A further analysis of the amplitude amplification algorithm
Query complexity: expected value and variance

Philippe Lamontagne

June 18, 2012
This talk is about amplitude amplification:

- the algorithm;
- previous analysis;
- new analysis.
The problem

Given: \( f : \{0, \ldots, N-1\} \rightarrow \{0, 1\} \).
Goal: find any \( x \) such that \( f(x) = 1 \).
The problem

Given: $f : \{0, \ldots, N - 1\} \rightarrow \{0, 1\}$.
Goal: find any $x$ such that $f(x) = 1$.

Very general setting in computer science:
- all NP-complete problems fit this form;
- optimization: feasibility problem;
- equivalent with function problems (learn $y = g(x)$ by searching $(x, y)$ such that $g(x) = y$).
Quadratic speed-up

Hardest: $f$ is black-box.

- classical: $O(N/t)$
- quantum (Grover): apply operator $G = -HS_f HS_0$ a number of times in $O(\sqrt{N/t})$. 

Suppose $\exists$ classical algorithm $A$ finds $x$ with known probability $a$.

- classical: $O(1/a)$ applications of $A$
- quantum (Ampl. Amplification): apply operator $Q = -AS_f AS_0$ a number of times in $O(\sqrt{1/a})$.
Hardest: \( f \) is black-box.

- classical: \( O(N/t) \)
- quantum (Grover): apply operator \( G = -HS_f HS_0 \) a number of times in \( O(\sqrt{N/t}) \).

Suppose \( \exists \) classical algorithm \( A \) finds \( x \) with known probability \( a \).

- classical: \( O(1/a) \) applications of \( A \)
- quantum (Ampl. Amplification): apply operator \( Q = -AS_f AS_0 \) a number of times in \( O(\sqrt{1/a}) \)
Algorithm $QSearch(f, A, c)$ for $1 < c < 2$:

1. Set $\ell = 0$.
2. $\ell \leftarrow \ell + 1$ and $M \leftarrow \lceil c^{\ell} \rceil$.
3. Pick $j \in_R \{1, \ldots, M\}$
4. Apply $Q^j$ to the state $A|0\rangle$, measure and get $|x\rangle$.
5. If $f(x) = 1$ stop. Otherwise, go to step 2.

The probability of measuring a good solution at step 4 is $\sin^2((2j + 1)\theta)$ where $\theta$ is defined so that $\sin^2(\theta) = a$. 
Success probability

Figure: $\sin^2((2j + 1)\theta)$
Success probability

Figure: \[ P_M = \frac{1}{2} - \frac{\sin(4M\theta)}{4M \sin(2\theta)} \]
Suppose $c < 4/3$. Let $M_0 = 1/ \sin(2\theta)$. 
Suppose $c < 4/3$. Let $M_0 = 1/\sin(2\theta)$. When $M \geq M_0$, we fail with prob. at most $3/4$. 

Hence $E[X] \leq K + \sum_{i \geq 0} M_0 \cdot (\frac{3}{4})^i \in O(\sqrt{1/a})$. So $E[X] \in O(\sqrt{1/a})$. 

Philippe Lamontagne
A further analysis of the amplitude amplification algorithm
Suppose $c < 4/3$. Let $M_0 = 1/\sin(2\theta)$.
When $M \geq M_0$, we fail with prob. at most $3/4$.
So, $M \geq M_0 c^i$ with probability at most $(\frac{3}{4})^i$.
Suppose $c < 4/3$. Let $M_0 = 1/ \sin(2\theta)$.

When $M \geq M_0$, we fail with prob. at most $3/4$.

So, $M \geq M_0 c^i$ with probability at most $(\frac{3}{4})^i$. Hence

$$E[X] \leq K + \sum_{i \geq 0} M_0 \cdot (c \frac{3}{4})^i \in O(M_0)$$

since $c \frac{3}{4} < 1$. 
Suppose \( c < 4/3 \). Let \( M_0 = 1/\sin(2\theta) \).

When \( M \geq M_0 \), we fail with prob. at most \( 3/4 \).

So, \( M \geq M_0 c^i \) with probability at most \((3/4)^i\). Hence

\[
E[X] \leq K + \sum_{i \geq 0} M_0 \cdot \left(c^{3/4}\right)^i \in O(M_0)
\]

since \( c^{3/4} < 1 \).

So \( E[X] \in O(M_0) = O(\sqrt{1/a}) \).
What about variance?

**Theorem**

The variance of the number of queries made by the amplitude amplification algorithm is unbounded for $c > \sqrt{2}$.
What about variance?

**Theorem**

The variance of the number of queries made by the amplitude amplification algorithm is unbounded for $c > \sqrt{2}$.

**proof sketch.**

There exists $M_0$ such that $1/2 > 1 - P_{M_0} > 1/c^2$. 
What about variance?

**Theorem**

The variance of the number of queries made by the amplitude amplification algorithm is unbounded for $c > \sqrt{2}$.

