Electronic Colloquium on Computational Complexity, Revision 2 of Report No. 151 (2014)

# Amplitude Amplification for Operator Identification and Randomized Classes

Debajyoti Bera[1]

Indraprastha Institute of Information Technology-Delhi (IIIT-D), India
dbera@iiitd.ac.in

**Abstract.** Amplitude amplification (AA) is tool of choice for quantum algorithm designers to increase the success probability of query algorithms that reads its input in the form of oracle gates. Geometrically speaking, the technique can be understood as rotation in a specific two-dimensional space. We study and use a generalized form of this rotation operator to design algorithms in a geometric manner.Specifically, we apply AA to algorithms that take their input in the form of input states and in which rotations with different angles and directions are used in a unified manner. We show that AA can be used to sequentially discriminate between two unitary operators, both without error and with bounded-error, in an asymptotically optimal manner. We also show how to reduce error probability in one and two-sided bounded error algorithms more efficiently than the usual parallel repetitions technique; in particular, errors can be completely eliminated from the exact error algorithms.

## 1 Introduction

*Amplitude amplification* (AA) is the engine that powers the "unordered quantum search" algorithm proposed by L. Grover in 1996 [1]. A lot of efficient quantum algorithms essentially ride this horse in some way or the other [2–5] and one wonders how much more can this idea deliver. It is now routine to apply AA for boosting the success probability of quantum algorithms. One reason behind this unmatched popularity is the black-box manner in which this technique can be applied. *Suppose $\mathcal{A}$ is a quantum algorithm without any intermediate measurement such that after measuring the output of $\mathcal{A}|00\ldots0\rangle$, we obtain a solution to $\mathcal{A}$ that may be "good" with some probability, say $p$. Then AA can be applied to $\mathcal{A}$ to generate an algorithm $Q$ that basically calls $\mathcal{A}$ (and $\mathcal{A}^\dagger$) as black-boxes in an iterative manner.* Temptation to use AA becomes stronger due to the uniform nature of $Q$: $\mathcal{A}$ and $\mathcal{A}^\dagger$ are used as black-box here and the input state to $\mathcal{A}$ as well as the measurement operators at the end remain unchanged (maybe, extended). Therefore, it makes sense to apply this technique to a family of $\mathcal{A}$, e.g., to $\{\mathcal{A}_x\}_{x\in\{0,1\}^*}$ in which $\mathcal{A}_x$ uses an oracle gate to read bits of input string $x$. This is why AA has so far been applied in the query-complexity model in which $\mathcal{A}$ can read the "input" by making oracle queries.

The second reason behind the popularity of AA is the square-root promise that *the amplification algorithm $Q$ makes $O(\sqrt{p})$ calls to $A$ (and $A^\dagger$) and can*

ISSN 1433-8092

*guarantee a good solution with high probability*; this is in contrast to classical techniques that require $O(p)$ calls to $A$. There are also several improvements to workaround the requirement of knowing $p$ beforehand [6, 7].

This work is motivated by two other observations about AA. Amplitude amplification requires use of a diffusion operator that essentially depends upon the input state of the algorithm $\mathcal{A}$. Therefore, it is worth investigating if, and when, can amplitude amplification be applied to non-query algorithms, i.e., algorithms in which the input is supplied in the form of an input state. In this setting, we have a family of input states instead of a family of algorithms and therefore, we no longer have a uniform amplification circuit for different input states. We find that AA works in general, but with a subtlety for communication protocols.

Amplitude amplification can also be viewed as a rotation in a particular 2-dimensional space. Our second observation is that it is possible to mix-match rotations in different directions and by different angles but in a uniform manner across different instances – this we call as "differential amplification". This is an extension of the idea present in the original search algorithm by Grover that if $\mathcal{A}$ has no solution, then the amplified algorithm too will produce no solution — geometrically, the same amplification routine rotated different states differently.

*Contribution: Sequential operator discrimination [Section 3].* A common manner of differentiating between output distributions of algorithms is to run them in parallel and statistically analyse the aggregate of the outcomes [8, 9]. Differential amplification can be seen as a sequential technique for the same purpose. For instance, a recently proposed fault detection method for quantum circuits uses a classical repeated sampling of the output of a quantum circuit to distinguish between several output distributions, one for each type of faulty circuit [10]. Our technique can be used to replace the classical repetition by quantum amplification and we show a limited form of this in this work. Specifically, we design both exact and bounded-error sequential algorithms for discriminating between two unitary operators (given as black-box) without using any special input state for the operators, whereas, the existing parallel and sequential methods require preparation of a specific "optimum" state [9, 11]. Moreover, if the optimum state is used, then our algorithm makes at most additional call compared to the optimum. In this process we also strengthen and generalize some known upper and lower bounds on sequential and parallel discrimination algorithms.

*Contribution: Sequential amplification of bounded-error algorithms [Section 4].* Quantum algorithms that operate in the non-query mode, i.e., take input in the form of input states, appear sidelined in the crowd of quantum query algorithms. However, important problems like "Factoring" and "Discrete-logarithm" with eye-catching quantum algorithms, belong to the non-query **BQP** class. The current technique for boosting the success probability of **RQP** (one-sided error) and **BQP** (two-sided error) is by parallely and independently running the original algorithm [8, Ch. 6],[12]. We use differential amplification for reducing error of bounded-error algorithms faster compared to the parallel ones. We also show that one-sided and two-sided "exact" error quantum classes (**ERQP** and **EBQP**) can be improved to be included in **EQP**, thus making **EQP** = **ERQP** = **EBQP**.

## 2 Grover Iterator Revisited

Brassard et al. [6] formalized the key technique of Grover's search algorithm as amplitude amplification (AA) and showed its use in general search problems. AA involves repeated application of an operator commonly known as the Grover iterator $G$. Traditionally $G$ has been defined based on a quantum (oracle) algorithm $\mathcal{A}$ that on input $|00\dots0\rangle$ searches a state space and outputs a superposition $|\Psi\rangle$ of "good" and "bad" solution states (in the standard basis) of some search problem (say, searching for 1 in an unordered array). Another operator $U_{\Psi_0} = (I - 2\sum_{x:good}|x\rangle\langle x|)$ is used to identify "good" solution states. Then, $G$ is constructed as $G = -A(I - 2|00\dots0\rangle\langle00\dots0|)A^\dagger U_{\Psi_0} = (2|\Psi\rangle\langle\Psi| - I)U_{\Psi_0}$.

Soon after Grover proposed his quantum search algorithm, researchers observed that his algorithm, and the underlying amplitude amplification technique, has an elegant geometric interpretation of a rotation in a 2-dimensional state. Several extensions to Grover's search rely on this geometric interpretation, e.g., the generalization of Grover's search to handle arbitrary initial states [13, 14]. The algorithms that we study are not search algorithms and we want to mix-and-match more than one generalizations of $G$. Even though such generalized Grover's iterator has been analyzed in the context of unordered quantum search [13, 14], we did not find any independent characterization suitable for us.

