Quantum Inf Process (2012) 11:55–66
DOI 10.1007/s11128-011-0231-4

Can quantum entanglement detection schemes improve search?

Luís Tarrataca · Andreas Wichert

Received: 30 November 2010 / Accepted: 27 January 2011 / Published online: 16 February 2011

Abstract Quantum computation, in particular Grover's algorithm, has aroused a great deal of interest since it allows for a quadratic speed-up to be obtained in search procedures. Classical search procedures for an N element database require at most $O(N)$ time complexity. Grover's algorithm is able to find a solution with high probability in $O(\sqrt{N})$ time through an amplitude amplification scheme. In this work we draw elements from both classical and quantum computation to develop an alternative search proposal based on quantum entanglement detection schemes. In 2002, Horodecki and Ekert proposed an efficient method for direct detection of quantum entanglement. Our proposition to quantum search combines quantum entanglement detection alongside entanglement inducing operators. The quantum search algorithm relies on measuring a quantum superposition after having applied a unitary evolution. We deviate from the standard method by focusing on fine-tuning a unitary operator in order to infer the solution with certainty. Our proposal sacrifices space for speed and depends on the mathematical properties of linear positive maps Λ which have not been operationally characterized. Whether such a Λ can be easily determined remains an open question.

Keywords Quantum computation · Tree search · Entanglement detection

This work was supported by FCT (INESC-ID multiannual funding) through the PIDDAC Program funds and FCT grant DFRH–SFRH/BD/61846/2009.

L. Tarrataca (✉) · A. Wichert
GAIPS/INESC-ID, Department of Computer Science, Instituto Superior Técnico, Technical University of Lisbon, Avenida Professor Cavaco Silva, 2780-990 Porto Salvo, Portugal
e-mail: luis.tarrataca@ist.utl.pt

A. Wichert
e-mail: andreas.wichert@tagus.ist.utl.pt

1 Introduction

Computer scientists are often faced with the task of constructing algorithms capable of delivering a solution for a given problem. For some problems it is possible to engineer algorithms capable of producing a solution with a number of computational steps that is bounded by a polynomial n^k where n is the length of the input and k some constant. The class of problems for which a polynomial-time algorithm exists is known as P. Problems belonging to P are usually seen as being efficiently solvable, i.e. tractable. Class EQP represents the quantum equivalent of P.

For other problems it is possible to verify in polynomial-time if a given configuration is a solution, although there are no known methods for efficiently calculating a solution. For these type of problems, there is no alternative but to perform an exhaustive search of all possible configurations. The class NP consists of those problems whose possible configurations can be verified in polynomial-time. Clearly, $\mathrm{P} \subseteq \mathrm{NP}$ since the possibility of constructing a solution in polynomial time also implies that a solution can be verified efficiently. One of the outstanding questions in computer science consists in determining if the class NP is equivalent to the class P, i.e. $\mathrm{P} = \mathrm{NP}$? Traditionally, approaches to answering this question have focused at a subclass of NP, namely NP-complete problems. This subclass contains those problems which are both NP and NP-hard. A problem is said to be NP-hard if an algorithm capable of solving it can be translated into an adequate algorithm for any NP problem. By its own definition, an efficient solution for a problem in NP-complete implies that an efficient solution exists for all problems in NP.

The first clues that some problems which are classically hard may have an efficient quantum solution were provided in [6]. Shor's algorithm for efficient factorization [27] reinforced this idea. Later, Grover's search algorithm [9] provided an asymptotical quadratic speed-up over classical strategies. The quantum search algorithm systematically increases the probability of obtaining a solution with each iteration. After the algorithm has concluded, a measurement is performed in a quantum superposition, in order to obtain a solution with high probability. The superposition state represents the set of all possible results. Grover's approach sparked interest by the scientific community on whether it would be possible to devise a faster search algorithm. Unfortunately, it was proved that the search problem cannot be solved under $\Omega(\sqrt{N})$ time [3] using standard quantum computation approaches.

In this work we present an alternative search method based on the principles of tree search decomposition and quantum entanglement detection. Unlike traditional approaches, we opt not to concentrate our efforts on measuring a quantum superposition of possible values. Rather, we are more interested in exploiting the unitary operator that is applied to a quantum superposition in order to infer possible solutions with certainty. However, an implicit caveat exists associated to our quantum search proposal. Namely, our system implies a trade-off between speed and space that will become apparent in the following sections.

