

The Phase Matrix

Peter Høyer*

Department of Computer Science, University of Calgary, Canada.
hoyer@cpsc.ucalgary.ca

Abstract. Reducing the error of quantum algorithms is often achieved by applying a primitive called amplitude amplification. Its use leads in many instances to quantum algorithms that are quadratically faster than any classical algorithm. Amplitude amplification is controlled by choosing two complex numbers ϕ_s and ϕ_t of unit norm, called phase factors. If the phases are well-chosen, amplitude amplification reduces the error of quantum algorithms, if not, it may increase the error. We give an analysis of amplitude amplification with a emphasis on the influence of the phase factors on the error of quantum algorithms. We introduce a so-called phase matrix and use it to give a straightforward and novel analysis of amplitude amplification processes. We show that we may always pick identical phase factors $\phi_s = \phi_t$ with argument in the range $\frac{\pi}{3} \leq \arg(\phi_s) \leq \pi$. We also show that identical phase factors $\phi_s = \phi_t$ with $-\frac{\pi}{2} < \arg(\phi_s) < \frac{\pi}{2}$ never leads to an increase in the error, generalizing a recent result of Lov Grover who shows that amplitude amplification becomes a quantum analogue of classical repetition if we pick phase factors $\phi_s = \phi_t$ with $\arg(\phi_s) = \frac{\pi}{3}$.

Keywords: Quantum Computing. Algorithms. Amplitude Amplification. Randomized Algorithms.

1 Introduction to quantum searching

A decade ago, Lov Grover [5, 6] discovered a quantum mechanical algorithm that has since become one of the most famous quantum algorithms. The algorithm solves one of the most basic problems in algorithmics, that of searching an unstructured search space. It is based intrinsically on quantum mechanical effects and demonstrates beautifully a fundamental relationship between quantum mechanics and computations. The algorithm is very simple and runs quadratically faster than any classical algorithm in terms of query complexity. His algorithm is likely the most studied quantum algorithm ever, seconded only by the quantum Fourier transform. One of the early work related to Grover's algorithm is a generalization called *amplitude amplification* [2], which in rough terms shows that the benefits of Grover's algorithm carry over to arbitrary search processes and settings [2, 3]. Amplitude amplification is possibly an even simpler concept than

* Supported by the Canadian Institute for Advanced Research (CIAR), Canada's Natural Sciences and Engineering Research Council (NSERC), and The Mathematics of Information Technology and Complex Systems (MITACS).

Grover's algorithm. It allows to talk about arbitrary processes and algorithms, and helps devise simple yet optimal solutions to problems that can be related to searching. Amplitude amplification is sometimes referred to as *quantum searching* when applied specifically to search problems.

Grover's algorithm [5] and more generally amplitude amplification [2] are limited by the unitarity condition of quantum mechanics. In popular terms, the unitarity condition implies that if we run some algorithm and it solves some problem, then if we keep on running the algorithm (as opposed to stopping it and outputting the result found at that time), eventually the solution will be lost. The reason is that unitarity implies reversibility, and it thus seems tempting to conclude that there thus can be no fixed-point or one-way quantum search algorithms. However, the unitary limitation applies only if the following three conditions are satisfied: (1) we keep running the *same* process, (2) that process is *unitary*, and (3) we run it on a closed and *finite* quantum system. The remedy is to invalidate one or more of these conditions, which in earlier work [1, 3, 9] is done by introducing measurements, thus voiding (2), or embedding the quantum system into a much larger system, thus effectively voiding (3). Though these proposals certainly are remedies, they come with several downsides: they are somewhat technical, add to the overall complexity of the algorithm, are harder to understand than the original algorithm, are rather classical fixes to a quantum mechanical obstacle, and complicate applications.

In recent work, Grover [7] has suggested an idea that aims at voiding (1). When applying amplitude amplification, we pick two complex numbers of unit norm $\phi_s, \phi_t \in \mathbb{C}^*$, which are called phase factors. Grover [7] observes that if we pick the phase factor $\phi_s = \phi_t = e^{i\pi/3}$, then the amplitude amplification process automatically slows down as the error decreases. This naturally leads to the question if other phase factors have similar properties, and more generally, what influence does the phase factors have on the amplitude amplification process.