Given a state $|\Psi\rangle$ and a two-outcome projective measurement $\mathbf{P} = \langle P^0, P^1\rangle$, we study the following operator family for any pair of angles $0 \le a, b < 2\pi$:

$$G_{a,b} = [(1 - e^{ia})|\Psi\rangle\langle\Psi| - I] \cdot [I - (1 - e^{ib})P^1]$$

It is easy to show that $G_{a,b}$ is a unitary operator for any $a, b$. These operators were used to amplify query algorithms in which they are applied to rotate certain types of states that are related to $|\Psi\rangle$ and $P^1$ [6, 13, 14]. Our motivation was to characterize the transformation and which all states can this be applied on.

Define angle $\theta \in [0, \pi/2]$ and orthogonal states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ such that $P^0|\Psi\rangle = \cos\theta|\Psi_0\rangle$ and $P^1|\Psi\rangle = \sin\theta|\Psi_1\rangle$. Observe that $\sin^2\theta$ is the probability of observing outcome $P^1$ when $|\Psi\rangle$ is measured using $\mathbf{P}$. Denote the Hilbert space spanned by $|\Psi_0\rangle$ and $|\Psi_1\rangle$ by $\mathcal{H}$. If $P^0|\Psi\rangle = 0$ or $P^1|\Psi\rangle = 0$, then $\mathcal{H}$ is 1-dimensional, essentially spanned by $|\Psi\rangle$. In that case $G_{a,b} \overset{\varphi}{\simeq} I$; we use the notation $U \overset{\varphi}{\simeq} V$ to indicate that the two operators $U$ and $V$ are identical, except maybe for different global phases. So, henceforth, we will only consider the cases when $P^0|\Psi\rangle \neq 0 \neq P^1|\Psi\rangle$, and in that case, $\mathcal{H}$ is 2-dimensional.

We will use $CP_\rho$ to denote the conditional phase-change unitary operator $P^0 + e^{i\rho}P^1$. Observe that $CP_\rho \overset{\varphi}{\simeq} I$ if $\mathcal{H}$ is one-dimensional. We will use $R_x$ to denote rotation by angle $x$ in $\mathcal{H}$ in the anti-clockwise direction from $|\Psi_0\rangle$ to $|\Psi_1\rangle$.

The following theorem shows how to implement rotations in $\mathcal{H}$ and can be proved by observing the action of $G$ and $CP_\rho$ on two-dimensional $\mathcal{H}$ [15].

**Theorem 1.** *Given a state $|\Psi\rangle$ and a two-outcome projective measurement $\langle P^0, P^1\rangle$, let $\mathcal{H}$ be the space spanned by $P^0|\Psi\rangle$ and $P^1|\Psi\rangle$ and let $(|\Psi_0\rangle, |\Psi_1\rangle)$ be a basis of $\mathcal{H}$ such that $\langle\Psi_0|P^0|\Psi\rangle = \cos\theta$ and $\langle\Psi_1|P^1|\Psi\rangle = \sin\theta$ for some $\theta \in [0, \pi/2]$. Let $R_\alpha$ denote rotation by angle $\alpha$ in $\mathcal{H}$ from $|\Psi_0\rangle$ towards $|\Psi_1\rangle$.*

*Suppose $\mathcal{H}$ is two-dimensional. For any $0 \leq \theta' \leq 2\theta$, there exists angles $\rho, a, b \in [0, 2\pi]$ such that $R_{\theta'} \overset{\varphi}{\simeq} CP_\rho \cdot G_{a,b} \cdot CP_\rho^\dagger$. In particular, $R_{2\theta} = G_{\pi,\pi} = [2|\Psi\rangle\langle\Psi| - I] \cdot [I - 2P^1]$.*

*If $\mathcal{H}$ is one-dimensional then $G_{\pi,\pi} \overset{\varphi}{\simeq} I$ and $CP_\rho \cdot G_{a,b} \cdot CP_\rho^\dagger \overset{\varphi}{\simeq} I$ for any $\rho, a, b$.*

For any angle $\delta \in [0, \pi/2]$, $R_\delta$ can be implemented as $R_{\theta'} R_{2\theta}^k$ in which $k$ is the largest integer such that $\delta = k \cdot 2\theta + \theta'$. The above theorem allows us to rotate *any* state in $\mathcal{H}$ by any angle and may be of independent interest.

**Corollary 1.** *Let $|\Phi\rangle$ denote some state in $\mathcal{H}$ of the form $\cos\phi|\Psi_0\rangle + \sin\phi|\Psi_1\rangle$ for some $\phi \in [0, \pi/2]$ and let $\delta$ be some angle. Then, $\cos(\delta+\phi)|\Psi_0\rangle + \sin(\delta+\phi)|\Psi_1\rangle$ can be obtained by executing $R_\delta|\Phi\rangle \overset{\varphi}{\simeq} CP_\rho G_{a,b} CP_\rho^\dagger G_{\pi,\pi}^k |\Phi\rangle$ for some angles $\rho, a, b$ depending on $\delta$,$\theta$ and $k = \lfloor \frac{\delta}{2\theta} \rfloor$.*

In particular, let $|\chi\rangle = \cos x|\Psi_0\rangle + \sin x|\Psi_1\rangle$ be some other state in $\mathcal{H}$. Define project measurement operators $\mathcal{P} = \langle P'^0 = I - |\chi\rangle\langle\chi|, P'^1 = |\chi\rangle\langle\chi|\rangle$. Then there exists $\rho, a, b, k$ such that $\|P'^1 CP_\rho G_{a,b} CP_\rho^\dagger G_{\pi,\pi}^k |\Phi\rangle\|^2 = \|P'^1 R_{x-\phi}|\Phi\rangle\|^2 = \sin^2 x$.

Simpler rotation operators can surely be constructed for any Hilbert space. However, we shall see in the next two sections that the particular construction of $R_\delta$ allows us to *differentially amplify* different states in different manners.

## 3 Unitary Operator Discrimination

In the unitary operator discrimination problem, we are given a unitary operator $U \in \{U_1, U_2\}$ as a black-box with equal chance of picking either of the operators. The goal is to identify $U$. Let $\omega(U)$, for any unitary operator $U$, denote the angle of the smallest arc containing all the eigenvalues of $U$ (on the unit circle). Let $\omega$ represent $\omega(U_1^\dagger U_2)$. It is known that $\frac{1}{2}(1 - \sin\frac{\omega}{2})$ is the minimum probability of error to discriminate between $U_1$ and $U_2$ by making only one call to $U$ on an *appropriate input state* and using an appropriate measurement operator [9, 11]. Thus, if $\omega \geq \pi$ then there exists a $|\gamma\rangle$ such that $U_1|\gamma\rangle$ and $U_2|\gamma\rangle$ are orthonormal and therefore, can be *perfectly distinguished*.

