www.nature.com/scientificreports

SCIENTIFIC REPORTS

OPEN

Quantum Error Correction Protects Quantum Search Algorithms Against Decoherence

Received: 02 June 2016
Accepted: 04 November 2016
Published: 07 December 2016

Panagiotis Botsinis, Zunaira Babar, Dimitrios Alanis, Daryus Chandra, Hung Nguyen, Soon Xin Ng & Lajos Hanzo

When quantum computing becomes a wide-spread commercial reality, Quantum Search Algorithms (QSA) and especially Grover's QSA will inevitably be one of their main applications, constituting their cornerstone. Most of the literature assumes that the quantum circuits are free from decoherence. Practically, decoherence will remain unavoidable as is the Gaussian noise of classic circuits imposed by the Brownian motion of electrons, hence it may have to be mitigated. In this contribution, we investigate the effect of quantum noise on the performance of QSAs, in terms of their success probability as a function of the database size to be searched, when decoherence is modelled by depolarizing channels' deleterious effects imposed on the quantum gates. Moreover, we employ quantum error correction codes for limiting the effects of quantum noise and for correcting quantum flips. More specifically, we demonstrate that, when we search for a single solution in a database having 4096 entries using Grover's QSA at an aggressive depolarizing probability of 10^{-3}, the success probability of the search is 0.22 when no quantum coding is used, which is improved to 0.96 when Steane's quantum error correction code is employed. Finally, apart from Steane's code, the employment of Quantum Bose-Chaudhuri-Hocquenghem (QBCH) codes is also considered.

Moore's law is expected to delve in the quantum world in the early 2020 s, since quantum effects will appear when trying to further shrink the scale of the integration in classic chips[1]. Quantum computing may be one of the ways forward, promising substantial speed-up in some applications, when compared to the existing classical solutions. Grover's Quantum Search Algorithm (QSA)[2,3] succeeds in finding a specific desired entry out of the N entries in an unsorted database with ~100% success probability, after evaluating as few as $O(\sqrt{N})$ entries. One of the main assumptions that are adopted for achieving this near-perfect success is that the quantum bits or *qubits*, which take part in Grover's QSA, will only have their quantum state changed, if they pass through quantum gates, as described in the postulates of quantum mechanics[4–6]. In other words, in order to achieve ~100% success probability, the qubits experience no bit- or phase-flips between gates.

Quantum computing and quantum search algorithms may be beneficially exploited in diverse large-scale applications in wireless communications, such as multiple stream detection[7–11] or routing[12,13]. Numerous challenging optimization problems in wireless communications will be solved more efficiently by quantum search algorithms relying on Grover's QSA. In the Supplementary Section 3, we state a number of applications that may benefit from the employment of quantum search algorithms. However, when quantum computing systems become a wide-spread commercial reality, it is expected that errors will occur in the quantum circuits, due to the inevitable presence of quantum noise, conventionally termed as *decoherence*[4]. More precisely, decoherence is due to the deleterious interaction of the constituent qubits with the environment, which perturbs the flawless superposition of states[14–18]. The resultant errors, occurring between the application of two quantum gates even when highly fault-tolerant gates[16–18] are employed, may be modelled by the so-called depolarizing channels.

Similarly to classical error correction codes, the errors in the quantum domain may be corrected by employing quantum error correction codes. More explicitly, up to a limit, quantum codes rectify the impact of quantum noise for the sake of ensuring that the qubits retain their coherent quantum state with a high fidelity, which is a measure of "closeness" of two quantum states[19], thus in effect beneficially increasing the coherence time of the unperturbed quantum state. This has been experimentally demonstrated in refs 20–22. The inception of quantum codes dates back to 1995 when Shor[14] conceived the first quantum code, which was however only capable of

Southampton Wireless, School of Electronics and Computer Science, University of Southampton, United Kingdom. Correspondence and requests for materials should be addressed to L.H. (email: lh@ecs.soton.ac.uk)

correcting a single error. Since then the quest for approaching the quantum capacity bounds has continued. In this context, the astounding performance of quantum turbo codes[23–25], quantum-domain low density parity check codes[26–28] and quantum polar codes[29,30], which rely on long streams of information qubits, is of particular significance. However, we will argue that from an implementation-oriented perspective and particularly for application in Grover's QSA, the employment of short block codes is more feasible. Hence, in this treatise, we invoke Steane's Code[31] and Quantum Bose-Chaudhuri-Hocquenghem (BCH) codes[32–34] for improving the search-success probability of Grover's QSA, by substantially reducing the qubit error ratio of each link between a pair of serially concatenated gates.

Various noise models impairing Grover's QSA have been proposed[35–41] and some also have employed quantum error correction[35,42]. However, there is no study on the effect of depolarizing channels in diverse locations of the index register in generic Grover architectures, with no prior knowledge of the solution index, in conjunction with Steane's code or the QBCH code employed and evaluated in multiple search scenarios. Based on the aforementioned background, our novel contributions are:

1. We propose a system model, where depolarizing channels represent the deleterious effects of quantum errors between the employment of two consecutive quantum gates. The model is capable of describing the errors occurring to the index register in every part of Grover's operator, while distinguishing the index and the value registers in the Oracle and without prior knowledge of the problem's solution state.
2. We propose quantum error correction codes, such as the Steane Code[31] and Quantum Bose-Chaudhuri-Hocquenghem (QBCH) code[32–34] for detecting and correcting the qubit errors. The performance of the codes is presented in terms of Grover's QSA's success probability.
3. We characterize the effect that qubit errors have on the success probability of Grover's QSA, as well as the specific effect of the location of these errors in the quantum circuit have on the success probability of Grover's QSA. We statistically characterize the performance of Grover's realistic imperfect QSA, in terms of the number of Grover iterations L, the size of the database N and the depolarizing probabilities.

The structure of the paper is as follows. In the following section, we analyse Grover's idealized perfect QSA and its performance, when quantum decoherence and quantum noise is not an issue. Moreover, we investigate the effect that quantum noise has on the success probability of Grover's QSA. Then, we propose the employment of short quantum error correction codes for combating the performance degradations. Finally, our conclusions are offered in the corresponding Section.

Grover's Idealized Quantum Search Algorithm

In quantum computing, the unit of quantum information is the qubit $|q\rangle$, which may be found in the quantum states $|0\rangle$, $|1\rangle$, or a superposition of $|0\rangle$ and $|1\rangle$ as in $|q\rangle = a|0\rangle + b|1\rangle$, where the amplitudes of the quantum states a and b satisfy $|a|^2 + |b|^2 = 1$ and $a,\ b \in \mathbb{C}$. When a *measurement* or *observation* of a qubit $|q\rangle$ takes place, it may be found in the state $|0\rangle$ with $|a|^2$ probability or $|1\rangle$ with $|b|^2$ probability. The evolution of quantum states is manipulated with the aid of unitary operators or gates[4]. One of the most commonly used unitary gates is the Hadamard operator H, which carries out the operation of $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Multiple qubits may be processed together for forming composite systems. For example, two qubits $|q_1q_2\rangle$ may be found in the general state $|q_1q_2\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$, in conjunction with $|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$. Depending on whether the qubits of a composite system may be described separately or not, the quantum state is termed as *separable* or *entangled*[4]. For example, the 2-qubit quantum state $(|00\rangle + |11\rangle)/\sqrt{2}$ represents an entangled state, where a potential measurement of the first qubit directly determines the quantum state of the entangled qubit.

In Grover's QSA, the amplitudes of the quantum states are real-valued, as in $a,\ b \in \mathbb{R}$. Grover's QSA efficiently solves a search problem, where given a known value δ, the goal is to find a specific index x or address of a database of size N, which stores the known value δ. This can also be described with the aid of the function $f(x) = \delta$. More explicitly, Grover's QSA succeeds in finding the desired index x with ~100% probability of success, by observing the final composite system after applying Grover's operator $\mathcal{G}$, which is constituted by an L-fold serial concatenation of quantum gates. In order for Grover's operator to succeed in finding the address containing the value δ, the number of solutions S, which determines the number of different database indices x_i that correspond to $f(x_i) = \delta$, has to be known *a priori*.