We first give a novel analysis of amplitude amplification with emphasis on the choice of phases. Our analysis uses only basic linear algebra, yet still it allows us to prove new fundamental properties of amplitude amplification, properties that have not been identified using more involved methods of analysis. As our main analytical tool, we introduce a so-called phase matrix of dimension 2×2 . We use it to explain why $e^{i\pi/3}$ is an appropriate phase factor. We also show that any nontrivial phase factor with positive real part guarantees a reduction in the error in quantum searching. That is, pick any complex number $\phi \in \mathbb{C}^*$ of unit norm with $0 < \text{Re}(\phi) < 1$, and amplitude amplification with ϕ reduces the overall error. This is (at least to this author) a somewhat surprisingly strong result given that amplitude amplification is a very well-studied and often used primitive. Our analysis yields several other corollaries as well.

2 Amplitude amplification

Amplitude amplification [2, 3] is a technique for manipulating the amplitudes of quantum states. One of its uses is to boost the success probability of quantum

algorithms. To keep this paper self-contained, we give a concise description of amplitude amplification with emphasis on error reduction. Further details and other applications can be found in e.g. [3].

Consider that we are given, or have developed, some quantum algorithm for solving some problem. We assume the algorithm does not use any measurements, so we can describe the algorithm by a unitary operator A . We may run algorithm A on some initial state $|s\rangle$, producing a final state $|\Psi\rangle = A|s\rangle$. Suppose that our aim is in producing some target state $|t\rangle$ that represents a solution to the problem. The success probability of algorithm A is the squared overlap $|\langle t|\Psi\rangle|^2$ of the state $|\Psi\rangle$ produced by A with the target state $|t\rangle$. Let angle $0 \leq \theta < \pi/2$ be such that $|\langle t|\Psi\rangle|^2 = \sin^2 \theta$. Then θ is an angle that represents the success probability of A . The closer θ is to $\pi/2$, the higher success probability. We write¹ $|\Psi\rangle = \sin \theta |t\rangle + \cos \theta |t^\perp\rangle$, where $|t^\perp\rangle$ is the normalized projection of $|\Psi\rangle$ onto the subspace complementary to the subspace spanned by $|t\rangle$.

Let ϵ be such that $|\langle t|\Psi\rangle|^2 = \sin^2 \theta = 1 - \epsilon$, so that ϵ is the error probability of A . We want ϵ to be small. If ϵ is large, we may want to apply some boosting method. A standard classical boosting technique is by repetition. If we run A , say, three times, each time on the initial state $|s\rangle$, then the probability of all three runs failing is $\epsilon' = \epsilon^3$. Amplitude amplification offers a quantum alternative to classical repetition. It works as follows. Pick any two complex numbers of unit norm $\phi_s, \phi_t \in \mathbb{C}^*$, which we refer to as phase factors. We define two operators $R_s = I - (1 - \phi_s)|s\rangle\langle s|$ and $R_t = I - (1 - \phi_t)|t\rangle\langle t|$, where I is the identity operator. These two operators are pseudo-reflections, where the first acts nontrivially on the ray spanned by $|s\rangle$, and the second nontrivially on the ray spanned by $|t\rangle$. Set $Q = Q(\phi_s, \phi_t) = -AR_sA^{-1}R_t$. Applying operator Q is amplitude amplification.

Operator Q acts invariantly on the two-dimensional subspace spanned by the orthogonal states $|t\rangle$ and $|t^\perp\rangle$, and with respect to the ordered basis $(|t\rangle, |t^\perp\rangle)$, has the following matrix representation [3],

$$Q = \begin{bmatrix} \phi_t((1 - \phi_s) \sin^2 \theta - 1) & (1 - \phi_s) \cos \theta \sin \theta \\ \phi_t(1 - \phi_s) \sin \theta \cos \theta & -(1 - \phi_s) \sin^2 \theta - \phi_s \end{bmatrix}. \quad (1)$$

Analysis on amplitude amplification can be conducted via an analysis of this matrix, and is thus a basic exercise which surprisingly previously has eluded a full understanding of the rôle of the phase factors, including the phase factor of $e^{i\pi/3}$. One aim of this work is to provide such an understanding.

3 The Phase Matrix

Returning to the general setting, consider we apply algorithm A on the initial state $|s\rangle$, hereby producing $|\Psi\rangle = A|s\rangle$. The probability that a measurement \mathcal{M} of state $A|\Psi\rangle$ does not yield the outcome $|t\rangle$, is ϵ . If we repeat this experiment three times independently, we may reduce the error of never measuring $|t\rangle$ to ϵ^3 .