On the other hand, if $\omega < \pi$, then the optimal methods for exact discrimination require $k = \lceil \frac{\pi}{\omega} \rceil$ calls to $U$ on a bespoken input state followed by a measurement in a suitable basis. These $k$ calls may happen in parallel in which case the input state is a maximally entangled one over $kd$ qubits [11, 16] or may also happen sequentially in which the input state is a superposition of the eigenstates of $(U_1^\dagger U_2)$ [17]. Such bespoken input states may be difficult to create, all the more if $k$ is large. It may be desirable to have a method that uses easy to construct input states and it will be even better if any $U_1$ and $U_2$ can be discriminated using a single input state. Our method requires a sequential application of $U$ and can be applied to "any input state" (except a small subset).

To discriminate with a probability of error at most 1/3, Kawachi et al. [9] reported a method that used parallel calls to $U$ and an entangled state over $kd$

qubits. They proved an upper bound of $\lceil \frac{\pi}{3\omega} \rceil$ calls and also showed that there exists operators that require at least $\lceil \frac{2}{3\omega} \rceil$ calls to $U$. Their method can be easily generalized for an arbitrary error $\epsilon$ and after doing that along with additional tightening (see Appendix A), we obtain an upper bound of $\lceil \frac{2}{\omega} \sin^{-1}(1-2\epsilon) \rceil$ calls and a lower bound of $\lceil \frac{1-2\epsilon}{\sin(\omega/2)} \rceil$ calls that almost matches their upper bound. However, even for their method a specific input state is required. Our method can be seen as an alternative sequential method but with fewer qubits.

Duan et al. gave a lower bound on the number of calls required in a sequential method for perfect discrimination [17]. Their method can also be easily generalized (see Appendix A) to arbitrary error and we obtained the same lower bound as that obtained from the generalization of Kawachi et al.'s result that was mentioned earlier. Duan et al. also gave a sequential algorithm for perfect discrimination (using a specific input state) but it was not immediately clear how to extend their algorithm for bounded-error discrimination. In any case, we would like to see our discrimination algorithm as an alternative sequential method that uses the idea of amplitude amplification, is independent of the input state and makes almost the same number of calls to the black-boxes as the currently known parallel discrimination method.

### 3.1 Separation using amplitude amplification

Suppose that we want to use an input state $|\gamma\rangle$ which may be chosen optimally or may simply be available for use. We assume that we have access to the black-box $U \in \{U_1, U_2\}$ and its corresponding adjoint $U^\dagger$ as well. It should be noted that if $U$ is implemented as a quantum circuit, then $U^\dagger$ is usually easy to implement. We will discuss both cases of error probability $\epsilon < 0.5$ and $\epsilon = 0$.

Let $s$ be some phase and $\theta \in [0, \pi/4]$ be an angle such that $\langle\gamma|U_1^\dagger U_2|\gamma\rangle = \cos 2\theta e^{is}$; define $|\sigma_1\rangle = U_1|\gamma\rangle$ and $|\sigma_2\rangle = e^{-is}U_2|\gamma\rangle$ so that $\langle\sigma_1|\sigma_2\rangle = \cos 2\theta$ is real making it easier to apply Theorem 1. Given this $|\gamma\rangle$, the probability of error in discriminating between $U_1|\gamma\rangle$ and $U_2|\gamma\rangle$ can be expressed according to this well-known relationship: $\Pr[error] = \frac{1}{2}\left(1 - \sqrt{1 - |\langle\sigma_1|\sigma_2\rangle|^2}\right) = \frac{1-\sin 2\theta}{2}$

Observe that if $\theta = \frac{\pi}{4}$, the states $|\sigma_1\rangle$ and $|\sigma_2\rangle$ are already orthogonal and so can be perfectly discriminated; on the other hand, if $\theta = 0$ (i.e., $|\sigma_1\rangle$ and $|\sigma_2\rangle$ differ only by a global phase), then they cannot be discriminated better than a random guess. Therefore, we will focus on the case when $\theta \in (0, \pi/4)$.

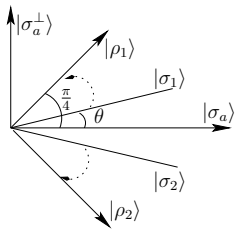



**Fig. 1.** The different states that are used in operator discrimination.

Construct an orthogonal basis for $\mathcal{H} = \mathcal{H}(|\sigma_1\rangle, |\sigma_2\rangle)$ by first defining $|\sigma_a\rangle = p|\sigma_1\rangle + p|\sigma_2\rangle$ and then defining an appropriate orthogonal state $|\sigma_a^\perp\rangle = p'|\sigma_1\rangle - p'|\sigma_2\rangle$; it suffices to use $p = 1/(2\cos\theta)$ and $p' = 1/(2\sin\theta)$. It is now easy to represent $|\sigma_i\rangle$ in the above basis; $|\sigma_1\rangle = \langle\sigma_a|\sigma_1\rangle|\sigma_a\rangle + \langle\sigma_a^\perp|\sigma_1\rangle|\sigma_a^\perp\rangle = \cos\theta|\sigma_a\rangle + \sin\theta|\sigma_a^\perp\rangle$ and $|\sigma_2\rangle = \langle\sigma_a|\sigma_2\rangle|\sigma_a\rangle + \langle\sigma_a^\perp|\sigma_2\rangle|\sigma_a^\perp\rangle = \cos\theta|\sigma_a\rangle - \sin\theta|\sigma_a^\perp\rangle$. Define operators $Q_0 = |\sigma_a\rangle\langle\sigma_a|$, $Q_1 = |\sigma_a^\perp\rangle\langle\sigma_a^\perp|$ and define a projective measurement $\mathcal{Q} = \langle Q_0, Q_1\rangle$. It will be easier to visualize all rotations in the basis $(|\sigma\rangle, |\sigma^\perp\rangle)$.

Now define $|\rho_1\rangle = \frac{1}{\sqrt{2}}|\sigma_a\rangle + \frac{1}{\sqrt{2}}|\sigma_a^\perp\rangle$ and $|\rho_2\rangle = \frac{1}{\sqrt{2}}|\sigma_a\rangle - \frac{1}{\sqrt{2}}|\sigma_a^\perp\rangle$. Use this to define a two-outcome projective measurement operator $\mathcal{P} = \langle P_1, P_2\rangle$ in which $P_1 = |\rho_1\rangle\langle\rho_1|$ and $P_2 = I - P_1 = |\rho_2\rangle\langle\rho_2|$. The different states that were constructed are explained in Figure 1.