**proof sketch.**

There exists $M_0$ such that $1/2 > 1 - P_{M_0} > 1/c^2$. The probability that $M \geq M_0 c^i$ is at least $\delta (1 - P_{M_0})^i$ where $\delta$ is the probability that $M \geq M_0$. 

$\text{Var}[X] \geq \delta M_0^2 \sum_i (1 - P_{M_0})^i$

This series is divergent since $(1 - P_{M_0})^i > 1$. 

Philippe Lamontagne
A further analysis of the amplitude amplification algorithm
What about variance?

**Theorem**

The variance of the number of queries made by the amplitude amplification algorithm is unbounded for \( c > \sqrt{2} \).

**proof sketch.**

There exists \( M_0 \) such that \( 1/2 > 1 - P_{M_0} > 1/c^2 \). The prob. that \( M \geq M_0 c^i \) is at least \( \delta (1 - P_{M_0})^i \) where \( \delta \) is the prob. that \( M \geq M_0 \).

\[
\text{Var}[X] \geq \delta M_0^2 \sum_{i \geq 0} (1 - P_{M_0})^i c^{2i}
\]
What about variance?

Theorem

The variance of the number of queries made by the amplitude amplification algorithm is unbounded for $c > \sqrt{2}$.

proof sketch.

There exists $M_0$ such that $1/2 > 1 - P_{M_0} > 1/c^2$. The prob. that $M \geq M_0 c^i$ is at least $\delta (1 - P_{M_0})^i$ where $\delta$ is the prob. that $M \geq M_0$.

$$Var[X] \geq \delta M_0^2 \sum_{i \geq 0} (1 - P_{M_0})^i c^{2i}$$

This series is divergent since $(1 - P_{M_0})c^2 > 1$. 
Finite for some values of $c$

**Theorem**

*The variance is finite for $1 < c < 1.193936$.***
### Theorem

The variance is finite for $1 < c < 1.193936$.

### Proof.

Let $c_0 = 1 - c/2$ and let $M_0 = 1/(2c_0\sqrt{a})$. 

The variance is finite for $1 < c < 1.193936$.

**Proof.**

Let $c_0 = 1 - c/2$ and let $M_0 = 1/(2c_0\sqrt{a})$. For $M \geq M_0$, we will have $M \geq M_0c^i$ with probability at most $p_0^i$ where

$$p_0 = \frac{1}{2} + \frac{1}{4M_0\sqrt{a}} = \frac{1}{2}(1 + c_0).$$
The variance is finite for $1 < c < 1.193936$. 

Proof.

Let $c_0 = 1 - c/2$ and let $M_0 = 1/(2c_0\sqrt{a})$. For $M \geq M_0$, we will have $M \geq M_0 c^i$ with probability at most $p_0^i$ where

$$p_0 = \frac{1}{2} + \frac{1}{4M_0\sqrt{a}} = \frac{1}{2}(1 + c_0).$$

Hence the variance can be upper bounded by $\sum_{i \geq 0} M_0^2(c^2 p_0)^i$. 
Theorem

The variance is finite for \( 1 < c < 1.193936 \).

Proof.

Let \( c_0 = 1 - c/2 \) and let \( M_0 = 1/(2c_0 \sqrt{a}) \). For \( M \geq M_0 \), we will have \( M \geq M_0 c^i \) with probability at most \( p_0^i \) where

\[
p_0 = \frac{1}{2} + \frac{1}{4M_0 \sqrt{a}} = \frac{1}{2} (1 + c_0).
\]

Hence the variance can be upper bounded by \( \sum_{i \geq 0} M_0^2 (c^2 p_0)^i \). This series converges when \( c^2 p_0 < 1 \), that is, when \( 1 < c < 1.193936 \).
What about the gap?

Philippe Lamontagne
A further analysis of the amplitude amplification algorithm

Computed by Wolfram|Alpha
Which $c$ to choose?

Why not just chose $c$ in the finite region?
Why not just chose \( c \) in the finite region?

- \( c \rightarrow 1 \implies \text{quantum} \rightarrow \text{classical} \);
Which $c$ to choose?

Why not just chose $c$ in the finite region?

- $c \to 1 \implies$ quantum $\to$ classical;
- $c \to 2 \implies$ $E[X] \to \infty$. 

Philippe Lamontagne

A further analysis of the amplitude amplification algorithm
Figure: Expected value as a function of $c$
Some ideas to reduce variance:

- First compute an estimate for $a$ using amplitude estimation with accuracy $\epsilon$. Get $\tilde{a} \in [(1 - \epsilon)a, (1 + \epsilon)a]$. Apply $Q^j$ for $j \in O(\tilde{a})$.
- Compute a very rough estimate of $a$ and repeatedly apply $Q^j$ for $j$ picked uniformly between 1 and $M \approx O(1/\sqrt{a})$. 
Further work

- Formalize the previous ideas.
- How to reduce the gap between values of $c$ with finite variance and those with infinite variance?
- What would be the optimal value for $c$ in terms of expected value?
The end.

Thank you! Merci!