¹ For simplicity, we ignore a possible global phase factor, which has no consequences in this work.

If we use amplitude amplification instead of classical boosting, we apply Q on $A|s\rangle$, unitarily producing the state $AR_sA^{-1}R_tA|s\rangle$, using a total number of three applications of A and its inverse. It is well-established that if we pick phase factors $\phi_s = \phi_t = -1$, we may achieve a quadratic improvement over classical repetition in many settings [5, 1]. The question is what happens for other choices of ϕ_s and ϕ_t .

We first write $|\Psi\rangle = A|s\rangle$ with respect to the ordered basis $(|t\rangle, |t^\perp\rangle)$ as a column vector, $A|s\rangle = [\sin\theta, \cos\theta]^T$. Applying Q on $A|s\rangle$ produces the state $QA|s\rangle$ represented by

$$\begin{bmatrix} \phi_t((1 - \phi_s)\sin^2\theta - 1) & (1 - \phi_s)\cos\theta\sin\theta \\ \phi_t(1 - \phi_s)\sin\theta\cos\theta & -(1 - \phi_s)\sin^2\theta - \phi_s \end{bmatrix} \begin{bmatrix} \sin\theta \\ \cos\theta \end{bmatrix}.$$

Our cardinal step is to isolate the influence of the phase factors ϕ_s and ϕ_t , rewriting $QA|s\rangle$ as

$$\begin{bmatrix} \sin\theta & 0 \\ 0 & \cos\theta \end{bmatrix} \begin{bmatrix} -\phi_s\phi_t & 1 - \phi_s - \phi_t \\ -1 + \phi_t - \phi_s\phi_t & -\phi_s \end{bmatrix} \begin{bmatrix} \sin^2\theta \\ \cos^2\theta \end{bmatrix}.$$

We now define the *phase matrix* P as

$$P = P(\phi_s, \phi_t) = \begin{bmatrix} -\phi_s\phi_t & 1 - \phi_s - \phi_t \\ -1 + \phi_t - \phi_s\phi_t & -\phi_s \end{bmatrix}. \quad (2)$$

This matrix allows us to give a simple intuitive study of the choices of phases, expressed independently of angle θ and thus also of the error probability ϵ . We may summarize the action of the amplitude amplification operator Q as follows.

$$Q : \begin{bmatrix} \sin\theta \\ \cos\theta \end{bmatrix} \mapsto \begin{bmatrix} \alpha \sin\theta \\ \beta \cos\theta \end{bmatrix} \quad \text{where} \quad \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = P \begin{bmatrix} \sin^2\theta \\ \cos^2\theta \end{bmatrix} = P \begin{bmatrix} 1 - \epsilon \\ \epsilon \end{bmatrix}. \quad (3)$$

Let ϵ' be the probability that a measurement \mathcal{M} of state $QA|\Psi\rangle$ does not yield the outcome $|t\rangle$. Then $\frac{\epsilon'}{\epsilon} = \beta^2$ is the relative change in error by applying amplitude amplification operator Q . We want β to be small.

In the next section, we use the above interpretation of amplitude amplification to give an analysis of the choices of phases.

4 Analysis of the Phase Matrix

Our analysis of the phase matrix P given by Eq. 2 begins with a consideration of the entry P_{21} . Recall that the phase matrix P is written with respect to the ordered basis $(|t\rangle, |t^\perp\rangle)$. The entry P_{21} thus captures how much amplitude may potentially be moved out of the solution subspace spanned by $|t\rangle$ to the error subspace spanned by $|t^\perp\rangle$. If entry P_{21} is zero, any amplitude that is moved into the solution subspace, stays in the solution subspace. Conversely, if entry P_{21} is non-zero, some amplitude might escape from the solution subspace.

If we insist on picking phase factors so that P_{21} is zero, then we effectively eliminate interference between the two subspaces, and the quantum algorithm becomes classical of nature. Indeed this is our interpretation of the main result of Grover [7] who shows that if we pick $\phi_s = \phi_t = e^{i\pi/3}$, then if the error of algorithm $A|s\rangle$ is ϵ , the error of algorithm $QA|s\rangle$ is ϵ^3 . It achieves the exact same error reduction as classical repetition. It is different from classical repetition in that it does not use intermediate measurements or additional storage space (e.g., an ancilla used for counting purposes). It is a truly in-place quantum mechanical version of classical repetition. It is fairly easy to see that this phase factor is unique up to conjugation, and thus does play a pivotal rôle in amplitude amplification.

