Eur. Phys. J. Plus (2014) **129**: 128
DOI 10.1140/epjp/i2014-14128-9

THE EUROPEAN PHYSICAL JOURNAL PLUS

Regular Article

Two notes on Grover's search: Programming and discriminating*

Daniel Reitzner[1,2,a] and Mário Ziman[1,3]

[1] Institute of Physics, Slovak Academy of Sciences, Dúbravská cesta 9, 845 11 Bratislava, Slovakia
[2] Department of Physics, Hunter College of CUNY, 695 Park Avenue, New York, New York 10021, USA
[3] Faculty of Informatics, Masaryk University, Botanická 68a, 60210 Brno, Czech Republic

Received: 17 April 2014 / Revised: 14 May 2014
Published online: 23 June 2014 –

Abstract. In this work we address two questions concerning Grover's algorithm. In the first part we give an answer to the question on how to employ Grover's algorithm for actual search over database. We introduce a quantum model of an unordered phone book (quantum database) with programmable queries to search in the phone book either for a number or for a name. In the second part we investigate how successful the algorithm can be if the number of elements of the database is not known precisely. This question reduces to analysis of the distinguishability of states occurring during Grover's algorithm. We found that using an unambiguous discrimination scheme even a seemingly good guess that is close to the optimal one, can result in a rather small success rate.

1 Introduction

Grover's algorithm [1] is a typical example demonstrating the power of quantum computation. It is designed to search within an unstructured database of alternatives. Although it is used in many different applications and algorithms of quantum information theory (see, *e.g.* [2]), we have yet to succeed in finding any explicit example on how to use it to search over an actual (quantum) database. In the first part of the paper we will discuss how to design a (quantum) phone book and employ Grover's algorithm to search within either for a name or for a number. In the second part we will investigate how successful the algorithm can be if the number of elements of the database is not known (precisely). This question is posed as the analysis of the distinguishability of states occurring during Grover's algorithm.

Grover's algorithm proves to be quadratically faster than any (classical) algorithm performing the task and it was proven to be optimal [3] —there is no quantum (and no classical) algorithm that would do the task faster. The speed-up in the algorithm is in the number of oracle calls, *i.e.* evaluations of functions

$$f_x(y) = \begin{cases} 1, & \text{if } y \text{ matches } x, \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

This function evaluates whether the element x has property y (a specific example is Kronecker's delta which evaluates whether $x = y$). A set of these indexed functions $\{f_x\}_x$ can be represented by the set of paired elements (x, y) which define the database $\mathcal{D}$ of $N = |\mathcal{D}|$ elements. In this setting the database search is conveniently posed as a discrimination among the oracles implementing the functions f_x.

For its simplicity we will switch now to the phone book analogy. If we are given the task of finding the owner y of the phone number x in the phone book, then the phone book is used as an oracle in the following sense:

$$f_x(y) = \texttt{Compare}\{x, \texttt{Phonebook}(y)\}\,, \tag{2}$$

where the function $\texttt{Phonebook}(y)$ returns the phone number of the owner y and the function $\texttt{Compare}(x, x') \equiv f_x(x')$ compares the phone numbers x and x', returning 1 if and only if they match. The database search then consists of the identification of the oracle's input y returning the value 1.

* Contribution to the Focus Point on "Quantum information and complexity" edited by S. Mancini, G. Marmo, S. Pascazio.

a e-mail: reitzner@savba.sk

For the unstructured database (which we can interpret as a search for the owner of a given phone number in the phone book) each y is equally likely the correct one, *i.e.* the probability of $(x, y) \in \mathcal{D}$ has the same probability for all y's —if this were not the case, this prior information would help us search faster in the database. Therefore, in the classical case, the optimal average number of oracle queries identifying the particular oracle function is $N/2$. At this point the phone book is (typically) alphabetically ordered, thus, eq. (2) represents an efficient implementation of the oracle function. However, the efficiency of the oracle design is not of interest in the query complexity framework. It is assumed to be "expensive" in a sense that it requires a lot of resources —either energy or time to return a result that is independent of implementation. This being constant justifies the necessity to count only the number of the times the oracle is used and the complexity of the algorithm is calculated in the number of oracle calls.