Suppose $G_{a,b}^U$ denotes the operator $U[(1-e^{ia})|\gamma\rangle\langle\gamma| - I]U^\dagger \cdot [I - (1-e^{ib})Q_1]$ that uses the black-box $U$. Our first observation is that $G_{a,b}^{U_i}$ can also be written as $[(1-e^{ia})|\sigma_i\rangle\langle\sigma_i| - I]U^\dagger \cdot [I - (1-e^{ib})Q_1]$. Since the space spanned by $Q_0|\sigma_1\rangle$ and $Q_1|\sigma_1\rangle$ is $\mathcal{H}$ itself, and $\|Q^1|\sigma_1\rangle\|^2 = |\langle\sigma_a^\perp|\sigma_1\rangle|^2 = \sin^2\theta$, $G_{a,b}^{U_1}$ operators can be used in Theorem 1 for rotating any state in $\mathcal{H}$ in a counter-clockwise manner by some angle that is at most $2\theta$.

Our second observation arises from the fact that since $|\sigma_2\rangle = \cos\theta|\sigma_a\rangle + \sin\theta(-|\sigma_a^\perp\rangle)$, $G_{a,b}^{U_2}$ can still be used in Theorem 1 but the rotation will be from $|\sigma_a\rangle$ towards $-|\sigma_a^\perp\rangle$; that is, the rotation will be in a *clockwise* manner with everything else remaining the same as above (also illustrated in Figure 1).

For discriminating with low probability of error, say $\epsilon$, let $\varepsilon \in [0, \pi/2]$ be an angle such that $\sin^2\varepsilon = \epsilon$. Let $\phi = \pi/4 - \theta - \varepsilon$. Applying Corollary 1, one can calculate $\rho, a, b$ and set $k = \lfloor \frac{\phi}{2\theta} \rfloor$ such that $CP_\rho G_{a,b}^{U_i} CP_\rho^\dagger [G_{\pi,\pi}^{U_i}]^k$ rotates in the following manner. Here, $|\bar{\sigma}_a^\perp\rangle$ denotes the state $-|\sigma_a^\perp\rangle$.

$$|\sigma_1\rangle = \cos\theta|\sigma_a\rangle + \sin\theta|\sigma_a^\perp\rangle \xrightarrow{CP_\rho G_{a,b}^{U_1} CP_\rho^\dagger [G_{\pi,\pi}^{U_1}]^k} \cos(\theta+\varepsilon)|\sigma_a\rangle + \sin(\theta+\varepsilon)|\sigma_a^\perp\rangle$$

$$|\sigma_2\rangle = \cos\theta|\sigma_a\rangle + \sin\theta|\bar{\sigma}_a^\perp\rangle \xrightarrow{CP_\rho G_{a,b}^{U_2} CP_\rho^\dagger [G_{\pi,\pi}^{U_2}]^k} \cos(\theta+\varepsilon)|\sigma_a\rangle + \sin(\theta+\varepsilon)|\bar{\sigma}_a^\perp\rangle$$

Let $V^{U_i}$ denote the operator $CP_\rho G_{a,b}^{U_i} CP_\rho^\dagger [G_{\pi,\pi}^{U_i}]^k U_i$. Our discrimination procedure consists of first deriving the parameters $(\rho, a, b, k)$, constructing a circuit for the operator $V^U$ using the black-box $U$, executing $V^U|\gamma\rangle$ to obtain state $|\Psi\rangle$ and finally measuring $|\Psi\rangle$ in the basis $\mathcal{P}$. $U$ is declared to be $U_i$ if measurement outcome is $|\rho_i\rangle$. The probability of error can be calculated as $\|P_1 V^{U_2}|\gamma\rangle\|^2 = \|P_2 V^{U_1}|\gamma\rangle\|^2 = \sin^2\varepsilon = \epsilon$, as desired.

Finally, we would like to discuss the query complexity of discrimination. Since each call to $G_{a,b}^U$ involves one call to $U$ and one call to $U^\dagger$, the number of calls to $U^\dagger$ is $k+1$ while the number of calls to $U$ is $k+2$ (including the initial call to $|\gamma\rangle$). Therefore, the total number of queries is $2k+3$. Here $k = \lfloor \frac{\pi/4 - \theta - \sin^{-1}\sqrt{\epsilon}}{2\theta} \rfloor$ that can be simplified to $\mathsf{R}(\frac{\pi}{8\theta} - \frac{\sin^{-1}\sqrt{\epsilon}}{2\theta}) - 1$. We use $\mathsf{R}(f)$ to denote the nearest integer to any floating point number $f$ ($\mathsf{R}(0.5)$ is set to 1).

**Theorem 2.** *The above algorithm can differentiate between two operators $U_1$ and $U_2$ for any input state $|\gamma\rangle$ with probability of error at most $\epsilon$ as long as*

$\theta = \cos^{-1} |\langle\gamma|U_1^\dagger U_2|\gamma\rangle| \neq 0$ *and using* $2 * \mathsf{R}\left(\frac{\pi}{8\theta} - \frac{\sin^{-1}\sqrt{\epsilon}}{2\theta}\right) + 1$ *total calls to the black-boxes* $U$ *and* $U^\dagger$.

Of course, $|\gamma\rangle$ can be chosen optimally to maximize $\theta$. For the optimal $|\gamma\rangle$, $|\langle\gamma|U_1^\dagger U_2|\gamma\rangle|$ equals $\cos^2\frac{\omega}{2}$ (therefore, use $\theta = \omega/4$) which leads to the following corollary about optimal discrimination between $U_1$ and $U_2$.

**Corollary 2.** *The above algorithm can differentiate between two operators* $U_1$ *and* $U_2$ *without any error using the optimal input state and a total of* $2 \cdot \mathsf{R}\left(\frac{\pi}{2\omega}\right) + 1 \in \{\lceil\frac{\pi}{\omega}\rceil, \lceil\frac{\pi}{\omega}\rceil + 1\}$ *calls to the black-boxes. The number of calls to discriminate with probability of error* $\epsilon$ *is at most* $2 \cdot \mathsf{R}\left(\frac{\pi}{\omega} - \frac{2\sin^{-1}\sqrt{\epsilon}}{\omega}\right) + 1 = 2 \cdot \mathsf{R}\left(\frac{\sin^{-1}(1-2\epsilon)}{\omega}\right) + 1$ *and in particular, with error 1/3 is at most* $2 \cdot \mathsf{R}(0.34/\omega) + 1$.

For both exact and bounded-error algorithms, the query complexity of our algorithm using the optimal state is at most one more than current known bounds.

## 4 Randomized non-query classes

The current methods for improving success probability of bounded-error non-query quantum algorithms are parallel repetitions [12] that have the same complexity as classical methods. Intuitively, however, amplitude amplification ought to be applicable for such algorithms too.