Proposition 1. *Entry P_{21} of the phase matrix is zero iff $\phi_s = \phi_t = e^{\pm i\pi/3}$.*

With this uplifting simple explanation of Grover's result, we now study the phase matrix in more detail. Entry P_{21} is the sum of three unit numbers. We say that three unit numbers e^{ix}, e^{iy}, e^{iz} lie *within a half circle* if there exists a unit number w so that $e^{ix}w, e^{iy}w, e^{iz}w$ all have non-negative real part. We say they lie *strictly* within a half circle if there exists a unit number w so that $e^{ix}w, e^{iy}w, e^{iz}w$ all have nonzero and positive real part. The three vectors do not lie within a half circle if and only if every hyperplane strictly separates them. The sum of three unit vectors is related to whether they lie within a half circle.

Proposition 2. *The absolute value of the sum of three unit numbers is greater than one if they lie strictly within a half circle, is one if two of the numbers are each others negation, and is less than one otherwise.*

Proof. Consider the sum of three unit vectors e^{ix}, e^{iy}, e^{iz} . Without loss of generality, we may assume that $0 \leq z - y \leq \pi$. Fix y and z and consider the function $f(x) = |e^{ix} + e^{iy} + e^{iz}|$. The function is strictly monotonically increasing in the interval $[\frac{z+y}{2} - \pi, \frac{z+y}{2}]$, and it is one when $x = z - \pi$. Similarly, the function strictly monotonically decreasing in the interval $[\frac{z+y}{2} - 2\pi, \frac{z+y}{2} - \pi]$ and it is one when $x = y - \pi$. In summary, $f(x)$ is bigger than 1 if and only if the three vectors lie strictly within a half circle, the function is one if and only if $x = z - \pi$ or $x = y - \pi$, and it is less than one in all other cases. \square

We multiply entry P_{21} with $-\overline{\phi_t}$, apply Proposition 2 on $-1, \phi_s, \overline{\phi_t}$, and obtain the following characterization of $|P_{21}|$.

Lemma 1 (Contribution from solution subspace to error subspace).

$$|P_{21}| = \begin{cases} > 1 & \text{if } -1, \phi_s, \overline{\phi_t} \text{ lie strictly within a half circle} \\ = 1 & \text{if } \phi_s = 1, \phi_t = 1, \text{ or } \phi_s \phi_t = -1 \\ = 0 & \text{if } \phi_s = \phi_t = e^{\pm i\pi/3} \\ < 1 & \text{otherwise.} \end{cases}$$

To exhibit the significance of Lemma 1, reconsider Equation 3. We are interested in having $|\beta| < 1$ so that the error ϵ' of $\mathbf{QA}|s\rangle$ is smaller than the error ϵ of $\mathbf{A}|s\rangle$, the algorithm without amplitude amplification. The phase matrix \mathbf{P} is multiplied on the right by the column vector $[\sin^2 \theta, \cos^2 \theta]^T$. Since entry $|\mathbf{P}_{22}|$ is of unit norm, if $|\mathbf{P}_{21}| < 1$ then $|\beta| < 1$ and hence $\epsilon' < \epsilon$.

Theorem 1 (Strictly decreasing error). *If $-1, \phi_s, \overline{\phi_t}$ do not lie within a half circle, $\epsilon' < \epsilon$.*

The above theorem gives a sufficient condition for strict error reduction in amplitude amplification processes. Prior to Grover's recent work on the phase factor $e^{i\pi/3}$, no such condition was known. Our general condition is that $-1, \phi_s, \overline{\phi_t}$ do not lie close together.

5 Error reduction with phase matching

A desirable property of the phase matrix \mathbf{P} is to have $\arg(\mathbf{P}_{21}) = \arg(-\mathbf{P}_{22})$. If the two entries \mathbf{P}_{21} and \mathbf{P}_{22} point in opposite directions as vectors, the error introduced by the term $\mathbf{P}_{21} \sin^2 \theta$ partly cancels with the error introduced by the other term $\mathbf{P}_{22} \cos^2 \theta$. For fixed $|\mathbf{P}_{21}|$, having $\arg(\mathbf{P}_{21}) = \arg(-\mathbf{P}_{22})$ minimizes ϵ' (ϵ' is defined in Section 3 above). Our next lemma shows that the only nontrivial choices of phases for which $\arg(\mathbf{P}_{21}) = \arg(-\mathbf{P}_{22})$ is when $\phi_s = \phi_t$.