The next sections are organized as follows: Sect. 2 focuses on presenting the details of an NP-complete problem, namely the Boolean satisfiability problem, alongside classical tree search techniques of examining the problem space. Sect. 3 presents

our hybrid approach, combining tree search decomposition alongside with quantum entanglement detection schemes. Sect. 4 presents the conclusions of this work.

2 Traditional approaches to tackling NP-Complete problems

The satisfiability (SAT) problem was the first problem ever shown to be NP-complete [4]. SAT asks whether a given boolean formula is satisfiable. Any polynomial-time algorithm capable of solving SAT automatically enables an efficient solution for all of NP. In complexity theory, the satisfiability problem is a boolean formula ϕ composed of [5]

- n boolean variables: $x_1, x_2, \ldots, x_n$;
- m boolean connectives: any boolean function with one or two inputs and one output, such as $\wedge$ (AND), $\vee$ (OR), $\neg$ (NOT), $\rightarrow$ (implication) and $\leftrightarrow$(if and only if);
- parentheses.

We are interested in determining a set of values for the variables of ϕ, i.e. variable configuration, which cause the overall expression to be satisfiable, i.e. evaluate to true. At any given point in time we need to consider the n variables alongside m gates, i.e. we can verify any configuration in $n + m$ time. However, the number of possible configurations to consider grows exponentially with the cardinality of the variable set. As an example lets consider the simple formula presented in Expression 1.

$$\phi = (x_1 \wedge x_2) \vee x_3 \tag{1}$$

The standard approach to solve such a problem would be to enumerate all possible configurations of the m variables. This procedure can be better understood with the help of a simple tree diagram such as the one illustrated in Fig. 1. At each depth level a specific the possible values for a specific binary variable are considered, e.g. depth 0 considers the possible values for x_1, depth 1 considers variable x_2 and so on. With each depth level an additional binary variable is taken into account. Considering n binary

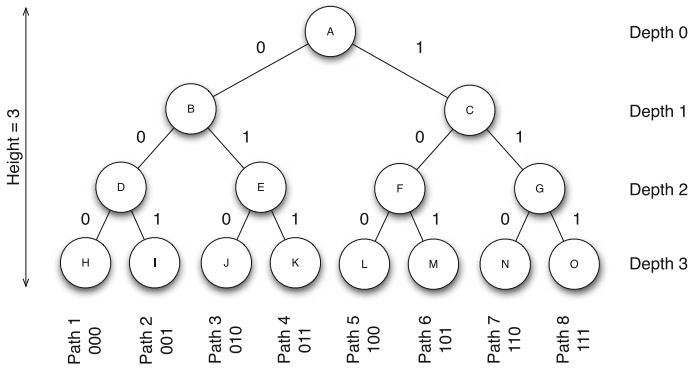

Fig. 1 The possible paths for a binary search tree of depth 3

variables requires examination of 2^n possible leaf states, i.e. $\Omega(2^n)$. In tree search vocabulary these states are also known as paths. If the specific case of Expression 1 is mapped into the tree elements of Fig. 1 then paths 1,4,6,7 and 8 would evaluate to true.

3 Approach

How can we proceed by developing an alternative approach to that of Grover's? First lets start by considering the following scenario: suppose we have a bipartite quantum system respectively labeled as the query register, $|q\rangle$, and the answer register, $|a\rangle$, acting on Hilbert space $\mathcal{H} = \mathcal{H}_q \otimes \mathcal{H}_q$. The query register is an n-qubit register where possible values for the binary variables of the SAT problem will be setup, i.e. $|q\rangle = |x_1 x_2 \cdots x_n\rangle$. Notice that in order to gain a quantum advantage over classical computation we need to place $|q\rangle$ in a uniform superposition of the computation basis. This can be done efficiently by applying the Hadamard transform H a total of n times to the n-qubit state $|0\rangle$, i.e. $H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$. Such a procedure enables the creation of a superposition containing an exponential number of states, each of which representing a possible tree path, by only employing a polynomial number of gates. The answer register contains a single qubit which is initialized to state $|0\rangle$. The overall state of the system can thus be described as illustrated in Expression 2.

