Grover's Search quantum algorithm

Search problem
Let \( f : \{0,1\}^n \rightarrow \{0,1\} \).
Find an \( x \) so \( f(x) = 1 \), if there is one.

Classical algorithm: Try the different \( x \)'s one at a time \( \Rightarrow \Theta(2^n) \) calls.

Quantum algorithm:
Assume, for simplicity, that \( f(x) = 1 \) has a unique solution, \( f(a) = 1 \).
\[
|1\rangle \mapsto \left[ \begin{array}{c}
U_f \\
1 \rightarrow 1
\end{array} \right] (-1)^{f(a)} |1\rangle
\]
\[\Rightarrow|\psi_0\rangle = \sum_x (-1)^{f(x)} |x\rangle |x\rangle
\]
\[\sum_x |x\rangle \mapsto \left[ \begin{array}{c}
V_f \\
1 \rightarrow 1
\end{array} \right] \sum_x (-1)^{f(x)} |x\rangle |x\rangle
\]

General abstract quantum algorithm design paradigm:
Let \( R_1, R_2 \) be reflections (i.e., \( R_1^2 = R_2^2 = 1 \)).
Apply \( R, R_2, R, R_2, R, R_2 \ldots \) alternating reflections
(more later)

In this case, \( V_f \) is a reflection, \( V_f^2 = 1 \), \( V_f = 1 - 2 |a\rangle |\langle a|\).
Since, so far as we know, all inputs are equally likely,
we should use something symmetrical. As the symmetrical state is
\[|1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle,\]
a natural choice is to reflect about the \( n \)-dimensional subspace spanned by \( |1\rangle \), i.e., let
\[W = 2|1\rangle \langle 1| - I.\]

Algorithm:
Start in state \( |1\rangle \in \mathbb{C}^n \)
Apply \( V \)
Apply \( W \)
Apply \( V \)
Apply \( W \)

...
Analysis:
Consider the subspace spanned by $|x\rangle$ and $|\overline{x}\rangle$

\[
\begin{align*}
|\overline{x}\rangle &= \cos \theta |x\rangle + \sin \theta |\overline{x}\rangle \\
|\overline{\overline{x}}\rangle &= \cos \frac{\theta}{2} |x\rangle + \sin \frac{\theta}{2} |\overline{x}\rangle
\end{align*}
\]

The operators $V$ and $W$ both fix this subspace. Therefore the quantum computer state will always lie in this subspace.

The product $V^2 = (|x\rangle \langle x| - |\overline{x}\rangle \langle \overline{x}|)(I - 2|\overline{x}\rangle \langle x|)$ implements a rotation by angle $2\theta$

\[
\Rightarrow \text{state rotates by } 2\theta \approx \frac{\pi}{2^n} \text{ in every iteration.}
\]

After $\sim \frac{T/4}{2\sqrt{2^n}} = O(\sqrt{2^n})$ iterations, the state lies close to $|x\rangle$. Measuring in the computational basis will give $x$ with constant probability.

Implementing the algorithm:
If we have done before
the "diffusion operator" $W = 2|+\rangle \langle +| - I = 2 \left( \begin{array}{cc} 1 & 1 \\ 0 & 0 \end{array} \right)$ - \left( \begin{array}{c} 1 \\ 0 \end{array} \right)$

\[
= \prod_{n=0}^{100} \left( \begin{array}{cc} 2 & 10^n \langle 0| \end{array} \right. \end{array} \right) \left( \begin{array}{cc} 1 & \langle 0| \end{array} \right) H^\otimes n
\]
can be implemented with $O(n)$ gates, and is independent of $f$

\Rightarrow Overall complexity is $O(\sqrt{2^n})$ calls to $f$
and $O(\sqrt{2^n} n)$ total operations.
- a square-root speedup!
More generally, if there are \( M \) solutions \( a_1, \ldots, a_M \), then
\[
\psi_f = 1 - 2 \sum_{j=1}^{M} |a_j \rangle X_j |a_j \rangle.
\]

The subspace spanned by \( |a_j \rangle \)

\[\rightarrow 14 \]

The alternating reflections, by symmetry, will keep the state in the two-dimensional subspace spanned by
\[\psi_f = \frac{1}{\sqrt{2}} \sum_{x \in \{-1,1\}} |x \rangle \text{ and } 14 \psi_f = \frac{1}{\sqrt{M}} \sum_{j=1}^{M} |a_j \rangle\]

Since \( \langle 14 | \psi_f \rangle = \frac{M}{\sqrt{NM}} = \sqrt{\frac{M}{N}} \) with \( N = 2^n \), the number of steps required is only \( O\left(\frac{\sqrt{N}}{M}\right)\), (Classically \( \frac{N}{M} \) steps are needed.)