Consider the randomized complexity class $\mathbf{RQP}_\epsilon$. For any language $L \in \mathbf{RQP}_\epsilon$, there exists a corresponding uniform family of quantum circuits $\{C\}_n$, say, over $n + a$ qubits and an initial state $|\alpha\rangle$ over $a$ ancilla qubits that may depend on $n$. As per standard practice, we assume that after $C$ is applied the first qubit is measured in the standard basis, i.e., the output state is measured by the projective measurement operator $\mathcal{P} = \langle P^0 = |0\rangle\langle 0| \otimes I, P^1 = |1\rangle\langle 1| \otimes I\rangle$. This can be easily generalized to any other decision criteria that involves measuring the output state by a two-outcome projective measurement. We denote the output state $C_n(|x\rangle \otimes |\alpha\rangle)$ by $|\Psi_x\rangle$ in which $n$ denotes $|x|$. Let $\theta \in (0, \pi/2)$ be an angle such that $\sin^2\theta = \epsilon$; note that if $\theta = \pi/2$, then $p = 1$ and in that case we anyway have $L \in \mathbf{EQP}$. Since $L \in \mathbf{RQP}_\epsilon$, the following should hold for any $x \in \{0,1\}^*$.

$$x \in L \implies \|P^1|\Psi_x\rangle\|^2 \geq \epsilon = \sin^2\theta, \quad \text{and} \quad x \notin L \implies \|P^1|\Psi_x\rangle\|^2 = 0 = \sin^2 0$$

We also define the *exact one-sided error quantum class* $\mathbf{ERQP}_\epsilon$ by extending $\mathbf{RQP}_\epsilon$: for $x \in L$, $\|P^1|\Psi_x\rangle\|^2 = \epsilon$ and the probability is zero for $x \notin L$.

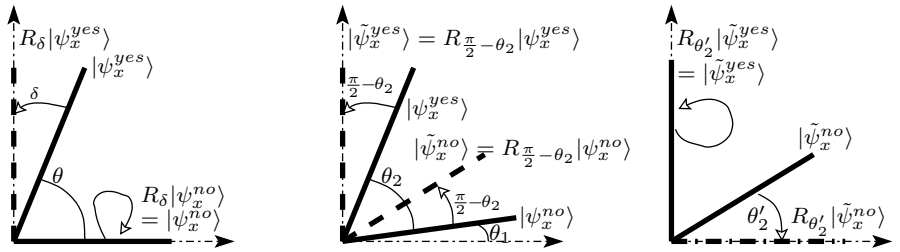
We can similarly define two-sided bounded-error quantum classes. For any $0 \leq \epsilon_2 < \frac{1}{2} < \epsilon_1 \leq 1$, define $\mathbf{BQP}_{\epsilon_1,\epsilon_2}$ as the class of languages $L$ such that:

$$x \in L \implies \|P^1|\Psi_x\rangle\|^2 \geq \epsilon_2, \qquad \text{and} \qquad x \notin L \implies \|P^1|\Psi_x\rangle\|^2 \leq \epsilon_1 \quad \text{for any } x$$

Also, define its exact error version [1] $\mathbf{EBQP}_{\epsilon_1,\epsilon_2}$ which consists of languages with error probabilities that is exactly $\epsilon_1$ if $x \in L$ and exactly $\epsilon_2$ if $x \notin L$.

[1] A similar question on exact two-sided-error classical class was asked in `http://cstheory.stackexchange.com/questions/20027`.

Furthermore, define $\mathbf{ERQP} = \bigcup_{\epsilon} \mathbf{ERQP}_{\epsilon}$ and $\mathbf{EBQP} = \bigcup_{\epsilon_1,\epsilon_2} \mathbf{EBQP}_{\epsilon_1,\epsilon_2}$. Obviously, $\mathbf{EQP} \subseteq \mathbf{ERQP}$ and $\mathbf{EQP} \subseteq \mathbf{EBQP}$.




(a) Amplification of **ERQP**

(b) Stage-1 of **EBQP** amplification

(c) Stage-2 of **EBQP** amplification

**Fig. 2.** Amplification of exact-error classes can be seen as conditional rotations. Solid lines denote the states before rotation and dashed lines denotes the states after rotation.

### 4.1 One-sided exact error class: ERQP

Languages in $\mathbf{ERQP}_{\epsilon}$ can be amplified immediately by using Theorem 1. Consider any such $L$ and any $x \in L$. Let $\mathcal{H}$ denote the space spanned by $P^1|\Psi_x\rangle$ and $P^0|\Psi_x\rangle$; clearly, $|\Psi_x\rangle \in \mathcal{H}$. Let $\delta = \pi/2 - \theta$. Construct rotation operator $R_\delta$ using $|\Psi_x\rangle$ and $P^1$. Applying this $R_\delta$ on $|\Psi_x\rangle$ gives us a state such that $\|P^1 R_\delta |\Psi_x\rangle\|^2 = 1$. On the other hand, if $x \notin L$, $\mathcal{H}$ is one-dimensional and in that case the constructed operator $R_\delta$ acts as the identity operator; therefore, $\|P^1 R_\delta |\Psi_x\rangle\|^2 = 0$. Figure 2a illustrates the action of $R_\delta$ for both the cases.

We only need to show that $R_\delta$ can be constructed in a uniform manner for a fixed $L$. $R_\delta$ will be constructed as $R_{\delta'} R_{2\theta}^k$ where $k = \lfloor \frac{\delta}{2\theta} \rfloor$ and $\delta' = \delta - k \cdot 2\theta$. However, the difficulty lies in constructing the $R_{\delta'}$ and $R_{2\theta}$ operators. Both of them involve some uniformly chosen gates (that depend upon $|\alpha\rangle$, $P^1$, $\delta$ and $2\theta$) but also operators of the type $[(1 - e^{i\gamma})|\Psi_x\rangle\langle\Psi_x| - I]$ that seem to be dependent on $x$. The key observation here is that

$$((1 - e^{i\gamma})|\Psi_x\rangle\langle\Psi_x| - I) = C \cdot ((1 - e^{i\gamma})|x\rangle\langle x| \otimes |\alpha\rangle\langle\alpha| - I) \cdot C^\dagger$$

and that a Fanout gate [18] can be used to make a copy of the input state $|x\rangle$ at the beginning which can be used later to implement $|x\rangle\langle x|$. The detailed construction of the above operator is given in Appendix B. Essentially we are able to construct a uniform circuit $R_\delta$ that can completely eliminate any error in deciding strings in **ERQP** languages.

**Theorem 3.** $\mathbf{EQP} = \bigcup_{\epsilon} \mathbf{ERQP}_{\epsilon} = \mathbf{ERQP}$.

We will now analyse the complexity of amplification. Let $s(n)$ be an upper bound on the size (number of gates) the circuits $C_n$ and $C_n^\dagger$. Let $C_n'$ denote the amplified zero-error circuit that calls $C_n$ and $C_n^\dagger$ and let $s'(n)$ denote the size of $C_n'$. Assuming that $A, B, E$ can be implemented without much overhead on size, $s'(n)/s(n)$ is proportional to $1 + 2(k+1) \approx 2(\frac{\pi}{4 \sin^{-1} \sqrt{\epsilon}} - \frac{1}{2}) + 3 \leq \frac{1.6}{\sqrt{\epsilon}} + 2$.