$$|q\rangle|a\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle \tag{2}$$

Additionally, suppose that a quantum oracle with the form presented in Expression 3 is constructed. The auxiliary function $\phi : \{0,1\}^n \rightarrow \{0,1\}$ employed simply verifies if an argument is a solution or not for a specific SAT instance, as illustrated by Expression 4. We should be careful to point out that an efficient oracle responsible for verifying the validity of a variable configuration for a specific ϕ can be easily constructed by mapping the m boolean connectives of the network onto a reversible circuit (see [2]) in order to ensure a unitary mapping.

$$O|q\rangle|a\rangle = |q\rangle|a \oplus \phi(q)\rangle \tag{3}$$

$$\phi(q) = \phi(x_1, x_2, \ldots, x_n) = \begin{cases} 1 & \text{if } q \text{ evaluates to true} \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

If oracle O is applied to the combined state of Expression 2 a result like the one illustrated in Expression 5 may be obtained, where $|\psi'\rangle$ denotes the overall superposition evaluation. For simplification issues we assume that there exists at least a solution. Naturally, some of the query values produce a solution, whilst others do not.

$$|\psi'\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} O|x\rangle|0\rangle = \begin{cases} |\underbrace{00\cdots0}_{\text{nbits}}\rangle|0\rangle \\ |00\cdots1\rangle|0\rangle \\ \quad\vdots \\ |11\cdots0\rangle|1\rangle \\ |11\cdots1\rangle|0\rangle \end{cases} \tag{5}$$

From this point on the system's state can no longer be expressed as a tensor product between query and answer register, i.e. the system becomes entangled. Quantum entanglement is a key feature of quantum mechanics which details the connections between subsystems of compound quantum systems. It was a key aspect of the quantum world formalism proposed by von Neumann [24]. Although the intriguing impacts of quantum inseparability were only later grasped by Einstein et al. [7] alongside Schrödinger [26]. Quantum entanglement is also a key resource in quantum information.

Mathematically, we can describe the state of each register by tracing out the remaining register, through the partial trace mechanism. In this case we are interested in the overall state of the answer register. In order to calculate the partial trace of the answer register we first need to calculate ϱ the density operator of the quantum state presented in Expression 5. The overall form for ϱ^a is illustrated in Expression 7

$$\begin{aligned} \varrho &= |\psi\rangle\langle\psi| \\ &= \tfrac{1}{\sqrt{2^n}}(|00\cdots0\rangle|0\rangle + \cdots + |11\cdots1\rangle|0\rangle) \\ &\quad \tfrac{1}{\sqrt{2^n}}(\langle00\cdots0|\langle0| + \cdots + \langle11\cdots1|\langle0|) \\ &= \tfrac{1}{2^n}|00\cdots0\rangle|0\rangle(\langle00\cdots0|\langle0| + \cdots + \langle11\cdots1|\langle0|) \\ &\quad + \cdots + \\ &\quad \tfrac{1}{2^n}|11\cdots1\rangle|0\rangle(\langle00\cdots0|\langle0| + \cdots + \langle11\cdots1|\langle0|) \end{aligned} \tag{6}$$

$$\begin{aligned} \varrho^a &= \mathrm{Tr}_q(\varrho) \\ &= \tfrac{1}{2^n}(\langle00\cdots0||00\cdots0\rangle|0\rangle\langle0| + \langle00\cdots1||00\cdots1\rangle|0\rangle\langle0| \\ &\quad + \cdots + \\ &\quad \langle11\cdots0||11\cdots0\rangle|1\rangle\langle1| + \langle11\cdots1||11\cdots1\rangle|0\rangle\langle0|) \\ &= \tfrac{1}{2^n}\left[(2^n-1)|0\rangle\langle0| + |1\rangle\langle1|\right] \end{aligned} \tag{7}$$

Generally, the result presented in Expression 6 can be improved if we take into account the number of solutions. Accordingly, let k denote the overall number of solutions, then ϱ^a takes the form shown in Expression 8. Notice that the overall state is separable only when $k = 0$, i.e. no solution exists, or when $k = 2^n$, each value belonging to $[0, 2^n - 1]$ is a solution. Otherwise, the system is entangled.

$$\varrho^a = \frac{1}{2^n}\left[(2^n-k)|0\rangle\langle0| + k|1\rangle\langle1|\right] \tag{8}$$

Thus, the problem of determining whether or not a solution to a problem exists can be reduced to the problem of determining whether the overall quantum state is separable or entangled.