If \( M \) is unknown, then guess
\( \tilde{M} = N, \tilde{M} = N/2, \tilde{M} = N/4, \ldots, \tilde{M} = 1 \)

going down until a solution is found.

Applications of Grover's search algorithm

1. Solve \( NP \)-complete problems?
   Let \( f \) be the evaluation of a 3SAT formula, so \( f(x) = 1 \) means \( x \) is a satisfying assignment
   \( \sqrt{2^n} \) instead of \( 2^n \) steps
   (still exponential time)

2. Unsorted database search
   Let \( x \) index the items in a database, \( f(x) \) a predicate on that database entry
   Note: database needs to be stored in memory that can be accessed coherently (ie in superposition) at unit cost

3. Many other algorithms use search as a subroutine, e.g.,
   Minimum, Approx. Counting, Collision, Matriu Mult. Verification
   \( n^2 \rightarrow n^{0.88} \)
Lower bounds:

\[ \text{SAT: } f(x_1, \ldots, x_n) = c_1 \land c_2 \land \cdots \land c_m \]

Is there a satisfying assignment?

\[ \text{SAT} \leq \text{Unique-SAT} \quad \text{[Valiant, V. Vazirani]} \]

A poly(n)-time algorithm would give \( P = \text{NP} \).

A poly(n)-time quantum algorithm would give \( \text{BQP} = \text{NP} \).

**Theorem:** Let \( f \) be a black-box-accessible function either

\[ f \equiv 0 \text{ or } \exists ! a \text{ s.t. } f(a) = 1. \]

Then any quantum search algorithm must make \( \mathcal{O}(\sqrt{N}) = \mathcal{O}(2^{n/2}) \)

queries.

(no black-box exponential speedup is possible for SAT)

**Proof:** Suppose \( \psi \) solves search in \( T \)-steps.

**Calibration:** Run \( x \) on \( f \equiv 0 \).

\[ 1\phi_e > \text{state after } t \text{ queries} = \sum_{x} |x> \otimes |\phi_e > = U_t |\phi_e > \]

query register

\[ \|1\phi_e >\| = 1 \Rightarrow T + \sum_{x} \|\phi_e >\|^2 = 1 \]

Since \( \sum_{x \in [0,1]^{n}} \|\phi_e >\|^2 = T = \sum_{x \in [0,1]^{n}} \sum_{x \in [0,1]^{n}} \|\phi_e >\|^2 \]

there is some \( z \) with \( \sum_{x \in [0,1]^{n}} \|\phi_e >\|^2 \leq \frac{T}{N} \). Fix \( z \).

**Hybrid argument:** Now run \( x \) on \( f \) with \( f(x) = 1 \), \( f(z) = 0 \) \( \forall x \neq z \).

\[ 1\psi_e > \text{ state after } t \text{ queries} = U_t (\mathbb{1} - 2 I \otimes \mathbb{1} \otimes \mathbb{1}) |\psi_e > \]

\[ 1\psi_e > = 1\phi_e > \]

\[ 1\phi_e > = U_1 (\mathbb{1} - 2 I \otimes \mathbb{1} \otimes \mathbb{1}) |\psi_e > \]

\[ = U_1 |\phi_e > - 2 I \otimes \mathbb{1} \otimes \mathbb{1} |\psi_e > \]

\[ = |\phi_e > + 1\mathbb{E}_f > \]

\[ 1\psi_e > = U_2 (\mathbb{1} - 2 I \otimes \mathbb{1} \otimes \mathbb{1}) |\psi_e > \]

\[ = U_2 |\phi_e > - 2 I \otimes \mathbb{1} \otimes \mathbb{1} > + U_2 (\mathbb{1} - 2 I \otimes \mathbb{1} \otimes \mathbb{1}) |\mathbb{E}_f > \]

\[ = |\phi_e > + 1\mathbb{E}_f > + 1\mathbb{E}_f > + \cdots + 1\mathbb{E}_f > \]

\[ \Rightarrow \|1\psi_e > - |\phi_e >\| \leq \sum_{e \in [0,1]^{n}} \|1\mathbb{E}_f >\| \leq 2 \sum_{g \in [0,1]^{n}} \|1\mathbb{E}_f >\| \]

\[ \leq 2 T \left( \sum_{g \in [0,1]^{n}} \|1\mathbb{E}_f >\|^2 \right)^{1/2} \text{ by Cauchy-Schwarz} \]

\[ \leq 2 \left( \frac{T}{N} \right)^{1/2} \Rightarrow T = \mathcal{O}(\sqrt{N}) \]