The quantum algorithm discovered by Grover identifies the oracle in $O(\sqrt{N})$ calls, hence, the ability to discriminate quantum implementations of different oracle functions requires a quadratically smaller number of queries than in the classical case. Without loss of generality we may assume that both x and y are indexed from 0 to $N-1$, and choose $\mathcal{D} = \{(x, x) : x = 0, \ldots, N-1\}$. The quantum oracle is a quantum analogue of the function (1). In the quantum gate formalism it is implemented as a gate

$$R_x = I - 2|x\rangle\langle x|, \tag{3}$$

with the states $|x\rangle$ forming an orthonormal computational basis of the N-dimensional Hilbert space $\mathcal{H}_N$. This quantum oracle is a special case of a standardly used oracle

$$V_x|y\rangle \otimes |k\rangle = |y\rangle \otimes |k \oplus f_x(y)\rangle,$$

where $k = 0, 1$, thus V_x acts on the Hilbert space $\mathcal{H}_N \otimes \mathcal{H}_2$. Initializing the qubit register in the state $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2} \in \mathcal{H}_2$ we obtain $V_x|y\rangle \otimes |-\rangle = (R_x|y\rangle) \otimes |-\rangle$. From the construction of R_x in eq. (3) there follows that, for $|y\rangle$ being an element of the chosen computational basis, the states $|y\rangle \otimes |-\rangle$ are eigenvectors of V_x with eigenvalue either one or minus one (if y is the searched for element).

Each call of the oracle from eq. (3) is in the algorithm followed by a unitary operation G, called *inversion about average*, which acts as

$$G = 2|\overline{y}\rangle\langle\overline{y}| - I,$$

where $|\overline{y}\rangle = \frac{1}{\sqrt{N}} \sum_y |y\rangle$ denotes the equal superposition of all computational basis states.

After m repetitive calls of the unitary evolution $U_x = DR_x$ the initial query state $|\psi_0\rangle = |\overline{y}\rangle$ evolves into

$$|\psi_m\rangle = \sin \frac{(2m+1)\omega}{2}|x\rangle + \cos \frac{(2m+1)\omega}{2}|\overline{y}_x\rangle, \tag{4}$$

where $\cos\omega = (N-2)/N$ and $|\overline{y}_x\rangle = \frac{1}{\sqrt{N-1}} \sum_{y \neq x} |y\rangle$. We shall call the states $|\psi_m\rangle$ *Grover's states*. Clearly, if the condition $(2m+1)\omega = \pi$ is met, then $|\psi_m\rangle = |x\rangle$, hence, the search algorithm succeeds — we will mark this (in general non-integer) "number of steps" with m_0. Strictly speaking, this is possible only for $N = 4$, when a single step is needed. In all other cases the condition can never be exactly reached (for an integer), however, for large N this does not cause any problems, as the probability

$$P_G = \sin^2(2m+1)\frac{\omega}{2}$$

will still be sufficiently close to the unity. The optimal number of steps scales as $O(\sqrt{N})$ and it was shown [3] that Grover's algorithm is optimal in sense, that it reaches the boundary on the number of steps needed to find targeted element x. For more details on Grover's algorithm we refer to any quantum computation textbook, for instance [4].

This paper contains two results on Grover's oracles. In sect. 2 we look closer at the implementation of the oracle and uncover a symmetry within the "quantum database". In sect. 3 we evaluate the quantum search algorithm with unknown size of the database, which reduces to the discrimination of quantum states appearing during the Grover search algorithm.

2 Programmable search quantum database

Let us switch back again to the phone book analogy where Grover's algorithm searches over now completely unstructured phone book. Not only are the numbers of owners disordered, but now, for the sake of the argument, also the owners are randomly stored in the phone book. Such database $\mathcal{D}$ consists of N pairs (n, A); n will represent the phone number and A its owner, $\mathcal{D}_1$ will be the set of all the names (persons) in the database and $\mathcal{D}_2$ the set of all numbers. Let us stress that both the names and the numbers can be repeated and only pairs of them are unique.