3.1 Quantum entanglement detection

The quantum separability problem consists in determining if a given a density matrix ϱ representing a quantum state is entangled or separable [8]. Efficiently deciding on the nature of such states has grabbed researchers attention and remains a problem of crucial importance to the fields of quantum computation and information [18]. Generally speaking, quantum entanglement is studied in accordance with a varied mix of properties (just to name a few of these: bipartite vs. multipartite systems, pure vs. mixed states, bound entanglement; for exhaustive reviews please refer to [11,16,21]). It is important to mention that the quantum separability question has been approached from the classical and quantum perspectives. These approaches typically consider the nature of the input (classical vs. quantum), and whether any required processing will be performed on a classical or quantum computer [17]. This problem was shown to be NP-hard classically [12]. However, as mentioned in [17] the processes involving both quantum input and processing have not been thoroughly investigated.

In the case of our specific approach we would only need to consider bipartite quantum systems with mixed states. As pointed out in [13] the mixed state requirement stems from the fact that any potential laboratory demonstration of this approach would have to deal with mixed states rather than pure ones, due to the uncontrolled interactions with the environment. These requirements are present in one of the existing quantum detection schemes, namely the one proposed in [15]. The method employed by the authors is experimentally viable and provides for a direct detection mechanism of quantum entanglement. Their approach is based on the theoretical foundations laid down in [13]. The method determines whether a state ϱ is separable or not, i.e. entangled, based on the mathematical properties of linear positive maps acting on matrices. More specifically [16], let $M_d \rightarrow M_d$ be the space of matrices of dimension d, a map $\Lambda : M_d \rightarrow M_d$ is called positive if it is Hermitian and has non-negative spectrum. Additionally, the map Λ is completely positive if and only if $I \otimes \Lambda$ is positive for identity map I on any finite-dimensional system. A state ϱ is separable if and only if the result presented in Expression 9 is observed for all positive but not completely positive maps $\Lambda : M_d \rightarrow M_d$.

$$[I \otimes \Lambda](\varrho) \geq 0 \tag{9}$$

Expression 9 cannot be directly used since it requires knowing state ϱ beforehand. Additionally, positive maps Λ cannot be directly implemented in laboratory. Fortunately, it is possible to obtain a physically realizable map by mixing an appropriate proportion of $[I \otimes \Lambda]$ with a depolarizing map. This approach allows for a new map $[\widetilde{I \otimes \Lambda}]$ to be obtained, which have been referred to as structural physical approximations. For more on this subject please refer to [28]. The separability criterion can then be restated as follows [15]: ϱ is separable if and only if for all positive maps Λ the condition presented in Expression 10 is observed.

$$[\widetilde{I \otimes \Lambda}](\varrho) \geq \frac{d^2\lambda}{d^4\lambda + 1} \tag{10}$$

Where λ corresponds to the most negative eigenvalue obtained when the induced map $[(I \otimes I) \otimes (I \otimes \Lambda)]$ acts on the maximally entangled state of the form $\frac{1}{d^2} \sum_{i=1}^{d^2} |i\rangle|i\rangle$. Accordingly, Expression 10 states that the lowest eigenvalue of the transformed state $\varrho' = \widetilde{[I \otimes \Lambda]}(\varrho)$ should be greater than $\frac{d^2\lambda}{d^4\lambda+1}$ for ϱ to be separable.

The authors devised a method which allows for an estimate of the lowest eigenvalue to be obtained efficiently and directly. It requires that a joint measurement be performed on N copies of state ϱ'. The overall input density operator of the estimation problem is $\varrho'^{\otimes N}$, which exists on the Nth tensor power $\mathcal{H}^{\otimes N}$ [20]. The error ϵ associated with the estimate of the lowest eigenvalue decreases exponentially with N. Such a measurement can be represented as a quantum network implementing projections on the symmetric and partially symmetric subspaces [15]. An efficient method addressing these questions was proposed in [1] requiring a number of auxiliary gates that grows quadratically with the dimension of the input, i.e. $O(n^2)$, where n is the number of bits. If ϱ' represents the state of an n qubit register, then each additional tensor power will mean that another n bits should be taken into account. Consequently, an $\varrho'^{\otimes N}$ system will have a total of $N \times n$ bits. Which means that the quantum network responsible for estimating the lowest eigenvalue will have $O(N^2n^2)$ complexity.