Lemma 2 (Phase matching). *$\arg(\mathbf{P}_{21}) = \arg(-\mathbf{P}_{22})$ if and only if $\phi_s = \phi_t$ and $\text{Re}(\phi_s) < \frac{1}{2}$.*

Proof. Suppose $\arg(\mathbf{P}_{21}) = \arg(-\mathbf{P}_{22})$. Then $\arg(1 - \phi_t + \phi_s \phi_t) = \arg(-\phi_s)$, and by adding $-\phi_s$ on the left hand side, $\arg((1 - \phi_t)(1 - \phi_s)) = \arg(-\phi_s)$. Multiplying through by $\overline{\phi_s}$, this implies that $\arg((1 - \overline{\phi_s})(1 - \phi_t)) = 0$, which is satisfied only if $\phi_s = \phi_t$, $\phi_s = 1$, or $\phi_t = 1$. Conversely, if $\phi_s = \phi_t$ and $\text{Re}(\phi_s) < \frac{1}{2}$, then $\arg(\mathbf{P}_{21}) = \arg(-\mathbf{P}_{22})$, while in the other cases, $\arg(\mathbf{P}_{21}) = \arg(\mathbf{P}_{22})$. \square

Note that for any number $0 \leq p \leq 3$, there always exists a phase factor $\phi \in \mathbb{C}^*$ so that if we set $\phi = \phi_s = \phi_t$, then $|-1 + \phi_t - \phi_s \phi_t| = p$. This implies that for any choice of phases $\tilde{\phi}_s, \tilde{\phi}_t \in \mathbb{C}^*$, there exists a phase factor $\phi \in \mathbb{C}^*$ so that the error if applying $\mathbf{Q}(\phi, \phi)$ is no larger than if applying $\mathbf{Q}(\tilde{\phi}_s, \tilde{\phi}_t)$. That is, picking identical phases is never suboptimal in terms of error reduction.

Picking identical phases is already known to have other advantageous properties. In work on Grover's algorithm, Long, Li, Zhang, and Niu [9], consider the choices of phases for which amplitude amplification may yield exact algorithms and they derive the phase matching condition $\phi_s = \phi_t$ (the term 'exact quantum algorithm' is explained in the next paragraph). Together with a later paper by Long, Xiao, and Song [8], they give a general and thorough analysis of the conditions we must put on ϕ_s and ϕ_t for obtaining exact algorithms. One instance of their scenario requires the *phase matching* condition $\phi_s = \phi_t$. Phase matching is particularly appealing as then the relationship between ϕ_s and ϕ_t

does not depend on ϵ , it helps simplifying the analysis, and it might be easier to implement just one phase factor instead of working with two.

Suppose we are given a classical randomized algorithm that succeeds in solving some problem with some probability $1 - \epsilon$. Then we may repeat the algorithm several times, hereby reducing the error probability. With only polynomially many repetitions, we can reduce the error to being exponentially small. However, there are no known schemes that would allow us to reduce the error to zero with only polynomial overhead for arbitrary processes. There are in short no general derandomization schemes. In contrast, amplitude amplification can be used to obtain exact quantum algorithms in some settings. We say a quantum algorithm is *exact* if its error probability is zero. Exact quantum algorithms for decision problems that run in polynomial time comprise the quantum analogue \mathcal{EQP} of the classical complexity class \mathcal{P} .

Under phase matching, the phase matrix simplifies to

$$P = P(\phi, \phi) = \begin{bmatrix} -\phi^2 & 1 - 2\phi \\ -1 + \phi - \phi^2 & -\phi \end{bmatrix}. \quad (4)$$

Theorem 2 gives a necessary and sufficient condition for having $\epsilon' < \epsilon$. It generalizes Theorem 1 under phase matching to include necessary conditions, and states that $\epsilon' < \epsilon$ if and only if $\text{Re}(\phi) > -\frac{\epsilon}{1-\epsilon}$ for nontrivial ϕ . The right hand side, $-\frac{\epsilon}{1-\epsilon}$, may be arbitrarily close to 0, and thus if the expression $\text{Re}(\phi) > -\frac{\epsilon}{1-\epsilon}$ is to be true for all nonzero ϵ , we effectively require that $\text{Re}(\phi) \geq 0$. Expressed in terms of trigonometric functions, $\epsilon' < \epsilon$ if and only if $\cos(\varphi) > -\tan^2(\theta)$ where $\phi = e^{i\varphi}$.