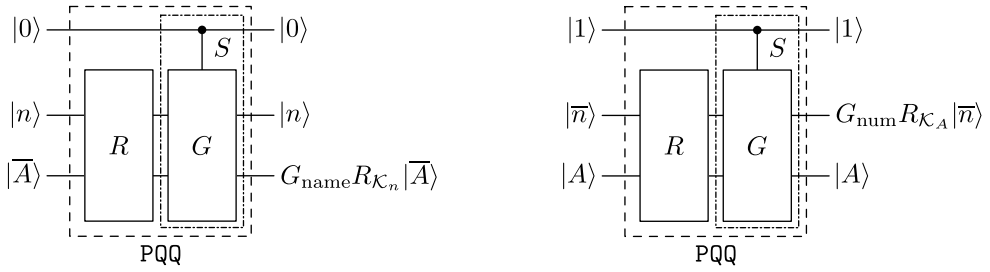

Fig. 1. The *programmable quantum query* gate performing one step of the Grover's algorithm over the phone book, when searching (a) for the name belonging to the number $|n\rangle$ or (b) for the number belonging to the name $|A\rangle$. Operation R is independent on the type of query and can be considered to be quantum database, while operation S is controlled inversion about average depending on the task performed —0 triggers inversion on the name space, while 1 triggers inversion on the number space.

Let us denote by $\mathcal{K}_n$ the subset of people having the same phone number n and by $\mathcal{K}_A$ the subset of phone numbers belonging to the person A. Then,

$$R_{\mathcal{K}_n} = I - 2\sum_{A\in\mathcal{K}_n} |A\rangle\langle A|$$
$$R_{\mathcal{K}_A} = I - 2\sum_{n\in\mathcal{K}_A} |n\rangle\langle n|$$

are Grover's oracles for searching over the names and the numbers, respectively.

We now make the key observation for the rest of this section. It is straightforward to verify that the following identity holds:

$$\sum_{n\in\mathcal{D}_1} |n\rangle\langle n| \otimes R_{\mathcal{K}_n} = \sum_{A\in\mathcal{D}_2} R_{\mathcal{K}_A} \otimes |A\rangle\langle A| \equiv R\,. \tag{5}$$

Therefore, the unitary gate,

$$R = I\otimes I - 2\sum_{(n,A)\in\mathcal{D}} |n\rangle\langle n| \otimes |A\rangle\langle A|\,,$$

can be understood as the quantum database (oracle) encoding the unstructured phone book.

Now we will show how Grover's algorithm can be employed to search over such unstructured phone book. We introduce a programmable quantum query gate (PQQ gate) allowing us to run Grover's algorithm to search either for a name, or for a phone number in a programmable fashion, *i.e.* the query is represented by the choice of the input state of the device and is completely independent of the PQQ gate containing the information stored in quantum database R. The PQQ gate is illustrated in fig. 1 and is defined by the following equation:

$$\texttt{PQQ} = S_0 \otimes (I\otimes G_{\text{name}})R + S_1 \otimes (G_{\text{num}}\otimes I)R\,, \tag{6}$$

where $G_{\text{name}} = 2|\overline{A}\rangle\langle\overline{A}| - I$, $G_{\text{num}} = 2|\overline{n}\rangle\langle\overline{n}| - I$ are the inversions over the respective averages, and $S_j = |j\rangle\langle j|$ is a classical (can be made also quantum) switch determining whether the name or the number is going to be searched for, respectively. Neither the switch nor the quantum database R depend on the particular value of the database query. The quantum query (program) $|1\rangle\otimes|\overline{n}\rangle\otimes|A\rangle$ programs PQQ gate to run Grover's search algorithm to identify the phone number matching the name A. Similarly, the query $|0\rangle\otimes|n\rangle\otimes|\overline{A}\rangle$ implements Grover's search algorithm to identify the name matching the phone number n.

In this way, we showed that the programmable oracle, due to the symmetry (5), provides not only a way to search for the owner of a phone number, but also the other direction —to search for the phone number of some owner. Both these searches can be made in time $O(\sqrt{N})$ and, recalling that the database R is unstructured in both items, it provides a quadratic speedup in both cases.