Clearly, this approach is dependent on map Λ which have not been operationally characterized so far [14]. As pointed out in [16] in general the set of positive but not completely positive maps is not characterized and it involves a hard problem in contemporary linear algebra. However, for low dimensional systems, namely those with dimension $2 \otimes 2$ or $2 \otimes 3$, the positive partial transpose map proposed in [25] can be employed as the Λ. In [14] the authors draw attention to the fact that 'Recently, the progress in this direction has been made [22,23] which suggests that tests of separability based on positive maps will soon acquire practical meaning beyond the scope of two-qubit systems." Whether such a map Λ acting on $\mathcal{H}_d \otimes \mathcal{H}_d$ quantum systems can be determined remains an open question.

3.2 Subset entanglement inducing oracle

Grover's algorithm provides an $\Omega(\sqrt{N})$ lower bound when employing oracles searching on the full range of searchable items. It would be desirable to develop an alternative search approach not solely based on amplitude amplification schemes. In classical tree search it is a standard technique to start by analyzing subtrees and deciding whether these may eventually lead to a solution. Based on problem requirements it is possible to automatically exclude, i.e. prune, certain subtrees. The act of pruning may eventually be responsible for large sections of the tree to be discarded, and therefore allow the search to terminate faster. We will draw inspiration from these concepts of classical search in order to develop our approach to quantum hierarchical search.

Quantum algorithms employing traditional oracles provide at most a polynomial advantage over classical algorithms for total functions, i.e. functions defined for the whole of $\{0, 1\}^n$, where n is the number of bits. The oracle model contemplates superpolynomial advantage but only when partial functions are defined which operate on a subset of $\{0, 1\}^n$ [19]. Notice that classical search can be viewed as a procedure which evaluates subsets of an initial range. Since in quantum computation the oracle

operator can be applied to a superposition of computational basis, evaluating subsets is equivalent to only evaluating specific ranges of the superposition. Accordingly, it is possible to develop an oracle responsible for evaluating only a certain subset of the initial range $[0, 2^n - 1]$ allowed with n qubits. Although we are only interested in evaluating a specific subset there are other alternatives for trying to decompose a quantum search space. For instance, Grover concluded in [10] that determining the first n bits of a solution by employing amplitude amplification schemes is only slightly easier than determining the total bits.

This model for a range specific entanglement inducing oracle can be described as presented in Expression 11 which employs an auxiliary function $f_{[a,b]}(q)$ defined in Expression 12. In the case of the SAT problem it would be convenient to define $f_{[a,b]}(q)$ as $\phi_{[a,b]}(q)$.

$$O_{[a,b]}|q\rangle|a\rangle = |q\rangle|a \oplus f_{[a,b]}(q)\rangle \tag{11}$$

$$f_{[a,b]}(q) = \begin{cases} 1 & \text{if } f(q) \text{ is a solution and } q \in [a,b] \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

As was previously pointed out, the oracle evaluation process has the overall effect of entangling the quantum registers. By testing whether the oracle has induced, or not, quantum entanglement it is possible to check for the presence of a solution state in a given range. This mechanism allows for ranges containing solutions to be further decomposed. In contrast, the absence of a solution allows for a specific range to be pruned from the overall search procedure.

Ideally, the entanglement detection scheme should present some type of polynomial upper-bound behavior such as the one described in the previous section.[1] If the state ϱ resulting from applying an oracle O with the form presented in Expression 12 is separable then the range evaluated can automatically be discarded. Discarding a wide range of potential candidates *en masse* can be understood as the classical tree search operation of pruning certain subtrees. On the other hand, if ϱ is entangled then it is possible to further decompose the associated range. Eventually, this sort of recursive branch and bound procedure, by constantly readjusting the range of oracle O, will "zoom in" on a solution. Additionally, it would be a relatively easy task to search problem spaces comprising of multiple solutions k. Namely, one would simply need to systematically focus on previously non-expanded but solution-bearing ranges.

