# NOTES ON AMPLITUDE AMPLIFICATION

MATTHEW MOORE

**The Problem.** Suppose that we are given the following.

- $\mathcal{A}$, a quantum circuit using no measurements.
- $|\texttt{start}\rangle$ and $|\texttt{end}\rangle$, quantum states with $\mathcal{A}\,|\texttt{start}\rangle = |\texttt{end}\rangle$.
- $|\texttt{end}\rangle = |A\rangle + |B\rangle$ with $\langle A \mid B\rangle = 0$, $\langle A \mid A\rangle = a$, and $\langle B \mid B\rangle = b = 1 - a$.

Let us consider $|A\rangle$ as a superposition of all "correct" outcomes of algorithm $\mathcal{A}$. Upon measuring $|\texttt{end}\rangle$, the probability of observing $|A\rangle$ is $a$. We would like a procedure to increase the probability of observing $|A\rangle$.

We assume that we have a basis $(\psi_i)_{i\in I}$ such that $I = A \cup B$ and a function $\chi : I \to \{0,1\}$ such that $\chi(A) = 1$ and $\chi(B) = 0$. Define

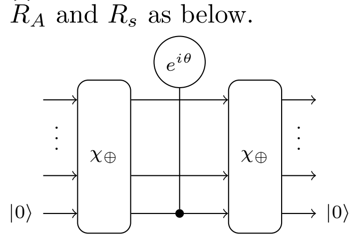
$$|\Psi(\alpha,\beta)\rangle = \alpha\,|A\rangle + \beta\,|B\rangle$$

and note that $|\Psi(1,1)\rangle = |\texttt{end}\rangle$.

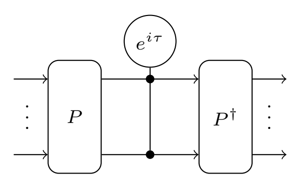
## A solution

Let $P$ be a permutation matrix such that $P\,|\texttt{start}\rangle = |1\cdots 1\rangle$ and define quantum circuits $\widehat{R}_A$ and $R_s$ as below.

$\widehat{R}_A =$




$\widehat{R}_{\mathtt{s}} =$




Define operators

$$R_A = \frac{e^{i\theta}-1}{a}\,|A\rangle\,\langle A| + I, \qquad R_{\mathtt{s}} = (e^{i\tau}-1)\,|\texttt{start}\rangle\,\langle\texttt{start}| + I$$

and note that $R_A\,|\Psi(\alpha,\beta)\rangle = \left|\Psi(e^{i\theta}\alpha,\beta)\right\rangle$. Finally, define $\mathcal{G} = -\mathcal{A}\circ R_{\mathtt{s}}\circ\mathcal{A}^\dagger\circ R_A$.

**Lemma 1.** *$\widehat{R}_A$ computes $R_A$ using 1 ancilla and $\widehat{R}_s$ computes $R_s$.*

**Lemma 2.**

$$\mathcal{G}\,|\Psi(\alpha,\beta)\rangle = -\left|\Psi\Big(\big(ae^{i\tau}+b\big)e^{i\theta}\alpha + \big(e^{i\tau}-1\big)b\beta,\ \big(e^{i\tau}-1\big)e^{i\theta}a\alpha + \big(be^{i\tau}+a\big)\beta\Big)\right\rangle.$$

**Theorem 3.** *Suppose that $\mathcal{A}$ acting on $|\texttt{start}\rangle$ produces correct answers with probability $a \in (0,1)$. The circuit $\mathcal{G}\circ\mathcal{A}$ acting on $|\texttt{start}\rangle$ is exact if and only if $\theta = \tau = \arccos(1 - 1/(2a))$ and $a \in [1/4, 1)$.*

---

*Date*: March 29, 2020.

*Proof.* From Lemma 2, we have

$$\mathcal{G}\,|\Psi(1,1)\rangle = -\Big|\Psi\Big(\big(ae^{i\tau}+b\big)e^{i\theta}+\big(e^{i\tau}-1\big)b,\ \big(e^{i\tau}-1\big)e^{i\theta}a+be^{i\tau}+a\Big)\Big\rangle$$

The probability of observing an incorrect answer when this state is measured is

$$b\big((e^{i\tau}-1)e^{i\theta}a+be^{i\tau}+a\big)^2.$$

$\mathcal{G}\circ\mathcal{A}$ is exact if and only if this quantity is equal to 0. Setting it equal to 0 and solving for $e^{i\theta}$ and $e^{i\tau}$ (we assume $a,b\neq 0$) yields

$$e^{i\theta} = \frac{be^{i\tau}+a}{a(1-e^{i\tau})} = \frac{a-b}{2a}+\left(\frac{\sin(\tau)}{2a(1-\cos(\tau))}\right)i \qquad \text{and}$$
$$e^{i\tau} = \frac{(e^{i\theta}-1)a}{ae^{i\theta}+b} = \frac{a(a-b)(1-\cos(\theta))}{a^2+2ab\cos(\theta)+b^2}+\left(\frac{a\sin(\theta)}{a^2+2ab\cos(\theta)+b^2}\right)i.$$

Equivalently,

$$\cos(\theta) = \frac{a-b}{2a}, \qquad \sin(\theta) = \frac{\sin(\tau)}{2a(1-\cos(\tau))},$$
$$\cos(\tau) = \frac{a(a-b)(1-\cos(\theta))}{a^2+2ab\cos(\theta)+b^2}, \qquad \sin(\tau) = \frac{a\sin(\theta)}{a^2+2ab\cos(\theta)+b^2}.$$

Focusing on $\cos(\theta)$, using $b=1-a$ this implies that $a\in(1/4,1)$. Substituting the expression for $\cos(\theta)$ into the one for $\cos(\tau)$ yields

$$\cos(\tau) = \frac{(1/2)(a-b)^2}{a^2+b(a-b)+b^2} = \frac{a-b}{2a} = \cos(\theta).$$