Now contrast this with the usual parallel scheme of running multiple copies of $C_n$ in parallel (on copies of $|x\rangle \otimes |\alpha\rangle$, with $|x\rangle$ being copied using a Fanout gate). First of fall, such a parallel scheme cannot possible achieve 100% probability of success. Secondly, the size increases by a factor proportional to $\frac{1}{-\ln(1-\epsilon)} \approx \frac{1}{\epsilon}$ that is quadratic ally large compared to the amplified $C'_n$ with zero-error.

### 4.2 Two-sided exact error class EBQP

Two-sided bounded-error classes can be treated similarly as their one-sided counterparts. We will leave out the details and only chalk the main ideas using the $R_\theta$ rotation operators for suitable $\theta$. We have already explained in the earlier subsections how to implement $R_\theta$ in a uniform manner; this is sufficient to give us uniform circuits to decide languages with a higher probability of success.

For the two-sided exact error class **EBQP** and some language $L \in \mathbf{EBQP}$, consider the two-stage amplification process illustrated in Figure 2. Consider any $n$-bit $x$ and let $C$ denote the corresponding circuit and $|\alpha\rangle$ denote the (uniformly generated) fixed-state ancilla register. Let $|\Psi_x\rangle$ denote $C|x\rangle \otimes |\alpha\rangle$.

Consider any $x^{yes} \in L$ and denote $C|x^{yes}\rangle \otimes |\alpha\rangle$ by $|\Psi_x^{yes}\rangle$. Similarly, if $x^{no} \notin L$, denote $C|x^{no}\rangle \otimes |\alpha\rangle$ by $|\Psi_x^{no}\rangle$. Furthermore, let $0 < \theta_1 < \theta_2 < \pi/2$ be angles such that $\sin^2\theta_1 = \epsilon_1$ and $\sin^2\theta_2 = \epsilon_2$.

In stage-1 (Figure 2b), first $R_{\pi/2-\theta_2}$ is applied to $|\Psi_x\rangle$; let $C_1$ denote the circuit and $|\tilde{\Psi}_x\rangle = C_1|x\rangle \otimes |\alpha\rangle$ denote the state thus obtained. Here $R_{\pi/2-\theta_2}$ is constructed by using $|\Psi_x\rangle$ and $P^1$ and involves $C$ and $C^\dagger$ similar to the construction in Subsection 4.1. If $x \in L$, then $|\tilde{\Psi}_x\rangle$ is now aligned with $P^1|\Psi_x\rangle$ whereas if $x \notin L$, then $|P^1|\tilde{\Psi}_x\rangle| = \sin(\pi/2 - (\theta_2 - \theta_1))$.

Let $\theta'_2$ denote $\pi/2 - (\theta_2 - \theta_1)$. Observe that $|\tilde{\Psi}_x\rangle$ belongs to the same Hilbert space spanned by $P^1|\Psi_x\rangle$ and $P^0|\Psi_x\rangle$. In stage-2 (Figure 2c), $\tilde{R}_{\theta'_2}$ is applied on $|\tilde{\Psi}_x\rangle$ but now $\tilde{R}_{\theta'_2}$ is constructed using $|\tilde{\Psi}_x\rangle$ and $P^0$ and involves $C_1$ and $C_1^\dagger$ similar to the construction in Subsection 4.1; $C_1$ and $C_1^\dagger$ in turn calls $C$ and $C^\dagger$.

First consider the case of $x \in L$. $P^0|\tilde{\Psi}_x\rangle = 0$ implies that $\tilde{R}_{\theta'_2}|\tilde{\Psi}_x\rangle$ is identical to $|\tilde{\Psi}_x\rangle$ (up to a global phase). Then consider the case of $x \notin L$. Since, $|P^0|\tilde{\Psi}_x\rangle| = \sin(\theta_2 - \theta_1)$, $\tilde{R}_{\theta'_2}|\tilde{\Psi}_x\rangle$ will be now aligned with $P^0$.

Thus we get the resultant circuit $C' = \tilde{R}_{\theta'_2} R_{\pi/2-\theta_2} C$ and the final state applying $C'$ is measured using $(P^0, P^1)$. If $P^0$ is observed, (correctly) decide that $x \notin L$ and otherwise, (correctly) decide that $x \in L$.

**Theorem 4.** $\mathbf{EQP} = \bigcup_{\epsilon_1,\epsilon_2} \mathbf{EBQP}_{\epsilon_1,\epsilon_2} = \mathbf{EBQP}$.

We will now discuss the complexity of the amplified algorithm and compare it with the usual parallel repetition algorithm for **BQP** that outputs the majority. Like for the **EQP** case, we will use $C$ and $C'$ for the original circuit and the zero-error amplified circuit, respectively. We will focus only on overhead caused by the multiple calls to $C$ and $C^\dagger$ hoping that the additional components in the $R_\delta$ gates can be implemented with a small number of gates.

For comparison with the parallel repetition algorithm, it will be convenient to assume that $\epsilon_2 = 1 - \epsilon_1$ and therefore, $\theta_2 = \pi/2 - \theta_1$ in which $\theta_2 > \pi/4$.

Apart from the initial call to $C$ to generate $|\Psi_x\rangle$, notice that the number of calls in the first phase is at most 2 since $\frac{\pi/2-\theta_2}{2\theta_2} < 1$. The number of calls in the second phase is $\approx 2\left(1 + \frac{\pi/2-(\theta_2-\theta_1)}{2(\theta_2-\theta_1)}\right) = 1 + \frac{\pi}{2(\theta_2-\theta_1)} = 1 + \frac{\pi}{2(\sin^{-1}\sqrt{\epsilon_2}-\sin^{-1}\sqrt{\epsilon_1})}$ $= 1 + \frac{\pi/2}{\sin^{-1}(\sqrt{\epsilon_2(1-\epsilon_1)}-\sqrt{\epsilon_1(1-\epsilon_2)})} \leq 1 + \frac{\pi/4}{\epsilon_2-1/2}$. Let $n_s$ denote this upper bound.

Contrast this with the parallel repetition method that takes the majority of several parallel executions of $C|x\rangle \otimes |\alpha\rangle$. Even though this method cannot collapse **EBQP** to **EQP**, suppose we are interested to improve the probability $\epsilon_2$ to $\sigma \approx 1$. Applying the usual Chernoff's bound based analysis, the number of parallel executions necessary is $\frac{4(1-\epsilon_2)}{(\epsilon_2-1/2)^2} \ln \frac{1}{1-\sigma}$ that we denote by $n_p$.