Theorem 2 (Error reduction with phase matching). *Suppose that $\phi = \phi_s = \phi_t$. Then*

$$\epsilon' = \begin{cases} = 0 & \text{if } \text{Re}(\phi) = \frac{1}{2}\left(1 - \frac{\epsilon}{1-\epsilon}\right) \\ < \epsilon & \text{if } \text{Re}(\phi) > -\frac{\epsilon}{1-\epsilon} \text{ and } \phi \neq 1 \\ = \epsilon & \text{if } \text{Re}(\phi) = -\frac{\epsilon}{1-\epsilon} \\ > \epsilon & \text{if } \text{Re}(\phi) < -\frac{\epsilon}{1-\epsilon}. \end{cases}$$

Proof. First note that $\epsilon' < \epsilon$ if and only if the absolute value of $P_{21}(1-\epsilon) + P_{22}\epsilon$ is less than one. If $\phi = \phi_s = \phi_t$ then $P_{21} = \phi(1 - 2\text{Re}(\phi))$ and $P_{22} = -\phi$, and thus $|P_{21}(1-\epsilon) + P_{22}\epsilon| = |(1 - 2\text{Re}(\phi))(1-\epsilon) - \epsilon|$. If $0 < \text{Re}(\phi) < 1$, then $|1 - 2\text{Re}(\phi)| < 1$ and hence $\epsilon' < \epsilon$. Now, suppose $\text{Re}(\phi) \leq 0$. Then $(1 - 2\text{Re}(\phi))(1 - \epsilon) - \epsilon < 1$ if and only if $\text{Re}(\phi) > -\frac{\epsilon}{1-\epsilon}$.

Similarly, if $\text{Re}(\phi) < -\frac{\epsilon}{1-\epsilon}$ then $\epsilon' > \epsilon$. Finally, $(1 - 2\text{Re}(\phi))(1 - \epsilon) - \epsilon = 0$ if and only if $\text{Re}(\phi) = \frac{1}{2}\left(1 - \frac{\epsilon}{1-\epsilon}\right)$. \square

It follows that any phase factor with positive real ensures strict error reduction.

Corollary 1 (Strictly decreasing error). *If $\phi_s = \phi_t \neq 1$ and $0 \leq \text{Re}(\phi_s) < 1$, then $\epsilon' < \epsilon$.*

It ϵ is known [1], we can obtain an exact quantum algorithm by choosing the phase factor ϕ so that $P_{21}(1 - \epsilon) + P_{22}\epsilon = 0$.

Corollary 2 (Exact algorithm). *If $\phi_s = \phi_t$ and $\text{Re}(\phi_s) = \frac{1}{2}(1 - \frac{\epsilon}{1-\epsilon})$, then $\epsilon' = 0$.*

Note that the condition $\text{Re}(\phi_s) = \frac{1}{2}(1 - \frac{\epsilon}{1-\epsilon})$ can be satisfied if and only if $\epsilon \leq \frac{3}{4}$. That is, we can achieve $\epsilon' = 0$ by a one-round amplitude amplification process if and only if the original error ϵ is at most $\frac{3}{4}$.

The next theorem states that phase matching with a phase factor $\phi \in \mathbb{C}^*$ with $\text{Re}(\phi) \leq \frac{1}{2}$ is never suboptimal in terms of error reduction. This implies that when applying amplitude amplification (as considered in this paper) we may restrict our attention to picking a single phase factor ϕ with $-1 \leq \text{Re}(\phi) \leq \frac{1}{2}$, as opposed to considering all possible choices of pairs $(\phi_s, \phi_t) \in \mathbb{C}^* \times \mathbb{C}^*$.