The quantum circuit of Grover's operator $\mathcal{G}$[2,3] is given in Fig. 1. In the same figure, we have included the potential positions, where it will be assumed in this paper that depolarization takes place in future practical implementations of Grover's QSA. Grover's QSA employs $n = \log_2(N)$ qubits and initializes them in an equiprobable superposition of all legitimate states as in

$$|q\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle, \qquad (1)$$

where $|x\rangle \in \{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$ is the decimal representation of the quantum states that the qubits are found in. For instance, we have $|00000\rangle \equiv |0\rangle$ and $|10110\rangle \equiv |22\rangle$. Initially, Grover's operator $\mathcal{G}$ applies the Oracle O, which is a unitary operator that "marks" the S specific quantum states, which represent solutions to the search problem, by flipping their sign. In other words, the Oracle maps $|x\rangle \to -|x\rangle$, only if $f(x) = \delta$. The quantum states that are not solutions of the search problem remain unaltered by the Oracle's operation. The next three quantum gates HP_0H of Fig. 1 describe the *diffusion* operator, which consists of the Hadamard operator applied twice and a phase flip gate, which maps $|x\rangle \to -|x\rangle$, only if $|x\rangle \neq |0\rangle$, while applying the identity operation to the quantum state $|0\rangle$. The

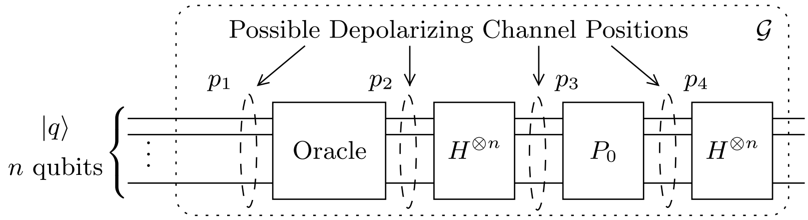


Figure 1. Quantum circuit of Grover's operator $\mathcal{G}$, along with the potential depolarizing channels' positions. The input quantum state $|q\rangle$ may either be in an equiprobable superposition of states, or the output of the previous application of Grover's operator. The depolarizing probability of the channel in the ith position is equal to p_i. The number of information qubits involved in each search is equal to $n = \log_2(N)$, where N is the size of the database. An auxiliary qubit is employed in the Oracle operator.

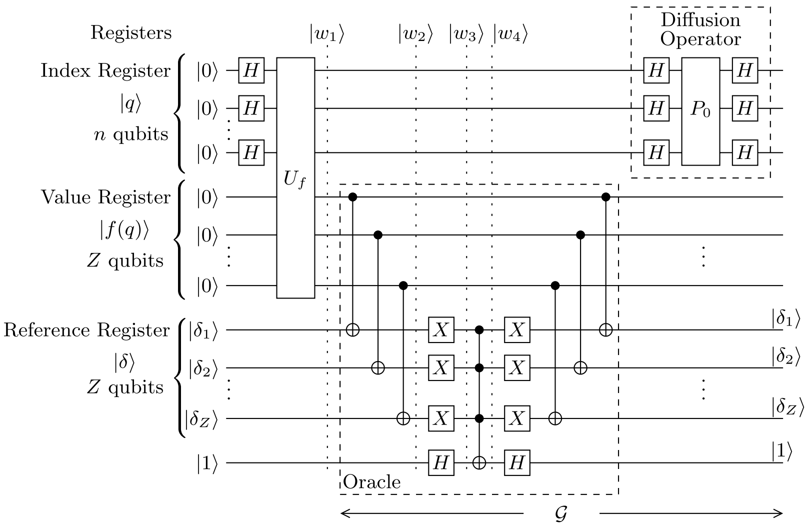


Figure 2. Quantum Circuit of Grover's QSA, showing the initialization and a single Grover iteration, which consists of a sequential employment of the Oracle and the Diffusion operator. In this architecture, only the index register is required to be maintained in a superposition of states outside the Oracle operator.

aim of Grover's QSA is to stop applying Grover's operator $\mathcal{G} = HP_0H \cdot O$ after a specific number of times L_{opt}, so that the resultant probability of success is as close to unity as possible (see Supplementary Section 4). The optimal number L_{opt} of Grover iterations, which maximizes the probability of success is equal to[43]

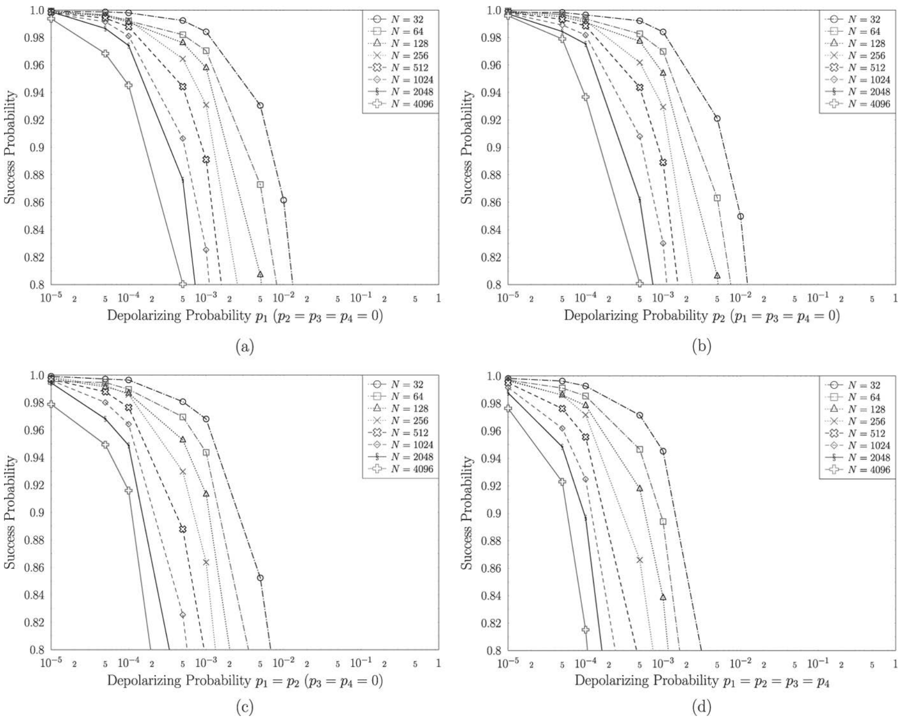
$$L_{opt} = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{S}} \right\rfloor. \tag{2}$$

The architecture of Grover's operator $\mathcal{G}$ is depicted in Fig. 2. Only the index register is visible in Fig. 1. The proposed noise model of Fig. 1, in conjunction with the architecture of Fig. 2 considers all possible noise locations of the index register in the Grover circuit, as it will be further explained in the next Section.

Imperfect Grover Quantum Search

If perturbations are imposed by the depolarizing channels on the quantum circuit of Fig. 1, each qubit may be affected by a bit flip termed as an X-error, a phase flip termed as a Z-error, or both a phase and a bit flip termed as a $Y = XZ$-error[4]. The depolarizing channel that models the depolarizing effects inflicts one of the three aforementioned qubit errors independently upon each qubit with a probability of $p/3$, where $p \in [0, 1]$ is the depolarizing probability of the channel. If a qubit remains unaffected by the channel with a probability of $(1 - p)$, it may be described as if the identity operator I was applied to it.

The fact that the quantum perturbations may occur independently on each of the $n = \log_2(N)$ qubits is translated in two or more quantum states, if $S > 1$, that represent solutions having a different amplitude at any point. Similarly, two or more quantum states that are not solutions may have a different amplitude and therefore a different probability to be observed. Figure 3 depicts the success probability of Grover's QSA, when a realistic practical circuit is subjected to a depolarizing channel, where $[p_1, p_2, p_3, p_4]$ corresponds to the depolarizing probabilities at four different locations in the circuit, as stated in Fig. 1, when the architecture of Fig. 2 is used. More specifically, we have introduced four different scenarios, where the depolarizing channels perturb the



(a)

(b)

(c)

(d)

Figure 3. Success probability of Grover's QSA, when depolarizing channels occur (**a**) only before the Oracle, (**b**) only right after the Oracle, (**c**) only before and right after the Oracle, (**d**) in all locations on Grover's operator's circuit, shown in Fig. 1, with respect to the depolarizing probability of the channels, when the architecture of Fig. 2 was used. Randomly generated databases with different sizes N were used, while a single solution $S = 1$ was present in a random position in the database in each search problem.

system only before the Oracle, associated with $[p_1, 0, 0, 0]$; only after the Oracle and before the first Hadamard gate, associated with $[0, p_2, 0, 0]$; both right before and right after the Oracle, associated with $[p_1, p_2, 0, 0]$; and finally, in every possible location, associated with $[p_1, p_2, p_3, p_4]$. Since the index register remains unaltered during a U_f operation, any bit flip or phase flip that may occur on the index register between the two U_f gates of Fig. 2, may be equivalently modelled as an error on the index register occurring after the Oracle and before the diffusion operator. The index register may be stored in a quantum memory[42], where quantum stabilizer codes are periodically employed, until the Oracle operation has been completed. A similar procedure may be applied for the value register, when the diffusion operator is applied to the index register. It should be noted that in every scenario of this contribution, all the non-zero depolarizing probabilities are set to be equal to each other, for the simplicity of presentation. In practice, the depolarizing probabilities may differ. A step-by-step example is provided in Supplementary Section 5. In Fig. 3, we have employed Grover's QSA to various randomly generated databases having different sizes N, for a sufficiently high number of times. All databases have a single solution $S = 1$, represented by a randomly selected quantum state. In each of the scenarios, Grover's QSA was stopped after L_{opt} number of iterations, as if it was based on an ideal, perturbation-free circuit, where L_{opt} was calculated according to (2) for a database size N and for $S = 1$ solution.