Substituting $\cos(\tau)=(a-b)/(2a)$ into the expression for $\sin(\theta)$ yields

$$\sin(\theta) = \frac{\sin(\tau)}{2a-a+b} = \sin(\tau).$$

It follows from these that $\theta=\tau=\arccos(1-1/(2a))$. All of the manipulations done were reversible, and equivalent to $\mathcal{G}\circ\mathcal{A}$ being exact, establishing the claimed equivalence. □

**Theorem 4.** *Let $\theta=\tau=\pi$. Then*

$$G^k\,|\Psi(1,1)\rangle = \left|\Psi\left(\frac{1}{\sqrt{a}}\sin\big((2k+1)\gamma\big),\ \frac{1}{\sqrt{b}}\cos\big((2k+1)\gamma\big)\right)\right\rangle$$

*where $\gamma$ is such that $e^{i\gamma}=\sqrt{b}+i\sqrt{a}$.*

*Proof.* Define sequences $(\alpha_k)_{k\in\mathbb{N}}$ and $(\beta_k)_{k\in\mathbb{N}}$ by

$$G^k\,|\Psi(1,1)\rangle = |\Psi(\alpha_k,\beta_k)\rangle\,.$$

From Lemma 2, these sequences are also defined recursively by

$$\alpha_k = (b-a)\alpha_{k-1}+2b\beta_{k-1}, \qquad \alpha_0 = 1,$$
$$\beta_k = -2a\alpha_{k-1}+(b-a)\beta_{k-1}, \qquad \beta_0 = 1.$$

This is a linear homogeneous recurrence, and its equivalent matrix form is

$$\begin{pmatrix}\alpha_k\\ \beta_k\end{pmatrix} = \begin{pmatrix}b-a & 2b\\ -2a & b-a\end{pmatrix}\begin{pmatrix}\alpha_{k-1}\\ \beta_{k-1}\end{pmatrix} = \begin{pmatrix}b-a & 2b\\ -2a & b-a\end{pmatrix}^k\begin{pmatrix}1\\ 1\end{pmatrix}.$$

Let $M$ be the matrix. $M$ diagonalizes as $M = PDP^{-1}$ where

$$D = \begin{pmatrix} \overline{\lambda}^2 & 0 \\ 0 & \lambda^2 \end{pmatrix}, \qquad P = \frac{1}{\sqrt{a}} \begin{pmatrix} i\sqrt{b} & -i\sqrt{b} \\ \sqrt{a} & \sqrt{a} \end{pmatrix}, \qquad P^{-1} = \frac{1}{2\sqrt{b}} \begin{pmatrix} -i\sqrt{a} & \sqrt{b} \\ i\sqrt{a} & \sqrt{b} \end{pmatrix}$$

for $\lambda = e^{i\gamma} = \sqrt{b} + i\sqrt{b}$. We have

$$\begin{pmatrix} \alpha_k \\ \beta_k \end{pmatrix} = PD^kP^{-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2\sqrt{b}} PD^k \begin{pmatrix} \overline{\lambda} \\ \lambda \end{pmatrix} = \frac{1}{2\sqrt{b}} P \begin{pmatrix} \overline{\lambda}^{2k+1} \\ \lambda^{2k+1} \end{pmatrix}$$

$$= \frac{1}{2\sqrt{ab}} \begin{pmatrix} i\sqrt{b}\left(\overline{\lambda}^{2k+1} - \lambda^{2k+1}\right) \\ \sqrt{a}\left(\overline{\lambda}^{2k+1} + \lambda^{2k+1}\right) \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{a}} \sin\left((2k+1)\gamma\right) \\ \frac{1}{\sqrt{b}} \cos\left((2k+1)\gamma\right) \end{pmatrix}. \qquad \square$$

**Corollary 5.** *Let* $m = \lfloor \pi/(4\gamma) \rfloor$ *where* $\sin(\gamma) = \sqrt{a}$. *If* $a \to 0$ *as* $n \to \infty$ *then* $\mathcal{G}^k \circ \mathcal{A}$ *produces correct answers with* $\Theta(1/\sqrt{a})$ *iterations of* $\mathcal{A}$ *and* $\mathcal{A}^\dagger$.

*Proof.* From Theorem 4, the circuit $\mathcal{G}^k \circ \mathcal{A}$ acting on $|\texttt{start}\rangle$ produces correct answers with probability $\sin((2k+1)\gamma)^2$. We have

$$\sin\left((2k+1)\gamma\right) \geq \sin\left(\left(\frac{\pi}{2\gamma} - 1\right)\gamma\right) = \sin\left(\frac{\pi}{2} - \gamma\right) = \cos(\gamma).$$

It follows that $\sin\left((2k+1)\gamma\right)^2 \geq b = 1 - a$.

Hence the probability that a correct answer is observed when $\mathcal{G}^k \circ \mathcal{A}\,|\texttt{start}\rangle$ is measured is at least $1 - a$, and after $1/(1-a)$ iterations we can expect to have measured a correct answer. The number of calls to $\mathcal{A}$ and $\mathcal{A}^\dagger$ after $1/(1-a)$ iterations of $\mathcal{G}^k \circ \mathcal{A}$ is $(2k+1)/(1-a)$. As $a \to 0$, we have $1 - a \to 1$ and $\gamma \to \sqrt{a}$ (since $\sin(\gamma) = \sqrt{a}$). Hence $(2k+1)/(1-a) \to \pi/(2\sqrt{a}) + 1$, so the number of iterations of $\mathcal{A}$ and $\mathcal{A}^\dagger$ is in $\Theta(1/\sqrt{a})$. $\square$