Moreover, the construction can be expanded by an additional type of information, *e.g.* mailing address or email, but the overall structure remains the same. Suppose we have k possible query tasks. The database $\mathcal{D}$ consists of N distinct k-tuples $\mathbf{x} := (x_0, x_1, \ldots, x_{k-1})$, the oracle (storing the database) is given as

$$R = I^{\otimes k} - \sum_{\mathbf{x}\in\mathcal{D}} |\mathbf{x}\rangle\langle\mathbf{x}|,$$

where $|\mathbf{x}\rangle = |x_0\rangle \otimes |x_1\rangle \otimes \cdots \otimes |x_{k-1}\rangle$. The PQQ gate is then integer-parametrized

$$\texttt{PQQ} = \sum_j S_j \otimes (I^{\otimes(j-1)} \otimes G_j \otimes I^{\otimes(k-j)})R, \tag{7}$$

when performing task j (knowing all other information but j-th); G_j is the corresponding inversion about average on register j, $G_j = 2|\bar{y}_j\rangle\langle\bar{y}_j| - I$.

A higher degree of free parameters also allows a wider variety of problems than the one mentioned above, which just serves to fill in the information j while the rest is known. In general we can be given a smaller subset of parameters characterizing the element we want to find in the database (*e.g.* knowing the phone number and email, we might want to find the name and address of the owner). This general case does not differ much from the previously discussed cases. The initial state is prepared as the equal superposition over the basis states of all unknown subspaces and as a given choice on the subspaces, where the information about the searched element is known. The PQQ is then similar to eq. (7) with j indexing the possible types of searches we might want to perform —the corresponding term in eq. (7) for given j will be then S_j tensored with operator having identity operator I on all the positions the information is known and respective G on all the positions the information is unknown to us.

Using the oracle point of view the construction and/or performance of the quantum database R is not an issue, however, from application point of view this question (especially the performance) is of high relevance. Here we have addresed only one implementation problem: the actual design of quantum database. The questions related to writing, or deleteing entries from database we left untouched.

3 Grover's search with unknown size of the database

The size of the Hilbert space we search for might be unknown, or not known precisely. It is generally a difficult problem to decide what the size of the Hilbert space is, especially when it might be rather large [5,6]. Having Grover's states as resources and being able to choose only the number of steps m after which Grover's algorithm stops, we might therefore not know how close we are to the optimal number of steps and we want to know how reliable our results will be. This question can be recast as a discrimination of quantum states produced by Grover's oracles after m uses, hence, the question is how distinguishable the states from eq. (4) are. We will investigate two extreme variations of the problem: the minimum-error discrimination optimizing the average success rate of our conclusions and the unambiguous discrimination allowing for error-free conclusions while tolerating inconclusive outcomes.

Our goal is to find a final measurement optimizing the associated success rates while keeping the rest of Grover's algorithm unchanged. Let us stress this problem is different from discrimination of Grover's oracles, where one is allowed to design also the test state and to employ ancillary systems and devices in order to optimize the success rates. In ref. [7] some results on unambiguous discrimination of Grover oracles are given, stating that the unambiguous discrimination of Grover's oracles is always possible. The exact protocols achieving perfect (error-free) discrimination of Grover's oracles were investigated in [8], where it was shown that in order to achieve such goal the number of queries scales as $N - \sqrt{N}$ with the size of the database. It achieves better scaling than any classical algorithm requiring at least $N - 1$ oracle calls. However, the quadratic speed-up is in this case lost. As far as we know, the oracle discrimination problem is still open. Grover's algorithm provides [9] an asymptotic solution to minimum-error case quantifying the number of queries needed for vanishingly small error.

3.1 Symmetry of Grover's oracles

Before we proceed, let us note that Grover's oracles U_x^m respect the following symmetry:

$$TU_{x-1}^m T^\dagger = U_x^m \ ,$$

where

$$T = \sum_x |(x+1) \mathrm{mod} N\rangle\langle x| \tag{8}$$

is the shift operator with $T^N = I$. The eigenvalues of T are $\lambda_a = \exp(\mathrm{i}2\pi a/N)$ for $a = 0, \ldots, N-1$ and corresponding eigenvectors are

$$|\gamma_a\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \mathrm{e}^{-\mathrm{i}\frac{2\pi a y}{N}} |y\rangle.$$

This symmetry feature has a favorable mathematical consequence. If we take the initial state of equal superposition $|\psi_0\rangle$, which is invariant under the action of T, *i.e.* $T|\psi_0\rangle = |\psi_0\rangle$, then the output states $|\psi_x(m)\rangle = U_x^m|\psi_0\rangle$ will respect

the same symmetry as the unitary matrices U_x^m. In this way, for each step m the Grover states $|\psi_x(m)\rangle = U_x^m|\psi_0\rangle$ form a family of symmetric states satisfying the relation $|\psi_x(m)\rangle = T^x|\psi_0(m)\rangle$, where $|\psi_0(m)\rangle = U_{x=0}^m|\psi_0\rangle$. This reduces our discrimination problems to discrimination of symmetric states $\{|\psi_x(m)\rangle\}_x$ being the set of potential output states after m steps of Grover's algorithm.