We may observe in Fig. 3 that the success probability is degraded when the size of the database N is increased, regardless of the specific locations of the depolarizing perturbations. This is expected, since when the search is performed in a larger database, more qubits are involved, therefore more errors will occur and due to the error propagation in the circuit, the success probability will be reduced. At the same time, the optimal number L_{opt} of iterations is higher in databases having higher size N, as encapsulated in (2), while keeping the number of solutions S fixed, allowing more depolarizing errors to affect the qubits and subsequently to reduce Grover's QSA's success probability. By comparing Fig. 3a to Fig. 3b, the success probability of Grover's QSA is seen to be similar for the same database size, indicating that the presence of depolarizing perturbations right before or right after the Oracle imposes a similar performance degradation on Grover's QSA. However, if depolarizing is inflicted both right before and right after the Oracle, the success probability of Grover's QSA erodes, as illustrated in Fig. 3c, due to the error propagation within the quantum circuit. This is also verified by Fig. 3d, where a depolarizing perturbations is imposed at every possible location of Fig. 1, resulting in a degraded performance, when compared to the other three scenarios.

Figure 4 presents the success probability of Grover's QSA for various database sizes and for diverse values of the depolarizing probability p_1, when quantum perturbations are only imposed right before the Oracle operator during each Grover iteration, in the architecture of Fig. 2. Each search problem includes a single solution associated with $S = 1$, randomly placed in the database. It may be observed that the inherent periodicity of Grover's QSA with respect to the number L of applying Grover's operator $\mathcal{G}$ is lost, while increasing the depolarizing probability, due to the associated error propagation, which becomes more and more dominant as more depolarizing perturbations are imposed on the search process. Once again, the effect that quantum perturbations have on larger databases is more catastrophic, than that inflicted upon smaller databases, since more error-prone qubits are employed. It is worth mentioning that according to Fig. 4a,b,c and d, when a depolarizing channel is introduced, the optimal number L_{opt} of Grover iterations, required for maximizing the success probability becomes lower upon increasing the depolarizing probability p_1. At the same time though, the maximum success probability that corresponds to L_{opt} is reduced as p_1 is increased.

Quantum Error Correction in Grover's Quantum Search Algorithm

In order to improve the performance of Grover's QSA, when quantum perturbations are present in the quantum circuit, quantum error correction codes may be employed. The quantum error correction codes may impose redundancy on the information, or *logical* qubits, at the positions in the circuit of Fig. 1, where quantum noise may appear and then flawlessly decode by correcting the quantum flips before the application of the subsequent unitary operator of the quantum circuit. For example, in the quantum circuit of Grover's operator in Fig. 1, quantum error correction codes may be used for encoding and decoding the information qubits, which will eventually be observed between each unitary operator. Naturally, since encoding and decoding quantum information itself needs unitary operators, the exact locations of where it is beneficial to include quantum error correction codes for stabilizing the quantum information states will be decided based on the technology selected for implementing quantum computers. In our proposed model, we have opted for introducing depolarizing perturbations between the main unitary operators of Grover's QSA for clarity and for ease of demonstrating its benefits, while stating that in practice quantum noise may also be present within the quantum operators, such as the Oracle operator for instance.

In general, quantum turbo codes[23–25], quantum low density parity check codes[26–28] and quantum polar codes[29,30], require a long stream of information qubits for achieving their full potential. Since the $n = \log_2(N)$ information qubits of Grover's QSA, presented in Fig. 1, are used simultaneously in parallel by each quantum gate, quantum codes that operate well with a short information qubit stream, such as Steane code[31] and QBCH codes[32–34], may be better suited for combating quantum perturbations in quantum search algorithms. Both the Steane code as well as the QBCH codes belong to the family of stabilizer codes[44,45], which is a generalized formalism for designing quantum codes from the known family of classical codes. The encoding circuit of the QBCH code is designed using the methodology of ref. 46, which is detailed in the Methods Section. Usually, the encoding and decoding circuits are assumed to be fault-tolerant[35,42,47]. Assuming erroneous encoders or decoders, the noise imposed may be represented by appropriately adjusting the depolarizing probabilities of the noise model.

Figure 5 shows the general schematic of a quantum system relying on a stabilizer code. An $[\mathtt{n,\ k}]$ stabilizer code maps a k-qubit information word, or k *logical* qubits, $|q\rangle$ onto an n-qubit codeword, or n *physical* qubits, $|\overline{q}\rangle$ with the aid of $(\mathtt{n} - \mathtt{k})$ ancillary qubits initialized to the state $|0\rangle$. Furthermore, if $\mathcal{P}$ is the channel error inflicted on the codewords, then $|\hat{\overline{q}}\rangle = \mathcal{P}|\overline{q}\rangle$ is the noisy codeword received at the decoder. A 3-step decoding process is then invoked for recovering the intended transmitted information $|\tilde{q}\rangle$, as described in the Methods Section and exemplified in Supplementary Section 6 with the aid of a step-by-step example.

Employment of Stabilizer Codes in Grover's Algorithm

In Fig. 6 we characterize the performance of Grover's QSA, in terms of the probability of successfully finding the single solution, when the Steane code having a coding rate of $R = 1/7$ is employed in the specific locations, where depolarizing perturbations appear in the architecture of Fig. 2. Four different scenarios have been investigated for various database sizes N, while including only a single solution associated with $S = 1$ in each search. We may observe that regardless of the locations of the depolarizing perturbations, the Steane code improves the performance of Grover's QSA. Quantitatively, Steane code is capable of correcting quantum errors, when the depolarizing probability is equal to or lower than approximately $5 \cdot 10^{-2}$. The Quantum Bit Error Ratio (QBER) improvement offered by the Steane code is increased, when the depolarizing probability is reduced, since the probability of overwhelming this single-error correcting code is reduced, which would result in correcting the wrong qubits, thereby inflicting extra errors. This is the reason why in Fig. 6 the improvement is more significant, when larger databases, associated with higher N values, are used. For example, based on Fig. 6d, when searching in a database of $N = 4096$, the system employing the Steane code may achieve a success probability of 0.98 for depolarizing probabilities 80 times higher than those required by the uncoded quantum search for achieving the same probability of success.

Similarly to their uncoded counterparts, the quantum systems that employ quantum error correction during the quantum search are affected by the quantum perturbations within the quantum circuit. More precisely, as we may observe in Fig. 6a and b, which correspond to the scenarios, where depolarizing may occur only right before or only right after the Oracle operator, respectively, they exhibit an equivalent performance. However, when quantum noise is present in both the aforementioned locations, according to Fig. 6c the success probability is reduced, even when quantum error correction is used. Finally, based on Fig. 6d, as expected due to error propagation, a degraded performance is achieved, when depolarizing perturbations occur everywhere in Grover's QSA circuit of Fig. 1.