Notice that this approach requires a new oracle to be defined with each iteration in terms of a specific subset that may be entangled. The set of oracles applied throughout the search can be viewed as a single "dynamic" oracle, which differs substantially from the standard "static" oracle applied in quantum search. Additionally, in contrast with Grover's algorithm, we are not interested in performing an amplitude amplification process, but rather we are concerned with decomposing the quantum search space.

[1] The entanglement detection approach described in [15] requires the overall bipartite system to be $d \otimes d$. Consequently, the answer register $|a\rangle$ should have the same dimension than $|q\rangle$, i.e. n bits. This requirement has no direct consequences in the overall oracle since unitary evolution can still be assured.

3.3 On the growth of the number of copies required

Clearly, one question still lingers: What can be said about the number of copies N of the system that are required? According to [19] any procedure that on input $|\psi_Z\rangle$ guesses whether $Z = X$ or $Z = Y$ will guess correctly with probbability at most $1 - \epsilon = \frac{1}{2} + \frac{1}{2}\sqrt{1 - \delta^2}$ where $\delta = |\langle\psi_x||\psi_y\rangle|$. For our particular case we are interested in distinguishing two specific cases, namely:

- $|\psi_{\text{solution}}\rangle$ which results from applying $U|\psi\rangle$ when *one* solution exists;
- $|\psi_{\text{no-solution}}\rangle$ which results from applying $U|\psi\rangle$ when *no* solution exists;

For search spaces of dimension L the initial amplitudes α_i associated with each computational basis i of the superposition $|\psi\rangle$ is $\frac{1}{\sqrt{L}}$. After having applied oracle O the two states remain exactly equal except for two computational basis where the amplitudes permuted. This means that when calculating the inner product the permuted computational basis will sum up to zero. Accordingly, the inner product will sum the value $\frac{1}{\sqrt{L}}^2$ a total of $L - 1$ times, i.e.

$$\delta = \langle\psi_{\text{solution}}||\psi_{\text{no-solution}}\rangle = \frac{L-1}{L} \tag{13}$$

Given a tensor product of N items, Expression 13 evolves into Expression 14. The three-dimensional plot of $\delta^{\otimes N}$ as a function of $L \in [2^1, 2^{30}]$ and $N \in [2^1, 2^{30}]$ is illustrated in Fig. 2.

$$\delta^{\otimes N} = \langle\psi_{\text{solution}}||\psi_{\text{no-solution}}\rangle^{\otimes N} = \frac{L-1}{L}^N \tag{14}$$

In order for these states to be distinguished with significant probability the inner product $\delta^{\otimes N}$ presented in Expression 14 must be made small. However, in order to achieve this one needs to choose a number of copies N that grows in accordance with the dimension of the search space L, i.e. $N = O(L)$. Consequently, this approach would not provide for any gains over classical search.

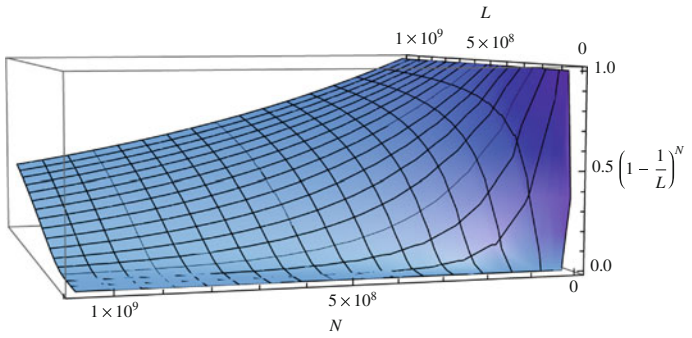

Fig. 2 Three-dimensional plot of $\delta^{\otimes N}$ as a function of $L \in [2^1, 2^{30}]$ and $N \in [2^1, 2^{30}]$