Theorem 3 (Phase matching with $\text{Re}(\phi) \leq \frac{1}{2}$). *For all phase factors $\phi_s, \phi_t \in \mathbb{C}^*$ there exists a phase factor $\phi \in \mathbb{C}^*$ with $\text{Re}(\phi) \leq \frac{1}{2}$ so that the error of $Q(\phi, \phi)A|s\rangle$ is no larger than the error of $Q(\phi_s, \phi_t)A|s\rangle$. Phase factor ϕ depends only on ϕ_s and ϕ_t , and not on A , $|s\rangle$, and $|t\rangle$.*

Proof. Let ϵ denote the error probability of $Q(\phi_s, \phi_t)A|s\rangle$. By the comments succeeding Lemma 2, we can without loss of generality assume that $\phi = \phi_s = \phi_t$ and thus use the simplified matrix given by Eq. 4. If we pick ϕ so that $\text{Re}(\phi) = \frac{1}{2}$, then $|(1 - 2\text{Re}(\phi))(1 - \epsilon) - \epsilon| = \epsilon$ whereas if $\text{Re}(\phi) > \frac{1}{2}$ then $|(1 - 2\text{Re}(\phi))(1 - \epsilon) - \epsilon| > \epsilon$. It follows that using ϕ with $\text{Re}(\phi) > \frac{1}{2}$ is never better than using ϕ with $\text{Re}(\phi) = \frac{1}{2}$. \square

We mention that picking conjugate phases aligns the entries P_{11} and P_{12} .

Proposition 3 (Conjugate phase matching). *$\arg(P_{11}) = \arg(P_{12})$ if and only if (1) $\phi_s = \overline{\phi_t}$ and $\text{Re}(\phi_s) > \frac{1}{2}$, (2) $\phi_s = 1$, or (3) $\phi_t = 1$.*

6 Computational considerations

Thus far we have primarily been concerned with error reduction in amplitude amplification and mostly ignored the computational costs. Amplitude amplification maps operator A to operator $A_1 = QA$,

$$A \mapsto A_1 = AR_sA^{-1}R_tA \quad (5)$$

at the cost of in total three applications of A and its inverse, and one application of each of R_s and R_t . We may repeat the amplification process on the thus formed algorithm A_1 , mapping

$$A_1 \mapsto A_2 = A_1R_sA_1^{-1}R_tA_1.$$

Applying the mapping k times utilizes $\frac{1}{2}(3^k + 1)$ applications of A , $\frac{1}{2}(3^k - 1)$ applications of the inverse A^{-1} , and $\frac{1}{2}(3^k - 1)$ applications of each of the pseudo-reflections R_s and R_t . That is, we use $\Theta(K)$ applications of each of the four operators A, A^{-1}, R_s, R_t , where $K = 3^k$.

The error ϵ' after k recursive applications of the mapping given by Eq. 5 depends on the choice of phase factors. If we apply Q with phase factor $e^{i\pi/3}$, then $\epsilon' = \epsilon^K$. This error is the exact same error as we could achieve by K classical repetitions, as exemplified in Section 3. Amplitude amplification with phase factor $e^{i\pi/3}$ is a genuinely quantum mechanical version of classical repetition. Note that $\text{Re}(e^{i\pi/3}) = \frac{1}{2}$. By Theorem 3, applying amplitude amplification with a phase factor ϕ having $\text{Re}(\phi) > \frac{1}{2}$ is suboptimal in terms of error reduction.

For matching phases ϕ with $\text{Re}(\phi) < \frac{1}{2}$, the error reduction β^2 is given by the square of $(1 - 2\text{Re}(\phi))(1 - \epsilon) - \epsilon$, where β is defined by Eq. 3. The factor of error reduction by three classical repetitions is $\frac{\epsilon^3}{\epsilon} = \epsilon^2$. Amplitude amplification is thus superior to classical boosting if and only if $-\epsilon < (1 - 2\text{Re}(\phi))(1 - \epsilon) - \epsilon < \epsilon$ which is valid if and only if $\frac{1}{2} \frac{1-3\epsilon}{1-\epsilon} < \text{Re}(\phi) < \frac{1}{2}$. The left-hand side $\frac{1}{2} \frac{1-3\epsilon}{1-\epsilon}$ is less than -1 if $\epsilon > \frac{3}{5}$, in which case the error reduction β^2 in amplitude amplification $Q(-1, -1)$ with phase factor $\phi = -1$ is better than the classical error reduction of ϵ^2 obtained by three repetitions.