In order to delve deeper into the intuition of depolarizing in Grover's QSA's circuit, let us investigate a scenario, where we have a database of size $N = 1024$ and $S = 1$ solution, which may be considered as the "worst-case" scenario, since according to (2) the maximum possible number of Grover iterations will be required for a fixed database size, when $S = 1$. Let us also assume that quantum perturbations may affect the qubits right before or right after the Oracle operation of Fig. 1, associated with $p_3 = p_4 = 0$. The curve of Grover's ideal QSA seen in Fig. 7 represents the upper limit of the achievable performance for each application of Grover's operator, since it corresponds to the case, where $p_1 = p_2 = p_3 = p_4 = 0$. It should be noted that in this scenario the optimal number

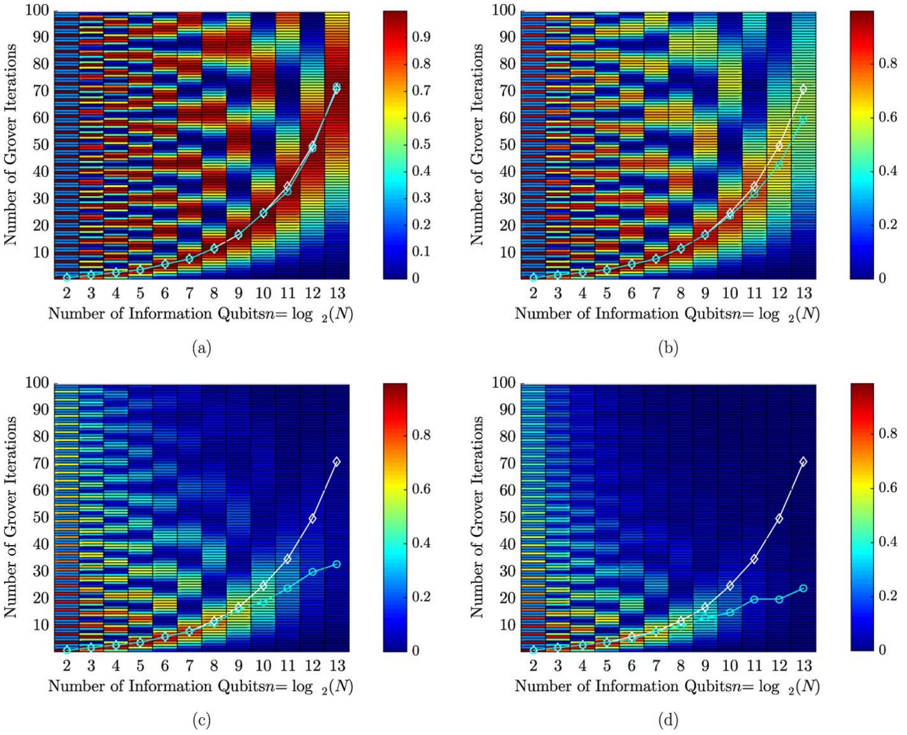


Figure 4. Success probability of Grover's QSA, when a depolarizing channel appears only right before the Oracle in Grover's operator's circuit, shown in Fig. 1, with respect to the depolarizing probability of the channel (**a**) $p_1 = 10^{-4}$, (**b**) $p_1 = 10^{-3}$, (**c**) $p_1 = 5 \cdot 10^{-3}$, (**d**) $p_1 = 10^{-2}$, the size of the database *N* and the number of Grover iterations *L*. The circuit architecture of Fig. 2 was employed. Randomly generated databases with different sizes *N* were used, while a single solution $S = 1$ was present in a random position in the database in each search problem. The white curve marked by the diamonds indicates the optimal number of Grover iterations L_{opt} that would be required in the ideal Grover's QSA, associated with $p_1 = 0$, while the cyan curve marked by the circles represents the actual optimal number of Grover iterations for the specific value of depolarizing probability p_1.

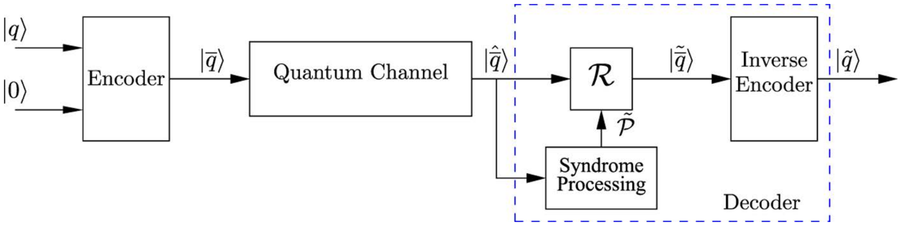
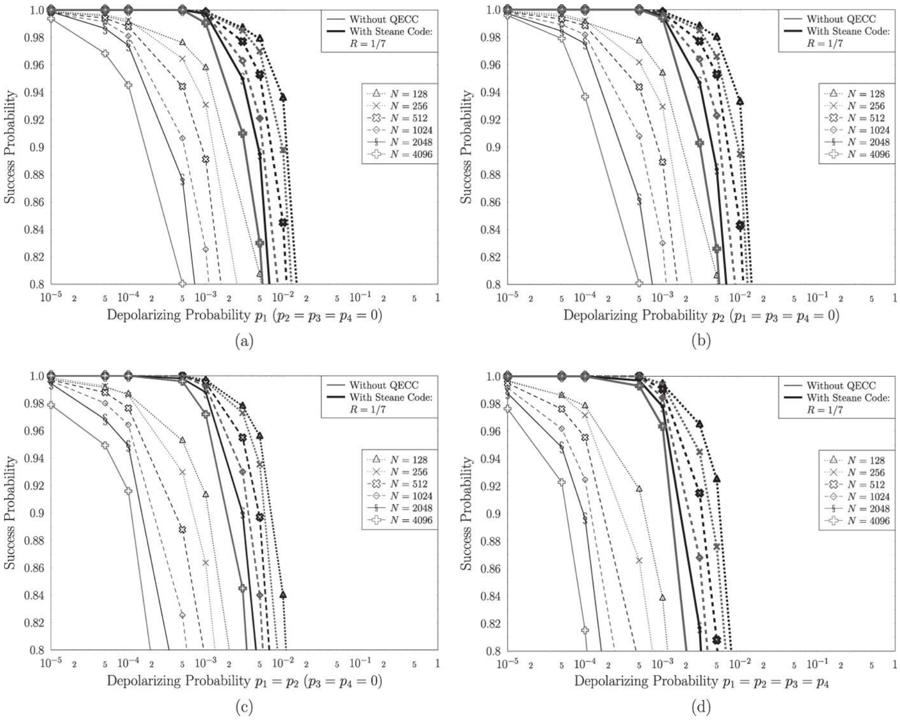


Figure 5. General schematic of a quantum system employing a stabilizer code.

of Grover iterations, given by (2), is equal to $L_{opt} = 25$. According to Fig. 7, when the quantum noise affects a qubit with a probability of $p_1 = p_2 = 10^{-3}$, the performance of the quantum search employing Steane's code for quantum error correction is near-optimal, reaching a success probability of 99.3% at $L = 25$ Grover iterations, indicating the ability of Steane's code to correct both the bit and phase flips introduced by the depolarizing perturbations. On the other hand, if no quantum error correction was employed for mitigating the effects of the depolarizing perturbations, the maximum achievable probability of success is equal to 66.7% at $L = 24$ Grover iterations. The performance degradation becomes higher, when the depolarizing probability is increased. Still based on Fig. 7, if we have say $p_1 = p_2 = 3 \cdot 10^{-3}$, then by using Steane's code we may reach a maximum success probability of 95.3% at $L = 25$ Grover iterations, instead of an inferior 33.3%, which would be the case if no quantum error correction was employed.

Since the QBCH[15, 7] is a block code, it may be used in a database associated with $n = 7$ information qubits, which results in a database with $N = 2^n = 128$ entries, so that all the qubits participate in the same encoding process. Even though the performance is expected to be worse than that of the Steane code, the coding rate of the QBCH[15, 7] code is higher than that of Steane code's. More specifically, the QBCH[15, 7] has a coding rate of $R_{QBCH[15,7]} = 7/15 = 0.47$, while Steane's code has a coding rate of $R_{Steane} = 1/7 = 0.14$. A QBCH[n, k] code associated with k logical qubits may also be employed in databases (n/k) times in parallel, where the number



(a) (b) (c) (d)

Figure 6. Success probability of Grover's QSA, when quantum noise occurs (**a**) only before the Oracle, (**b**) only right after the Oracle, (**c**) only before and right after the Oracle, (**d**) in all locations on Grover's operator's circuit, shown in Fig. 1, with respect to the depolarizing probability of the channels, when the architecture of Fig. 2 was used**.** Steane code with rate $R = 1/7$ has been employed for improving the performance of Grover's QSA. Randomly generated databases with different sizes N were used, while a single solution $S = 1$ was present in a random position in the database in each search problem.

of information qubits n is a multiple of its number of logical qubits k. For instance, the QBCH[15, 7] code may be used $(n/\text{k}) = 2$ times in parallel for Grover's QSA in databases associated with $n = 14$, which is translated into databases having a size of $N = 2^n = 16384$, encoding the first $k = 7$ qubits with each other, as well as the last $n - k = 7$ qubits with each other. Furthermore, the QBCH[15, 7] code may be combined with Steane's code for providing a hybrid combination of quantum error correction. For example, if we have a database associated with $N = 1024$ entries, we require $n = 10$ qubits in the index register. The QBCH[15, 7] code may be used for encoding the first 7 qubits, while the last 3 qubits may be encoded using Steane's code, requiring $15 + 7 \cdot 3 = 41$ physical qubits in total, instead of the 70 qubits that would be required by exclusively using Steane's code. However, a degraded performance is expected, when compared to using only Steane's code. Naturally, if a universal quantum computer processes multiple quantum algorithms simultaneously, information qubits of different processes may be encoded using the same quantum code for stabilizing purposes, if the timing allows it.