3.4 Consequences for efficient entanglement detection schemes

What would be the consequences if the number of system copies N was not a function of the search space? Suppose the proposed search procedure is executed on n-qubits placed on a superposition. Initially, the algorithm has to decompose the $[0, 2^n - 1]$ initial range. Lets assume that any specific range being considered is split in half. Accordingly, the procedure needs to verify if evaluating the elements in $[0, 2^{n-1} - 1]$ produces an entangled quantum state ϱ. If this is found to be true then subset $[0, 2^{n-1} - 1]$ can be also split in half and evaluated. Otherwise, subset $[2^{n-1} - 1, 2^n - 1]$ needs to be decomposed. Independently of what subset induces entanglement, the algorithm is able to prune half of the 2^n initial states, i.e. $2^n/2$. Accordingly, for iteration i, the oracle is able to focus on $2^n/2^i$ states. Clearly, when $i = n$ a single state is being considered and consequently a solution can be determined with certainty by employing $O(n)$ oracle queries. Associated with each oracle query is the quantum entanglement detection scheme bringing the overall complexity of our approach to $O(N^2 n^3)$. In the case of the SAT problem we have to consider the costs associated with each oracle query, respectively $n + m$. Consequently, a solution for SAT would be calculated in $O(N^2 n^4 + N^2 n^3 m)$ quantum polynomial time.

It is our believe that it is not possible to efficiently detect quantum entanglement. If we take into account the simplicity of the search procedure designed in Sect. 3.2 then if such a method existed we could efficiently search, i.e. in quantum polynomial time, a problem space of dimension d. Accordingly, we can define the following conjecture.

> Quantum entanglement detection conjecture—It is not possible to efficiently detect quantum entanglement non-classically since this would automatically imply that a simple algorithm exists proving that NP=EQP.

The above conjecture stresses the notion that there appears to be a relationship between entanglement detection and search in terms of computational complexity, *i.e.* both problems appear to be equally difficult. Indeed, since quantum entanglement detection via classical methods was shown to be NP-hard [12] any polynomial classical algorithm capable of solving NP-hard problems would allow for efficient mappings capable of tackling both quantum entanglement detection as well as exponential-growth search problems. From a quantum computation perspective it appears that, by employing such an entanglement detection scheme, there exists a direct relationship where a trade-off between space and time occurs. Nonetheless, this approach can still be perceived as a form of quantum computation, although one requiring a careful examination of the total time and space resources employed.

4 Conclusions

Shor's algorithm provided a superpolynomial speed-up by exploiting a hidden structure of the problem [27]. However, traditional tree search mechanisms are employed when such an element of structure cannot be determined. Quantum computation provides at best a polynomial speed-up when oracles mapping total functions are employed. Superpolynomial speed-up is achievable but only if a subset of a functions

domain is analyzed. In this work we focused on the dynamics of partial function unitary evolution alongside quantum entanglement detection schemes. The general characterization of positive but not completely positive linear maps Λ alongside quantum entanglement detection schemes and partial range entanglement inducing operators may eventually be responsible for producing efficient algorithmic solutions capable of searching exponential-growth search spaces. Although some research has already been carried out, further thorough analysis into the subject is still required. However, given that $N = O(L)$ current methods cannot be employed in order to speed up quantum search.

Acknowledgments We wish to thank the suggestions provided by the reviewers for an earlier version of this work.