Theorem 4 (Amplitude amplification works well for large error). *For $\epsilon > \frac{3}{5}$, amplitude amplification with phase factor $\phi = -1$ is superior to classical repetition.*

Buhrman, Cleve, de Wolf, and Zalka show in [4] that any quantum algorithm for improving the error from a constant, say $\frac{1}{2}$, to δ requires $\Omega(\log \frac{1}{\delta})$ applications of A . In particular, for small ϵ , amplitude amplification requires asymptotically the same number of applications of A as does classical repetition. The above theorem implies that in the range $1 > \epsilon > \frac{3}{5}$, standard amplitude amplification with phase factor $\phi = -1$ is superior to classical boosting in terms of error reduction.

7 Concluding remarks

Amplitude amplification is one of the most used and well-studied primitives in quantum algorithmics. One of its obstacles is that applying standard amplitude amplification (with phase factor -1) can sometimes be harmful. If the given quantum algorithm A has small error, then applying amplitude amplification may produce an algorithm QA that has larger error than A itself. It is in most cases not desirable to use computational efforts in creating worse algorithms.

In recent work [7], Grover shows that applying amplitude amplification with phase factor $e^{i\pi/3}$ is never harmful. If the error of algorithm A is ϵ , then amplitude amplification produces an algorithm QA with error ϵ^3 , which is never larger than ϵ . The limitation of the phase factor $e^{i\pi/3}$ is that the exact same error reduction can be achieved using the same computational efforts by classical repetition.

Applying amplitude amplification as a subroutine, as is done in many quantum algorithms, can be a challenge: Phase factor -1 might be harmful, phase factor $e^{i\pi/3}$ leads to no better error reduction than classical. Possibly one may consequently decide to choose phase factors ϕ_s, ϕ_t somewhere in between in lack of better.

In this paper, we provide a set of tools and results on picking phase factors. There is no unifying answer on phase picking—the preferable choice depends on the application at hand. We give a novel and simple, yet rigorous, analysis of the interplay between phase factors and error reduction. We show that one may always limit oneself to consider matching phases $\phi = \phi_s = \phi_t$ with argument in the range $\frac{\pi}{3} \leq \arg(\phi) \leq \pi$. We show that any phase with $\operatorname{Re}(\phi) > 0$ reduces the error for all $0 < \epsilon < 1$. The optimal choice in terms of error reduction is to pick $\phi = -1$ if $\epsilon \geq \frac{3}{4}$ and otherwise to pick ϕ so that $\operatorname{Re}(\phi) = \frac{1}{2} \frac{1-2\epsilon}{1-\epsilon}$.

Grover’s work has already lead to new applications based on the pivotal phase factor $e^{i\pi/3}$ [10, 11]. Our set of analytical tools and results may initiate other results related to amplitude amplification and quantum error reduction in more general settings.

References

1. M. Boyer, G. Brassard, P. Høyer, and A. Tapp. Tight bounds on quantum searching. *Fortschr. Phys.*, **46**(4-5):493–505, 1998.
2. G. Brassard and P. Høyer. An exact quantum polynomial-time algorithm for Simon’s problem. In *Proc. 5th Israeli Symp. Theory of Comput. and Systems*, pp. 12–23, 1997.
3. G. Brassard, P. Høyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. In: *Quantum Computation and Quantum Information: A Millennium Volume. AMS Contemp. Math.*, **305**:53–74, 2002.
4. H. Buhrman, R. Cleve, R. de Wolf, and Ch. Zalka. Bounds for small-error and zero-error quantum algorithms. In *Proc. 40th IEEE Symp. Found. Comput. Sci.*, pp. 358–368, 1999.
5. L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. 28th ACM Symp. Theory Comput.*, pp. 212–219, 1996.
6. L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, **79**(2):325–328, 1997.
7. L. K. Grover. A different kind of quantum search. quant-ph/0503205, May 2005.
8. G.-L. Long, X. Li, and Y. Sun. Phase matching condition for quantum search with a generalized initial state. *Phys. Lett. A*, **294**(3-4):143-152, 2002.
9. G.-L. Long, Y. S. Li, W. L. Zhang, and L. Niu. Phase matching in quantum searching. *Phys. Lett. A*, **262**(1):27–34, 1999.
10. T. Tulsi, L. K. Grover, and A. Patel. A new algorithm for directed quantum search. quant-ph/0505007, May 2005.
11. L. Xiao and J. Jones. An NMR implementation of Grover’s fixed-point quantum search algorithm. quant-ph/0504054, April 2005.