Let us compare the influence that the QBCH[15, 7] code has on Grover's QSA to that of Steane's code, when a quantum search is performed in a database having $N = 2^n = 128$ entries, where a single solution $S = 1$ is present. Based on Fig. 1, we opted for a system, where quantum perturbations may only be present only before or after the Oracle operator, represented as $p_3 = p_4 = 0$. In more detail, we investigate two scenarios, where $p_1 = p_2 = 0.003$ and $p_1 = p_2 = 0.005$. The success probability of Grover's QSA when no quantum error correction is used in both scenarios, as well as when the QBCH[15, 7] and Steane's code are employed, may be seen in Fig. 8. As expected, Steane's code offers an improved performance, when compared to the QBCH[15, 7] code, since it achieves a success probability of 99.1% and 97.3% for $p_1 = p_2 = 0.003$ and $p_1 = p_2 = 0.005$, respectively, after $L_{opt} = 8$ according to (2), while the QBCH[15, 7] code yields a success probability of 96.5% and 90.1% for $p_1 = p_2 = 0.003$ and $p_1 = p_2 = 0.005$, respectively, after the same number of Grover iterations. At the same time though, the QBCH[15, 7] code requires only 8 auxiliary qubits for encoding the 7 information qubits, resulting in a coding rate of $R = 7/15$, while again Steane's code requires 42 auxiliary qubits, due to its low coding rate of $R = 1/7$. Therefore, a trade-off between performance and available resources is unavoidable in this case. Still based on Fig. 8, Grover's QSA performs better when a quantum error correction code is used, and its probability of success is reduced, when we increase the number of Grover iterations, due to the error propagation in the information qubits.

In every scenario of Grover's imperfect QSA, the error propagation eventually results in the termination of the periodicity of Grover's QSA's success probability with respect to the number of Grover iterations as demonstrated in Fig. 4, by initially reducing the peak of the success probability and finally making it equivalent to a random guess. The speed of this phenomenon is increased, when a higher depolarizing probability is present in the quantum system, as depicted in Fig. 7.

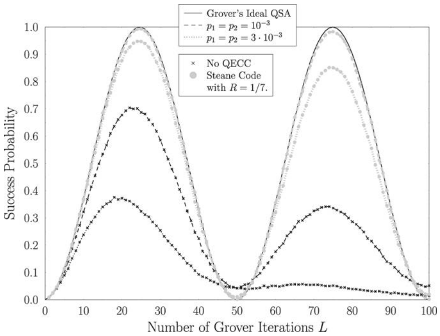


Figure 7. Success probability of Grover's QSA in a database with $N = 1024$ entries and $S = 1$ solution, with respect to the number of applications L of Grover's operator $\mathcal{G}$, when depolarizing channels appear before and after the Oracle operator of Fig. 1, associated with $p_3 = p_4 = 0$. The architecture of Fig. 2 is used. Two different depolarizing probabilities are assumed, namely $p_1 = p_2 = 0.001$ and $p_1 = p_2 = 0.003$, while the performance when Steane code is employed for cancelling the channels' effects is compared to that of an uncoded system. The performance of the ideal Grover's QSA is also attached as a reference.

Conclusions and Open Problems

In this treatise, we demonstrated that quantum error correction codes, which do not require long information qubit streams, may be employed for stabilizing the information qubits of quantum search algorithms. We presented a model of Grover's QSA in Fig. 1, where quantum perturbations may occur in different locations of its quantum circuit, modelled in the form of depolarizing channels, and evaluated its probability of success as a function of the number of Grover iterations, as well as that of the depolarizing probabilities of the existing channels. We also analysed and investigated a circuit architecture devised for Grover's QSA. In practice, the specific technologies used for creating a quantum computer will determine the particular locations, where it is beneficial to stabilize the qubits of a quantum algorithm, as well as the suitable circuit architectures. The methodologies we presented here are applicable to any arbitrary positions in the circuit of Grover's QSA.

Furthermore, the effect that depolarizing has on the optimal number of Grover iterations was also investigated in Fig. 4. Moreover, we managed to achieve a depolarizing probability improvement higher than an order of magnitude that may be tolerated, when aiming for a ~100% probability of success in large databases, when using Steane's code for correcting the quantum errors, as illustrated in Fig. 6. According to Fig. 8, the near-half-rate QBCH codes may also improve the performance of Grover's QSA, but as expected, they offer a lower gain, than that offered by Steane's code, again at a higher coding rate.

As future research, it may be beneficial to investigate the effect that depolarizing may have on other quantum search algorithms, variants of Grover's QSA, such as the Boyer-Brassard-Hø yer-Tapp (BBHT) QSA[43], or the Dürr-Hø yer algorithm[48], which are based on Grover's QSA, but may prove to be more resilient to bit and phase errors due to their pseudo-random methodology. In addition, an impactful research topic would be to investigate the performance of quantum search algorithms, when depolarizing perturbations occur within the quantum operators, such as the Oracle. Furthermore, more complex quantum error correction codes, such as the Quantum Low-Density Parity-Check (QLDPC) codes[28,49], or the Quantum Turbo Code (QTC)[23,25,50], may be employed for operating close to the Hashing bound in large-scale quantum systems, where multiple quantum computing algorithms will be running in parallel, therefore a plethora of qubits exploited by different algorithms will have to be stabilized simultaneously, assuming a central controller will perform the necessary synchronization.

Methods

Initialization and Oracle Circuit in Grover's QSA.

The operation of both Grover's operator and of the Oracle[51] is illustrated in Fig. 2. The *index register* $|q\rangle$ consists of $n = \log_2 N$ qubits and it is initialised to an equiprobable superposition of all legitimate states, as described in (1). When the quantum search algorithm is employed for searching through the values of a function *f*(*q*), then the unitary quantum gate U_f that computes this function is applied both to the n-qubit index register $|q\rangle$, as well as to the *Z*-qubit *value register* $|f(q)\rangle$, which is initialized to the all-zero state. The operation of U_f leaves the index register $|q\rangle$ unaltered, while entangling the qubits of the index register and of the value register with each other, hence resulting in the state

$$|w_1\rangle = \frac{1}{\sqrt{N}}\left(\sum_{x=0}^{N-1}|x\rangle|f(x)\rangle\right)|\delta\rangle|-\rangle, \tag{3}$$

where $|\delta\rangle$ is the *reference register* and $|-\rangle = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ is an auxiliary qubit. In other words, each legitimate input *x* of the function *f*(·) is entangled with its respective value *f*(*x*). The auxiliary reference register $|\delta\rangle$ also consists of *Z* number of qubits, since it will be compared to the value register $|f(q)\rangle$. Please note that as mentioned in the context of (3), the reference register is not found in a superposition of states, but instead is set to the reference value δ that we are looking for. Since we employ Grover's QSA in our scenario, Fig. 2 depicts the Oracle that searches for the specific value $|f(x)\rangle$ that is equal to $|\delta\rangle$. In order to achieve this, *Z* number of Controlled-NOT (CNOT) gates[4] are used in conjunction with the qubits of the value register acting as the control qubits, while

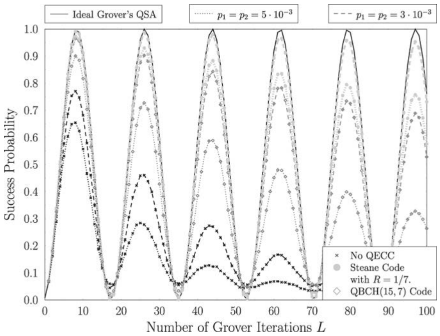


Figure 8. Success probability of Grover's QSA in a database with $N = 128$ entries and $S = 1$ solution, with respect to the number of applications L of Grover's operator $\mathcal{G}$, when depolarizing channels exist before and after the Oracle operator of Fig. 1, associated with $p_3 = p_4 = 0$, when the architecture of Fig. 2 is used. Two different depolarizing probabilities are assumed, namely $p_1 = p_2 = 0.003$ and $p_1 = p_2 = 0.005$, while the performance when QBCH[15, 7] code is employed for cancelling the channels' effects is compared to that of the Steane code, as well as that of an uncoded system. The performance of the ideal Grover's QSA is also attached as a reference.

those of the reference register represent the target qubits. During the operation of a CNOT gate, the state of the target qubit is flipped, when the control qubit is equal to $|1\rangle$.

