$ $0 \leq i < k$

- pick $K = k^2$ random inputs $z^0, \dots, z^{K-1}$.

Perform Grover's algorithm for finding j

$f(z^j) = y^i$ for some i

Overall: $\sqrt[3]{N} + \sqrt{K} \sim O(\sqrt[3]{N})$ queries to f

checks $\sqrt[3]{N} \times \sqrt[3]{N}^2 = N$ pairs

(enough to find a collision pair)

Application 3: element distinctness (§24.1.2)

$f: \{0, \dots, N-1\} \rightarrow \{0, \dots, N-1\}$

Want to know if f is one-to-one.

classically: N queries

Quantum also:

Step 0 split the inputs into $\sqrt{N}$ blocks.

(work with $\{0, 1\}^{n_0} \times \{0, 1\}^{n_0}$.)

Step 1 choose $y^0 \in \{0, 1\}^{n_0}$ randomly,

then query all $f(y^0, x)$ ($\sqrt{N}$ steps)

if we find a collision, we are done

Step 2 use Grover's algo. on everything else,

find z s.t. $f(z) = f(y^0, x)$ for some x

($\sqrt{N}$ steps, success prob. $\frac{1}{\sqrt{N}}$)

Step 3 treat the above as subroutine,

use "Grover's algo." to find a y^0 that will work

To justify the last part

Brassard - Høyer - Mosca - Tapp 2000,

Buhrman - Dürr - Heiligman - H. - Migniez - Santha - de Wolf
2000

Suppose $g : \{0, \dots, M-1\} \rightarrow \{0, 1\}$ is some function, A : unitary gate on $\mathbb{C}^M$ s.t. meas. of $A|0\rangle$ gives $|x\rangle$ s.t. $g(x)=1$ with prob. p . Then with $Q = A U_0 A^\dagger U_g$

U_g : phase query, $U_0 |x\rangle = \begin{cases} -|0\rangle & x=0 \\ |x\rangle & \text{otherwise} \end{cases}$

$k \sim \frac{\pi}{4\sqrt{p}}$, measurement of $Q^k A|0\rangle$ gives $|x\rangle$ s.t. $g(x)=1$ with prob. $\sim 1-p$

Grover's algorithm : $D = (H^{\otimes n}) U_0 (H^{\otimes n})^\dagger$

so we could take $A = H^{\otimes n}$.

Now : A : unitary gate implementing Steps 1 & 2.

so $p = \frac{1}{\sqrt{N}}$. $\Rightarrow k \sim \sqrt{\frac{1}{p}}$

So : overall we have $\sim \sqrt{\frac{1}{p}} \times \sqrt{N} \cdot \log N$ queries to f