3.2 Unambiguous discrimination

Let us start with the case of unambiguous discrimination [10]. In this case, the conclusions made are certain, hence, the algorithm is exact although it requires an inconclusive result. In ref. [11] a theory of unambiguous discrimination of (pure) symmetric states is described. In particular, if we are given a set of N pure symmetric states $|\phi_x\rangle = T^x|\phi_0\rangle$ for some unitary operator T (such that $T^N = I$), then using the result of ref. [11] we can evaluate the upper bound on probability of success in unambiguous discrimination as

$$P_{\text{suc}} \leq N \min_a |\langle\gamma_a|\phi_0\rangle|^2 , \tag{9}$$

where $|\phi_0\rangle$ is the test state and $|\gamma_a\rangle$ are the eigenvectors of T.

In our case T is given by eq. (8) and we are to discriminate the states $\{T^x|\phi_0(m)\rangle\}_x$ given $|\phi_0(m)\rangle = U_0^m|\gamma_0\rangle$. We find

$$P_{\text{suc}}(m) \leq N \min_a |\langle\gamma_a|U_0^m|\gamma_0\rangle|^2 \equiv \Gamma_0(m) .$$

Let us denote $|\overline{\gamma}\rangle = \frac{1}{\sqrt{N}}\sum_a |\gamma_a\rangle = |0\rangle$ and $|\overline{\gamma}_0\rangle = \frac{1}{\sqrt{N-1}}\sum_{a\neq 0} |\gamma_a\rangle$. Then a single step of Grover's algorithm can be expressed as

$$\begin{aligned} U_0 &= 2|\gamma_0\rangle\langle\gamma_0| + 2|\overline{\gamma}\rangle\langle\overline{\gamma}| - I - \frac{4}{\sqrt{N}}|\gamma\rangle\langle\overline{\gamma}| \\ &= (I_0 - I) + \left[(1 - \frac{2}{N})I_0 - i\frac{2\sqrt{N-1}}{N}Y_0\right] , \end{aligned} \tag{10}$$

where I_0, Y_0 are Pauli operators defined on the two-dimensional subspace $\mathcal{H}_0$ spanned by the vectors $|\gamma_0\rangle$, $|\overline{\gamma}_0\rangle$, thus, $I_0 = |\gamma_0\rangle\langle\gamma_0| + |\overline{\gamma}_0\rangle\langle\overline{\gamma}_0|$, $Y_0 = -i|\gamma_0\rangle\langle\overline{\gamma}_0| + i|\overline{\gamma}_0\rangle\langle\gamma_0|$, and $I - I_0$ is the projector onto the orthogonal subspace $\mathcal{H}_0^\perp$. As in the original Grover's algorithm we define the angle ω via the identity $\cos\omega = 1 - 2/N$. Then

$$U_0^m = (I_0 - I) + e^{-im\omega Y_0} .$$

Using the above form of U_0^m we find

$$\Gamma_0(m) = \min\left\{|\cos\omega m|, \frac{|\sin\omega m|}{\sqrt{N-1}}\right\} . \tag{11}$$

The minimized elements of this function (which is the upper bound on the success probability for unambiguous discrimination) is plotted in fig. 2 (upper plot). Since $|\cos m\omega|$ and $|\sin m\omega|$ have exactly opposite monotonicity, it follows that the maximal value (with respect to m) is achieved when they coincide, *i.e.* when $|\cos m\omega| = |\sin m\omega|/\sqrt{N-1}$. This condition gives us two solutions m_0 and m_0+1 when the perfect discrimination is possible as the Grover's states become orthogonal. Also it is not surprising that (in the limit of $N \to \infty$) the success probability approaches 1 for the number of calls coinciding with the number of calls needed in Grover's search. Indeed, at this point different oracles lead to mutually orthogonal quantum states.