Following the operation of the CNOT gates, the reference register will be entangled to the value register. Additionally, the value of the reference register's qubits returned for the specific solution state $|x_s\rangle$, for which we have $f(x_s) = \delta$, will always be $|0\rangle^{\otimes Z}$. In order to further clarify this, we have considered a brief example (see Supplementary Section 7). In other words, the Oracle marks the particular solution in the index register by flipping its sign with the aid of a concerted action by a value register, a reference register and an additional auxiliary qubit. Then, the inverse operation is performed for the sake of removing the entanglement between the value register and the reference register.

In this treatise, we assume that the value register is always error-free and any perturbations occur at the index register. This is the reason why only the index register is illustrated in Fig. 1. The diffusion operator is applied only to the index register, as depicted in Fig. 2. The depolarizing probabilities p_1 and p_2 of Fig. 1 correspond to the quantum circuit of Fig. 2. An example encapsulating the process of the diffusion operator is provided in Supplementary Section 5.

If other quantum search algorithms were employed, the Oracle's circuit would be different. For example, if we employed a variant of Grover's QSA, as proposed by Dürr and Høyer in ref. 48, which aims for finding the minimum of a database, then both the initialization stage of Fig. 2, as well as the diffusion operator would remain the same, but the Oracle's circuit of Fig. 2 would be replaced by a specific bit string comparator circuit, which would mark all the states that have a lower value than the reference value δ.

Encoder of Quantum BCH Code.

The Steane code is equivalent to the QBCH[7, 1] code. The PCM of the single error-correcting QBCH[15, 7], which is constructed from the dual-containing classical BCH(15, 11) code, is

$$\begin{aligned}\mathbf{H} &= [\mathbf{I}_{\mathtt{m}}|\mathbf{P}]\\ &= \left(\begin{array}{cccc|ccccccccccc} 1&0&0&0&1&1&1&1&0&1&0&1&1&0&0\\ 0&1&0&0&0&1&1&1&1&0&1&0&1&1&0\\ 0&0&1&0&0&0&1&1&1&1&0&1&0&1&1\\ 0&0&0&1&1&1&1&0&1&0&1&1&0&0&1 \end{array}\right).\end{aligned} \tag{4}$$

The encoding circuit of QBCH[15, 7] is derived as follows (see Supplementary Fig. 5):

- Let $\mathbf{H}$ be an $\mathtt{m} \times \mathtt{n} = 4 \times 15$ classical dual-containing PCM of (4). We transform $\mathbf{H}$ into the matrix $\widetilde{\mathbf{H}} = [\mathbf{I}_{\mathtt{m}}|\mathbf{P}]$ using row operations as well as column permutations. The resultant matrix $\mathbf{I}_{\mathrm{m}}$ is an $\mathtt{m} \times \mathtt{m}$ identity matrix, while $\mathbf{P}$ is an $\mathtt{m} \times (\mathtt{n} - \mathtt{m})$ binary matrix. For the $\mathbf{H}$ of (4), we have $\widetilde{\mathbf{H}} = \mathbf{H}$.
- As a next step, we apply row operations to $\mathbf{P}$, reducing it to $\widetilde{\mathbf{P}} = [\mathbf{I}_{\mathtt{m}}|\mathbf{Q}]$, where $\mathbf{Q}$ is an $\mathtt{m} \times (\mathtt{n} - 2\mathtt{m})$ binary matrix. Therefore, we get

$$\widetilde{\mathbf{P}} = [\mathbf{I}_{\mathtt{m}}|\mathbf{Q}] = \left(\begin{array}{cccc|ccccccc} 1&0&0&0&1&1&1&1&0&1&0\\ 0&1&0&0&0&1&1&1&1&0&1\\ 0&0&1&0&0&0&1&1&1&1&0\\ 0&0&0&1&1&1&1&0&1&0&1 \end{array}\right). \tag{5}$$

- Let $\mathcal{C}$ be the classical code having the PCM $\widetilde{\mathbf{H}}$ and the dual code $\mathcal{C}^{\perp}$, such that $\mathcal{C}^{\perp} \subset \mathcal{C}$. An $[\mathtt{n}, \mathtt{k}]$ dual-containing CSS code maps each of the 2^{k} superimposed states of a $\mathtt{k}$-qubit information word onto a unique coset of the dual code $\mathcal{C}^{\perp}$ in the code space of $\mathcal{C}$. The cosets of $\mathcal{C}^{\perp}$ in $\mathcal{C}$ may be obtained by adding a codeword of $\mathcal{C}$

to all the codewords of $\mathcal{C}^{\perp}$. However, only those codewords of $\mathcal{C}$ generate a unique coset of $\mathcal{C}^{\perp}$, which do not differ by an element of the $\mathcal{C}^{\perp}$. In this context, the encoder may be implemented in two steps (see Supplementary Fig. 5).

- In the first step, the matrix $\mathbf{Q}$ of (5) acts on the second block of $\mathtt{m} = 4$ qubits controlled by the last $\mathtt{k} = (\mathtt{n} - 2\mathtt{m}) = 7$ qubits, which constitute the information word. More explicitly, a CNOT gate acts on the *i*th qubit of the second block of $\mathtt{m}$ qubits, which is controlled by the *j*th information qubit, if $Q_{ij} = 1$. This may be encapsulated as follows

$$|0\rangle^{\otimes m}|0\rangle^{\otimes m}|q\rangle \rightarrow |0\rangle^{\otimes m}|\mathbf{Q}q\rangle|q\rangle. \tag{6}$$

  The resultant states constitute the set of codewords of $\mathcal{C}$, which do not differ by any element of $\mathcal{C}^{\perp}$ and there ore are capable of generating unique cosets of $\mathcal{C}^{\perp}$.
- The second stage adds the codewords of $\mathcal{C}^{\perp}$ to the codewords of $\mathcal{C}$ generated in the previous step. More specifically, the second stage on its own generates the codespace of $\mathcal{C}^{\perp}$ according to the PCM $\widetilde{\mathbf{H}}$. For a classical code $\mathcal{C}^{\perp}$, the first m bits are the systematic information bits, which can have either the value of 0 or 1. Consequently, the first $\mathtt{m} = 4$ auxiliary qubits undergo a Hadamard transformation. Finally, the matrix $\mathbf{P}$ of (4) acts on the last $(\mathtt{n} - \mathtt{m})$ qubits controlled by the first m qubits for the sake of generating the codespace of $\mathcal{C}^{\perp}$. More explicitly, a CNOT gate acts on the *j*th qubit of the last $(\mathtt{n} - \mathtt{m})$ qubit, which is controlled by the *i*th qubit, if $P_{ij} = 1$.

Decoding Process of Stabilizer Codes. Both the Steane code and the QBCH code, which are invoked in this treatise for improving the performance of Grover's QSA in the presence of perturbations, are dual-containing Calderbank-Shor-Steane (CSS) type[25] stabilizer codes. More specifically, these codes were designed from dual-containing classical codes. We derived the encoding circuit of QBCH using the method conceived by Mackay *et al.* in ref. 46. The decoding process of Fig. 5 proceeds as follows:

1. Syndrome Processing: Since any observation of a qubit perturbs its superimposed quantum state, a quantum decoder should not measure the received qubits. Therefore, inspired by the Parity Check Matrix (PCM)-based syndrome decoding of classical codes[52], a quantum decoder circumvents the associated measurement operation by observing the error syndromes, rather than the actual quantum information. For an $[\mathtt{n}, \mathtt{k}]$ stabilizer code, this is achieved by applying $(\mathtt{n} - \mathtt{k})$ commuting n-qubit Pauli operators[4], called stabilizers, to the received codewords $|\hat{\bar{q}}\rangle$. The stabilizers yield an eigenvalue of $+1$ for valid codewords and -1 for the corrupted ones, which corresponds to a syndrome value of 0 and 1, respectively. Analogous to the syndrome decoding of classical codes, a syndrome value of 0 marks the absence of quantum flips in a codeword, while a value of 1 denotes the presence of quantum flips. More specifically, the eigenvalue is $+1$ if $\mathcal{P}$ commutes with the *i*th stabilizer g_i, while it is -1 if $\mathcal{P}$ anti-commutes with the stabilizer g_i, which may be formulated as:

$$g_i|\hat{q}\rangle = \begin{cases} |\bar{q}\rangle, & g_i\mathcal{P} = \mathcal{P}g_i \\ -|\bar{q}\rangle, & g_i\mathcal{P} = -\mathcal{P}g_i, \end{cases}. \tag{7}$$