Note that if $\epsilon_2 \geq 3/4$, i.e., $\theta_2 \geq \pi/3$ and $\theta_1 \leq \pi/6$, then only 2 calls are necessary in the second phase. So, for comparison we consider $1/2 < \epsilon_2 < 3/4$. In that case, $n_p \geq \frac{1}{(\epsilon_2-1/2)^2} \ln \frac{1}{1-\sigma}$ and $n_s \approx \sqrt{n_p}$ (ignoring small constants).

### 4.3 Non-exact classes RQP and BQP

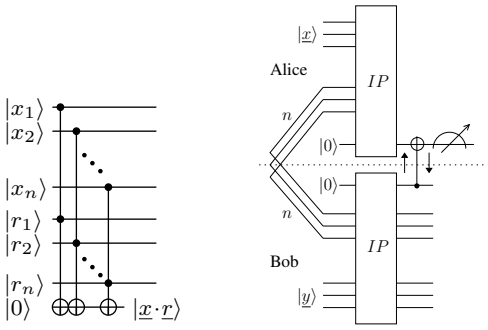
First we address the amplification of non-exact $\mathbf{RQP}_\epsilon$ languages. For such languages $1-\epsilon$ is only an upper bound on the failure probability (when $x \in L$). Since amplitude amplification requires knowledge of the success probability, there has been several attempts to generalize amplitude amplification for the cases when this probability is not known. An often followed approach guesses the value of $\epsilon$ in an exponentially increasing manner until a solution is found [6] or time-out happens. Instead we suggest using the quantum "fixed-point" search techniques for $\mathbf{RQP}_\epsilon$ languages, e.g., following the one proposed by Yoder et al. [7] gives us a quantum circuit that makes $O(\frac{1}{\sqrt{\epsilon}} \log \frac{2}{\sqrt{1-\delta}}) = O(\frac{1}{\sqrt{\epsilon}} \log \frac{1}{1-\delta})$ calls to $C$ and $C^\dagger$ and is sufficient to increase the success probability from $\epsilon$ to $\delta$. The gates in that circuit are either fixed for $L$ or of the form $G_{a,b}$ that we showed how to construct in a uniform manner in the earlier subsection. Contrast this to classical techniques for amplifying probability of **RP** languages; if $C$ was a classical algorithm, then $\frac{\ln(1-\delta)}{\ln(1-\epsilon)} \geq \frac{1}{\epsilon} \ln \frac{1}{1-\delta}$ calls to $C$ are required which is almost square of the number of calls required for the quantum case.

Circuits for **BQP** languages can also be amplified using ideas presented here. However, we leave out the specific details from this paper.

### 4.4 Communication Protocols

Apart from black-box/query algorithms, quantum amplitude amplification has also been applied to quantum communication protocols [19] for reducing probability of error and for distributed leader election [4] but they do not involve protocols that use pre-shared entangled bits. One can observe that existing quantum communication complexity protocols can be applied to protocols in which the parties get their input in the form of input state and not as oracle gates.

In this context we want to point out that the the subtle requirement that it is not possible to amplify protocols that use arbitrary shared entangled qubits as ancilla. This is in stark contrast to quantum circuits that may use ancilla in entangled states and yet, can be amplified.




(a) Circuit $IP$

(b) Circuit implementing randomized string equality

**Fig. 3.** Circuit to detect if $\underline{x} = \underline{y}$ with probability at least 1/2

Consider the quantum protocol illustrated in Figure 3 that implements the well-known randomized algorithm for $\mathbf{EQ}(x, y)$ that asks whether two $n$-bit string $x$ and $y$ are identical. The protocol compares $x \cdot r$ and $y \cdot r$ in which $r$ represents $n$ random bits known to both parties. The circuit uses $n$ EPR pairs to simulate $n$ public random bits used in the randomized algorithm. It can be verified that if $x = y$, then the output qubit is always observed to be in $|0\rangle$ whereas if $x \neq y$, then the output qubit is observed in $|0\rangle$ or $|1\rangle$ with equal probability. If we could somehow apply amplitude amplification to this protocol, then Grover iterator would be applied only once, i.e., involving a total communication of 6 qubits (each Grover iterator involves a call to the circuit and a call to its inverse). That would invalidate the well-established lower bound that computing **EQ** by a communication protocol that involves pre-shared EPR pairs requires communication of at least $n/2$ qubits [20].

## 5 Conclusion

Amplitude amplification is commonly used to improve the probability of success of quantum query algorithms. We extend their usage to non-query algorithms by exploiting the fact that what they essentially do is increase the difference in probability of success between two cases. Based on this observation, we obtain efficient sequential algorithms for discrimination of unitary operators and for improving success probability of bounded error quantum algorithms.

## References


[1] L. K. Grover. "A fast quantum mechanical algorithm for database search". In: *Proceedings of 28th STOC*. 1996.

[2] F. Magniez, M. Santha, and M. Szegedy. "Quantum Algorithms for the Triangle Problem". In: *SIAM Journal on Computing* 37.2 (2007).

[3] M. Ozols, M. Roetteler, and J. Roland. "Quantum Rejection Sampling". In: *ACM Trans. Comput. Theory* 5.3 (2013).

[4] K. M. Hirotada Kobayashi and S. Tani. "Simpler Exact Leader Election via Quantum Reduction". In: *Chicago Journal of Theoretical Computer Science* 2014.10 (2014).

[5] D. W. Berry, A. M. Childs, R. Cleve, R. Kothari, and R. D. Somma. "Exponential Improvement in Precision for Simulating Sparse Hamiltonians". In: *Proceedings of the 46th STOC*. 2014.

[6] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp. "Quantum amplitude amplification and estimation". In: *Contemporary Mathematics* 305 (2002).

[7] T. J. Yoder, G. H. Low, and I. L. Chuang. "Fixed-Point Quantum Search with an Optimal Number of Queries". In: *Phys. Rev. Lett.* 113 (21 2014).

[8] R. J. Lipton and K. W. Regan. *Quantum Algorithms via Linear Algebra: A Primer*. The MIT Press, 2014.

[9] A. Kawachi, K. Kawano, F. Le Gall, and S. Tamaki. "Quantum Query Complexity of Unitary Operator Discrimination". In: *Proceedings of 23rd COCOON*. 2017.

[10] D. Bera. "Detection and Diagnosis of Single Faults in Quantum Circuits". In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 37.3 (2018).

[11] A. Acin. "Statistical distinguishability between unitary operations". In: *Physical review letters* 87.17 (2001).

[12] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. "Strengths and Weaknesses of Quantum Computing". In: *SIAM Journal on Computing* 26.5 (1997).

[13] E. Biham, O. Biham, D. Biron, M. Grassl, and D. A. Lidar. "Grover's quantum search algorithm for an arbitrary initial amplitude distribution". In: *Physical Review A* 60.4 (1999).

[14] E. Biham and D. Kenigsberg. "Grover's quantum search algorithm for an arbitrary initial mixed state". In: *Physical Review A* 66.6 (2002).