References

1. Barenco, A., Berthiaume, A., Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C.: Stabilization of quantum computations by symmetrization. SIAM J. Comput. **26**(5),1541–1557 (1997) doi:10.1137/S0097539796302452. http://link.aip.org/link/?SMJ/26/1541/1
2. Bennett, C.: Logical reversibility of computation. IBM J. Res. Dev. **17**, 525–532 (1973)
3. Bennett, C.H., Bernstein, E., Brassard, G., Vazirani, U.: Strengths and weaknesses of quantum computing (1997) http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/9701001
4. Cook, S.A.: The complexity of theorem-proving procedures. In: STOC '71: Proceedings of the Third Annual ACM Symposium on Theory of Computing, pp. 151–158. ACM, New York, NY, USA (1971) http://doi.acm.org/10.1145/800157.805047
5. Cormen, T.H., Leiserson, C.E., Rivest, R.L., Stein, C.: Introduction to Algorithms, 2/e. MIT Press, Cambridge (2001)
6. Deutsch, D., Jozsa R.: Rapid solution of problems by quantum computation. R. Soc. Lond. Proc. Ser. A **439**: 553–558 (1992)
7. Einstein, A., Podolsky, B., Rosen, N.: Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. **47**(10), 777–780 (1935). doi:10.1103/Phys.Rev.47.777
8. Gharibian, S.: Strong NP-Hardness of the Quantum Separability Problem. ArXiv e-prints (2008)
9. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: STOC '96: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, pp. 212–219. ACM, New York, NY, USA (1996) http://doi.acm.org/10.1145/237814.237866
10. Grover, L.K., Radhakrishnan, J.: Is partial quantum search of a database any easier? (2004) http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/0407122
11. Gühne, O., Tóth, G.: Entanglement detection. Phys. Rep. **474**, 1–75 (2009). doi:10.1016/j.physrep.2009.02.004
12. Gurvits, L.: Classical deterministic complexity of edmonds' problem and quantum entanglement. In: STOC '03: Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing, pp. 10–19. ACM, New York, NY, USA (2003) http://doi.acm.org/10.1145/780542.780545
13. Horodecki, M., Horodecki, P., Horodecki, R.: Separability of mixed states:necessary and sufficient conditions. Phys. Lett. A **223**(1–2),1–8 (1996) doi:10.1016/S0375-9601(96)00706-2. http://www.sciencedirect.com/science/article/B6TVM-3VSFHG4-1J/2/30233fc8e862b1e50e0d0a7e340f7859
14. Horodecki, M., Horodecki, P., Horodecki, R.: Separability of n-particle mixed states: necessary and sufficient conditions in terms of linear maps. Phys. Lett. A **283**(1–2),1–7 (2001) doi:10.1016/S0375-9601(01)00142-6. http://www.sciencedirect.com/science/article/B6TVM-42YFC9G-1/2/9c9d0b6d096a6b59a89d0b03fe825977
15. Horodecki, P., Ekert, A.: Method for direct detection of quantum entanglement. Phys. Rev. Lett. **89**(12), 127,902 (2002). doi:10.1103/PhysRevLett.89.127902
16. Horodecki, R., Horodecki, P., Horodecki, M., Horodecki, K.: Quantum entanglement. ArXiv Quantum Physics e-prints (2007)
17. Ioannou, L.M.: Computational complexity of the quantum separability problem. ArXiv Quantum Physics e-prints (2006)

18. Ioannou, L.M., Travaglione, B.C.: Quantum separability and entanglement detection via entanglement-witness search and global optimization. Phys. Rev. A **73**(5), 052,314 (2006). doi:10.1103/PhysRevA.73.052314
19. Kaye, P.R., Laflamme, R., Mosca, M.: An Introduction to Quantum Computing. Oxford University Press, USA (2007)
20. Keyl, M., Werner, R.F.: Estimating the spectrum of a density operator. Phys. Rev. A **64**(5), 052,311 (2001). doi:10.1103/PhysRevA.64.052311
21. Krammer, P.: Quantum entanglement—detection, classification, and quantification. Master's thesis, University of Vienna, (2005)
22. Lewenstein, M., Kraus, B., Cirac, J.I., Horodecki, P.: Optimization of entanglement witnesses. Phys. Rev. A **62**(5), 052,310 (2000). doi:10.1103/PhysRevA.62.052310
23. Lewenstein, M., Kraus, B., Horodecki, P., Cirac, J.I.: Characterization of separable states and entanglement witnesses. Phys. Rev. A **63**(4), 044,304 (2001). doi:10.1103/PhysRevA.63.044304
24. von Neumann, J.: Mathematische Grund lagen der Quantenmechanic. Springer, Berlin (1932)
25. Peres, A.: Separability criterion for density matrices. Phys. Rev. Lett. **77**(8), 1413–1415 (1996). doi:10.1103/PhysRevLett.77.1413
26. Schrödinger, E.: Die gegenwärtige situation in der quantenmechanik. Naturwissenschaften **23**(807) (1935)
27. Shor, P.:Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134 (1994) doi:10.1109/SFCS.1994.365700
28. Fiurášek, J.: Structural physical approximations of unphysical maps and generalized quantum measurements. Phys. Rev. A **66**(5), 052,315 (2002). doi:10.1103/PhysRevA.66.052315