   Hence, within the 'syndrome processing' block of Fig. 5, the decoder computes the syndrome of the received sequence $|\hat{\bar{q}}\rangle$ and uses the resultant syndrome sequence to estimate the perturbation-induced error pattern $\widetilde{\mathcal{P}}$ with the aid of a classical syndrome decoding process.
2. Error Recovery ($\mathcal{R}$): The error recovery block '$\mathcal{R}$' of Fig. 5 restores the potentially error-free coded stream using the estimated error pattern $\widetilde{\mathcal{P}}$.
3. Inverse Encoder: Finally, the 'inverse encoder' of Fig. 5 processes the recovered coded sequence $|\hat{q}\rangle$, yielding the estimated original information qubits $|\tilde{q}\rangle$. Here the terminology of "inverse encoder" is used because, in contrast to an encoder, which maps logical qubits onto the physical qubits, an inverse encoder carries out the inverse operation by mapping physical qubits onto the logical qubits. More explicitly, an inverse encoder may have the same circuit as an encoder, but operates from right (physical qubits) to left (logical qubits).

Implementation. The systems investigated in this contribution were implemented using object oriented programming in C++, with the aid of the IT++ library, and simulated on the University's supercomputer. Since a universal quantum computer is not available at the time of writing, Grover's QSA was designed in the classical domain. Let us describe the steps of simulating Grover's QSA with the aid of a classical computer. Initially, a random database of size N is generated. Since the number of solutions S in the database is expected to be known prior to the search, S random entries are picked in the database, and the last $S - 1$ entries change their values to that of the first randomly picked solution. That value is equal to δ. Therefore, an N-element database with S entries equal to δ has been generated. Without loss of generality, the entries in the database assume values in the range of [0, 1], while making sure that no more than S entries have values equal to δ.

The unitary operators were implemented by using their matrix representation. The quantum states were described by their vector representation. The Oracle in Grover's QSA is also employed by using its matrix representation. Since the action of the Oracle effectively flips the phase of the specific state that is a solution, and since the simulations were performed in a classical computer, we are capable of finding the specific entries that represent solutions by performing a full search. The optimal number of Grover iterations L_{opt} is calculated before the initiation of the search according to (2).

The measurement of a quantum state was programmed by generating a uniformly-distributed random number in the [0, 1] range and searching which specific part of the cumulative sum of the measured state's probabilities it is found in. The particular quantum state that corresponds to the probability range that the randomly generated number belongs to is assumed to be the observed state.

Quantum error correction codes were emulated using the Heisenberg representation of the Gottesman-Knill theorem[53]. Explicitly, an n-qubit Clifford encoder, acting on a $2^{\mathtt{n}}$-dimensional Hilbert space, has a $2^{\mathtt{n}} \times 2^{\mathtt{n}}$ unitary matrix, which defines the evolution of the associated n-qubit system By contrast, the Gottesman-Knill theorem[53] facilitates efficient classical simulation of the $2^{\mathtt{n}} \times 2^{\mathtt{n}}$ matrix by specifying the action of the encoder under conjugation on the Pauli X and Z operators acting on each of the n qubits. Consequently, the operation of a Clifford encoder may be completely described by only tracking the evolution of the $2\mathtt{n}$ operators $\{Z_1, Z_2, \ldots, Z_n, X_1, X_2, \ldots, X_{\mathrm{n}}\}$, where Z_j and X_j represents the Pauli Z and X operator, respectively, acting on the jth qubit and the identity I on all other qubits. Furthermore, each of the $2\mathtt{n}$ operators may be represented by $(2\mathtt{n} + 1)$ classical bits, so that two classical bits are used for mapping each Pauli operator as follows

$$\begin{aligned} I &\rightarrow (0, 0) \qquad & X &\rightarrow (0, 1) \\ Z &\rightarrow (1, 0) \qquad & Y &\rightarrow (1, 1), \end{aligned} \tag{8}$$

while one bit is used for the phase. However, the encoders, which differ only through a global phase, have the same impact under conjugation. Therefore, the bit used for denoting phase can be ignored and the $\mathtt{n}$-qubit encoder may be characterized by a $(2\mathtt{n} \times 2\mathtt{n})$ binary matrix. Based on the resultant classical representation of the quantum codes, we classically simulated the performance of the system of Fig. 5 by following the evolution of the channel error induced as follows:

1. Quantum Channel: Recall that a quantum depolarizing channel, characterized by the probability p, inflicts either a bit-flip or a phase-flip or in fact both with a probability of $p/3$. Therefore, according to the Pauli-to-binary mapping of (8), the quantum depolarizing channel reduces to two Binary Symmetric Channels (BSCs), one channel for the phase errors and the other for the bit errors, each having a crossover probability of $2p/3$. Consequently, we simulated the quantum channel by generating two independent BSCs, yielding the classical error patterns P_z and P_x for phase and bit errors, respectively.
2. Syndrome Processing: The resultant error patterns P_z and P_x of the two BSCs were fed independently to a classical syndrome decoder for estimating the channel-induced classical errors $\widetilde{P}_z$ and $\widetilde{P}_x$.
3. Error Recovery: Then the error recovery operation of Fig. 5 was emulated by the modulo 2 addition of P_z and $\widetilde{P}_z$, and similarly the modulo 2 addition of P_x and $\widetilde{P}_x$, which yielded the residual phase and bit error, respectively, on the recovered output $|\hat{\bar{q}}\rangle$ of Fig. 5. This error recovery process may be encapsulated as

$$\widetilde{\overline{P}}_z = P_z \oplus \widetilde{\overline{P}}_z \qquad \widetilde{\overline{P}}_x = P_x \oplus \widetilde{\overline{P}}_x. \tag{9}$$

4. Inverse Encoding: Let $\widetilde{\overline{P}} = [\widetilde{\overline{P}}_z, \widetilde{\overline{P}}_x]$ be the 2n-bit residual error imposed on the recovered physical qubits $|\tilde{\bar{q}}\rangle$. Let us assume furthermore that V is the equivalent $(2\mathtt{n} \times 2\mathtt{n})$ binary matrix of the $\mathtt{n}$-qubit quantum code $\mathcal{V}$. Based on this notation, passing the residual error through the inverse encoder V^{-1} yields

$$\widetilde{\overline{P}} V^{-1} = [\widetilde{L}, \tilde{S}], \tag{10}$$

where $\widetilde{L}$ represents the residual error imposed on the logical qubits $|\tilde{q}\rangle$ of Fig. 5, while $\tilde{S}$ denotes the residual error on the auxiliary qubits, which were initialized to $|0\rangle$ at the input of the encoder of Fig. 5. Hence, we applied the error $\widetilde{L}$ to our intended logical qubits $|q\rangle$ of Fig. 5 to get the estimated logical qubits $|\tilde{q}\rangle$ of Fig. 5.

References

1. Waldrop, M. More than Moore. *Nature* **530,** 144–147 (2016).
2. Grover, L. K. A fast quantum mechanical algorithm for database search. *28th Annual ACM Symposium on the Theory of Computing Proceedings* 212–219 (1996).
3. Grover, L. K. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters* **79,** 325–328 (1997).
4. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
5. Imre, S. & Balázs, F. *Quantum Computing and Communications: An Engineering Approach* (John Wiley & Sons, 2005).
6. Imre, S. & Gyongyosi, L. *Advanced Quantum Communications: An Engineering Approach* (John Wiley & Sons, 2013).
7. Botsinis, P., Ng, S. X. & Hanzo, L. Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design. *IEEE Access* **1,** 94–122 (2013).
8. Botsinis, P., Ng, S. X. & Hanzo, L. Fixed-complexity quantum-assisted multi-user detection for CDMA and SDMA. *IEEE Transactions on Communications* **62,** 990–1000 (2014).
9. Botsinis, P., Alanis, D., Ng, S. X. & Hanzo, L. Low-complexity soft-output quantum-assisted multiuser detection for direct-sequence spreading and slow subcarrier-hopping aided SDMA-OFDM systems. *IEEE Access* **2,** 451–472 (2014).
10. Botsinis, P., Alanis, D., Babar, Z., Ng, S. & Hanzo, L. Iterative quantum-assisted multi-user detection for multi-carrier interleave division multiple access systems. *IEEE Transactions on Communications* **63,** 3713–3727 (2015).
11. Botsinis, P., Alanis, D., Babar, Z., Ng, S. X. & Hanzo, L. Noncoherent quantum multiple symbol differential detection for wireless systems. *IEEE Access* **3,** 569–598 (2015).
12. Alanis, D., Botsinis, P., Ng, S. X. & Hanzo, L. Quantum-assisted routing optimization for self-organizing networks. *IEEE Access* **2,** 614–632 (2014).