[15] P. Hoyer. "Arbitrary phases in quantum amplitude amplification". In: *Physical Review A* 62.5 (2000).

[16] G. M. D'Ariano, P. L. Presti, and M. G. Paris. "Using entanglement improves the precision of quantum measurements". In: *Physical review letters* 87.27 (2001).

[17] R. Duan, Y. Feng, and M. Ying. "Entanglement is not necessary for perfect discrimination between unitary operations". In: *Physical review letters* 98.10 (2007).

[18] D. Bera, F. Green, and S. Homer. "Small depth quantum circuits". In: *ACM SIGACT News* 38.2 (2007).

[19] P. Høyer and R. de Wolf. "Improved Quantum Communication Complexity Bounds for Disjointness and Equality". In: *STACS 2002*. 2002.

[20] H. Buhrman and R. de Wolf. "Communication Complexity Lower Bounds by Polynomials". In: *Proceedings of the 16th CCC*. 2001.

# A Appendix: Operator discrimination

In this section we generalize the operator discrimination upper and lower bounds given by Kawachi et al. [9] and the lower bound given by Duan et al. [17] to arbitrary bounded-error $\epsilon$.

## A.1 Upper bound for parallel method

Kawachi et al. showed that the probability of error in their operator discrimination algorithm that makes $k$ parallel calls to $U$ is given by $\frac{1}{2}(1 - \sin\frac{k\omega}{2})$ when $\omega < \pi$ [9, Lemma 2]. Equating that error to $\epsilon$ gives us the required upper bound on $k$ as $\lceil \frac{2}{\omega}\sin^{-1}(1-2\epsilon)\rceil$.

## A.2 Lower bound for parallel method

Kawachi et al. showed that if an operator discrimination algorithm makes $k$ parallel calls to $U$, then its error probability is at least $\frac{1}{2}(1 - \frac{k\omega}{2})$ [9, Theorem 5]. Equating the error to $\epsilon$ gives us the required lower bound of $\lceil \frac{1-2\epsilon}{\sin(\omega/2)}\rceil$.

## A.3 Lower bound for sequential method

Duan et al. showed that if $k\omega(U) < \pi$ for some operator $U$, then for any operators $X_1, X_2, \ldots X_{k-1}$, $\omega([X_{k-1}X_k \ldots X_1]^\dagger \cdot [UX_{k-1}UX_{k-2}\ldots UX_1U]) \leq k\omega(U)$. $\omega(O)$ was defined earlier as the length of the smallest arc containing all the eigenvalues of an operator $O$. Furthermore, it is known that the probability of discriminating two unitary operators $A$ and $B$ is $\frac{1}{2}(1 - \sin\frac{\omega(A^\dagger B)}{2})$ (using the optimal input state and measurement). Therefore, using $A = X_{k-1}X_k\ldots X_1$ and $B = UX_{k-1}UX_{k-2}\ldots UX_1U$ and equating for $k$ such that probability of error in discriminating between $A$ and $B$ is $\epsilon$ gives us $k \geq \lceil \frac{2}{\omega(U)}\sin^{-1}(1-2\epsilon)\rceil$. The authors then showed that this lower bound of discriminating between $A$ and $B$ translates to the lower bound $\lceil \frac{2}{\omega(U^\dagger V)}\sin^{-1}(1-2\epsilon)\rceil$ for any sequential algorithm to discriminate between $U_1$ and $U_2$.

# B Uniform Grover iterator

Consider the operator $((1-e^{i\gamma})|\Psi_x\rangle\langle\Psi_x| - I) = C\cdot((1-e^{i\gamma})|x\rangle\langle x|\otimes|\alpha\rangle\langle\alpha| - I)\cdot C^\dagger$ that is used in the differential amplifications of **ERQP** and **EBQP** circuits. We show how to implement it without using a gate that depends upon the input state $|x\rangle$.

Denote the middle operator $((1 - e^{i\gamma})|x\rangle\langle x| \otimes |\alpha\rangle\langle\alpha| - I)$ by $M$. Figure 4 explains how to implement $M$ in a uniform manner. $M$ acts on two registers, $R_1$ with $n$ qubits and $R_2$ with $a$ qubits. It is implemented using three sub-operators $A, B, E$ and uses $n + 2$ ancilla qubits. The states of the ancilla qubits are reset to their initial states at the end of $M$, and hence, these qubits can be reused during all calls to $G$.

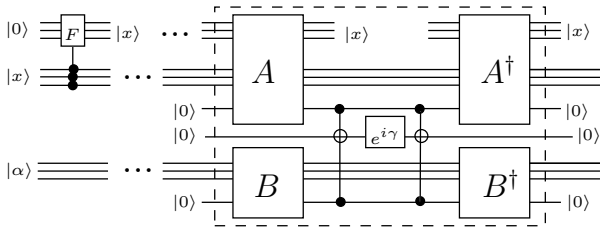



**Fig. 4.** Circuit to implement the module $((1 - e^{i\gamma})|\Psi_x\rangle\langle\Psi_x| - I)$

Operator $A$ acts on three registers, first one on $n$ qubits that is always fixed to $|x\rangle$ (corresponding to the classical input $x$), the third one is always fixed to $|0\rangle$ and the second register is $R_1$. The action of $A$ can be described by the mapping $|x\rangle|y\rangle_{R_1}|b\rangle \mapsto |x\rangle|y\rangle_{R_1}|b \oplus (x \stackrel{?}{=} y)\rangle$ on the basis states. It is important to note that the state of the first register of $A$ remains unchanged. At the very beginning of the circuit, a Fanout gate [18] can be applied to the input register (in state $|x\rangle$) to create a copy of $|x\rangle$ that can be used for the first register of $A$ in every call to $G$.

In a similar manner, $B$ acts on two registers in which the first register is always fixed to $|0\rangle$ and the second register is $R_2$. Since $|\alpha\rangle$ is known, $B$ can be implemented to map $|0\rangle|\alpha\rangle_{R_2} \mapsto |1\rangle|\alpha\rangle_{R_2}$ and $|0\rangle|\alpha^{\perp}\rangle_{R_2} \mapsto |0\rangle|\alpha^{\perp}\rangle_{R_2}$.

$E$ is a two-qubit operator that simply changes the phase by $e^{i\gamma}$ if both the input qubits are in the state $|1\rangle$, i.e., $E = I - (1 - e^{i\gamma})|11\rangle\langle 11|$.

It can be seen that $A, B$ and $E$ altogether changes the phase of $|x\rangle_{R_1}|\alpha\rangle_{R_2}$ by $e^{i\gamma}$ and leaves any orthogonal state in $R_1, R_2$ as it is — essentially implementing $-M$. After correctly changing the phase, $A^{\dagger}$ and $B^{\dagger}$ are executed to reset the states of the third register of $A$ to $|0\rangle$ and first register of $B$ to $|0\rangle$, respectively. Therefore, those registers can be reused in the next call to $G$.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il