13. Alanis, D., Botsinis, P., Babar, Z., Ng, S. X. & Hanzo, L. Non-Dominated Quantum Iterative Routing Optimization for Wireless Multihop Networks. *IEEE Access* **3,** 1704–1728 (2015).
14. Shor, P. W. Scheme for reducing decoherence in quantum computer memory. *Physical Review A* **52,** 2493–2496 (1995).
15. Preskill, J. Battling decoherence: the fault-tolerant quantum computer. *Physics Today* **52,** 24–32 (1999).
16. Devitt, S., Stephens, A., Munro, W. & Nemoto, K. Requirements for fault-tolerant factoring on an atom-optics quantum computer. *Nature Communications* **4,** 2524 (2013).
17. Liu, G.-Q., Po, H. C., Du, J., Liu, R.-B. & Pan, X.-Y. Noise-resilient quantum evolution steered by dynamical decoupling. *Nature Communications* **4,** 2254 (2013).
18. Rong, X. *et al.* Experimental fault-tolerant universal quantum gates with solid-state spins under ambient conditions. *Nature Communications* **6,** 8748 (2015).
19. Wilde, M. M. *Quantum Information Theory* (Cambridge University Press, 2013).
20. Cory, D. G. *et al.* Experimental quantum error correction. *Physical Review Letters* **81,** 2152–2155 (1998).
21. Reed, M. D. *et al.* Realization of three-qubit quantum error correction with superconducting circuits. *Nature* **482,** 382–385 (2012).
22. Arrad, G., Vinkler, Y., Aharonov, D. & Retzker, A. Increasing sensing resolution with error correction. *Physical Review Letters* **112,** 150801 (2014).
23. Wilde, M., Hsieh, M.-H. & Babar, Z. Entanglement-assisted quantum turbo codes. *IEEE Transactions on Information Theory* **60,** 1203–1222 (2014).
24. Babar, Z., Ng, S. X. & Hanzo, L. EXIT-chart-aided near-capacity quantum turbo code design. *IEEE Transactions on Vehicular Technology* **64,** 866–875 (2015).
25. Babar, Z., Botsinis, P., Alanis, D., Ng, S. X. & Hanzo, L. The road from classical to quantum codes: a hashing bound approaching design procedure. *IEEE Access* **3,** 146–176 (2015).
26. Hagiwara, M., Kasai, K., Imai, H. & Sakaniwa, K. Spatially coupled quasi-cyclic quantum LDPC codes. *IEEE International Symposium on Information Theory Proceedings* 638–642 (2011).
27. Kasai, K., Hagiwara, M., Imai, H. & Sakaniwa, K. Quantum error correction beyond the bounded distance decoding limit. *IEEE Transactions on Information Theory* **58,** 1223–1230 (2012).
28. Babar, Z., Botsinis, P., Alanis, D., Ng, S. & Hanzo, L. Fifteen years of quantum LDPC coding and improved decoding strategies. *IEEE Access* **3,** 2492–2519 (2015).
29. Renes, J. M., Dupuis, F. & Renner, R. Efficient polar coding of quantum information. *Physical Review Letters* **109,** 050504 (2012).
30. Renes, J. & Wilde, M. Polar codes for private and quantum communication over arbitrary channels. *IEEE Transactions on Information Theory* **60,** 3090–3103 (2014).
31. Steane, A. M. Error correcting codes in quantum theory. *Physical Review Letters* **77,** 793–797 (1996).
32. Grassl, M., Beth, T. & Pellizzari, T. Codes for the quantum erasure channel. *Physical Review A* **56,** 33–38 (1997).
33. Calderbank, A., Rains, E., Shor, P. & Sloane, N. Quantum error correction via codes over GF(4). *IEEE Transactions on Information Theory* **44,** 1369–1387 (1998).
34. Grassl, M. & Beth, T. Quantum BCH Codes. *International Symposium on Theoretical Electrical Engineering* 207–212 (1999).
35. Salas, P. J. Noise effect on Grover algorithm. *European Physical Journal D* **46,** 365–373 (2008).
36. Cohn, I., De Oliveira, A. L. F., Buksman, E. & De Lacalle, J. G. L. Grover's search with local and total depolarizing channel errors: Complexity analysis. *International Journal of Quantum Information* **14** (2016).
37. Long, G. L., Li, Y. S., Zhang, W. L. & Tu, C. C. Dominant gate imperfection in Grover's quantum search algorithm. *Phys. Rev. A* **61,** 042305 (2000).
38. Chen, J., Kaszlikowski, D., Kwek, L. C. & Oh, C. H. Searching a Database under Decoherence. *eprint arXiv:quant-ph/0102033* (2001).
39. Ellinas, D. & Konstadakis, C. Noisy Grover's Search Algorithm. *eprint arXiv:quant-ph/0110010* (2001).
40. Azuma, H. Decoherence in Grover's quantum algorithm: Perturbative approach. *Phys. Rev. A* **65,** 042311 (2002).
41. Shapira, D., Mozes, S. & Biham, O. Effect of Unitary Noise on Grover's Quantum Search Algorithm. *Phys. Rev. A* **67,** 042301 (2003).
42. Oskin, M., Chong, F. T. & Chuang, I. L. A Practical Architecture for Reliable Quantum Computers. *Computer* **35,** 79–87 (2002).
43. Boyer, M., Brassard, G., Høyer, P. & Tapp, A. Tight Bounds on Quantum Searching. *Fortschritte der Physik* **46,** 493–506 (1998).
44. Gottesman, D. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Physical Review A* **54,** 1862–1868 (1996).
45. Gottesman, D. *Stabilizer Codes and Quantum Error Correction.* Ph.D. thesis, California Institute of Technology (1997).
46. MacKay, D., Mitchison, G. & McFadden, P. Sparse-graph codes for quantum error correction. *IEEE Transactions on Information Theory* **50,** 2315–2330 (2004).
47. Preskill, J. Reliable Quantum Computers. *Proceedings of the Royal Society of London Series A* **454,** 385 (1998).
48. Durr, C. & Høyer, P. A quantum algorithm for finding the minimum. *Quantum Physics* **9607014** (1996).
49. Hsieh, M.-H., Brun, T. A. & Devetak, I. Entanglement-assisted quantum quasicyclic low-density parity-check codes. *Physical Review A* **79,** 032340 (2009).
50. Babar, Z., Ng, S. & Hanzo, L. EXIT-chart aided near-capacity quantum turbo code design. *IEEE Transactions on Vehicular Technology* **64,** 866–875 (2014).
51. Ju, Y. L., Tsai, I. M. & Kuo, S. Y. Quantum circuit design and analysis for database search applications. *IEEE Transactions on Circuits and Systems I: Regular Papers* **54,** 2552–2563 (2007).
52. Babar, Z., Ng, S. X. & Hanzo, L. Reduced-complexity syndrome-based TTCM decoding. *IEEE Communications Letters* **17,** 1220–1223 (2013).
53. Gottesman, D. The Heisenberg representation of quantum computers. *Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics* 32–43 (2001).

Acknowledgements

This work was supported in part by the European Research Council through the Advanced Fellow Grant, in part by the Royal Society's Wolfson Research Merit Award, and in part by the Engineering and Physical Sciences Research Council under Grant EP/L018659/1.

Author Contributions

All authors contributed to the ideas and discussions presented in this paper. P.B. and D.A. designed Grover's QSA, while Z.B., D.C. and H.N. implemented the quantum error correction codes. P.B., D.A. and Z.B. carried out the simulations of the scenarios. P.B., Z.B., S.X.N. and L.H. were involved in writing the manuscript, with input from all authors. All authors reviewed the manuscript.

Additional Information

Supplementary information accompanies this paper at http://www.nature.com/srep

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Botsinis, P. *et al.* Quantum Error Correction Protects Quantum Search Algorithms Against Decoherence. *Sci. Rep.* **6**, 38095; doi: 10.1038/srep38095 (2016).