Relating to the question we answer in this paper, knowing the length of the database (the size of the Hilbert space) only approximately, an interesting observation is at hand. If our chosen number of steps m will be the closest integer larger than the optimal number m_0 (we recall, that m_0 is integer only for $N = 4$) but smaller than $m_0 + 1$ the unambiguous discrimination scheme can fail as the minimal term in eq. (11) will be the cosine term going to zero. If ωm is close to $\pi/2$ —this happens when $m = m_0 + 1/2$— by eq. (11) the success probability will be bounded from above by 0 and the search will be unsuccessful as Grover's states in this case are linearly dependent. This can however exactly happen only for $N = 2$ but one can get very close to this point for large N as well and the success probability can be very small, as after m_0 it drops fast towards zero —see the lower plot of fig. 2.

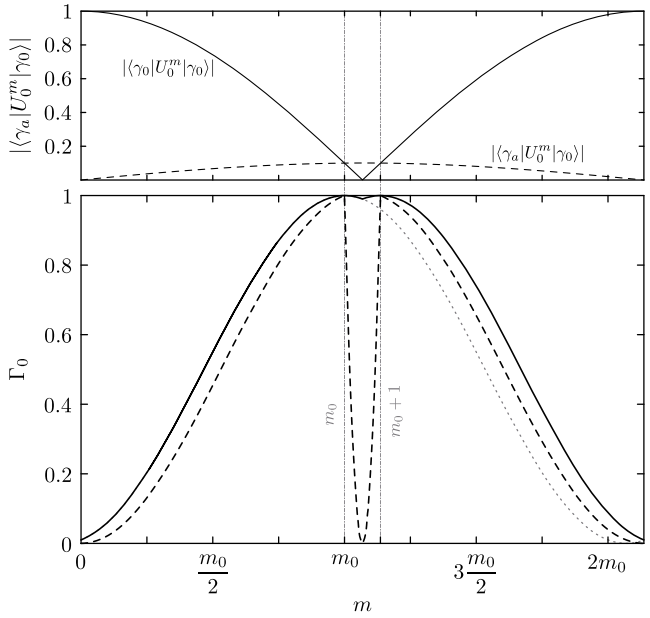

Fig. 2. Illustration (with exaggerated differences —small size of database with $N = 100$) of the bound on success probability for discrimination of Grover's oracles. The upper plot depicts the terms in Γ_0 over which we minimize, while the lower plot shows the success probabilities for the different discrimination schemes —unambiguous discrimination (dashed line) has a dip between optimal number of steps m_0 and $m_0 + 1$ that can lead to unsuccessful discrimination. The minimum-error discrimination (solid line) does not suffer from this problem and up to the point m_0 copies the usual Grover's success probability (dotted line).

3.3 Minimum-error discrimination

In the case of minimum-error discrimination, the results from ref. [12] provide necessary and sufficient conditions for discriminating states, while in ref. [13] specific results on the discrimination of states are provided. Minimum-error discrimination of pure symmetric states was addressed in ref. [14], where the optimal success probability P_M was shown to be

$$P_M = |\langle\psi_0(m)|\Omega^{-1/2}|\psi_0(m)\rangle|^2, \tag{12}$$

with

$$\begin{aligned}\Omega &= \sum_{x\in[N]} |\psi_x(m)\rangle\langle\psi_x(m)| \\ &= N\cos^2 m\omega|\overline{y}\rangle\langle\overline{y}| + \frac{N}{N-1}\sin^2 m\omega(I - |\overline{y}\rangle\langle\overline{y}|).\end{aligned}$$

Since $|\langle\psi_0(m)|\overline{y}\rangle|^2 = \cos^2 m\omega$, from eq. (12) we find

$$P_M = \left|\frac{1}{\sqrt{N}}\cos m\omega + \sqrt{\frac{N-1}{N}}\sin m\omega\right|^2.$$

From this equation we obtain (see also fig. 2)

$$P_M = \begin{cases}\sin^2(2m+1)\omega/2, & \text{for } m \le m_0 + 1/2,\\ \sin^2(2m-1)\omega/2, & \text{for } m \ge m_0 + 1/2.\end{cases}$$

Again, we may notice perfect discrimination ($P_M = 1$) not only at $m = m_0$ but also at $m = m_0 + 1$ when the states would be orthogonal and the minimum-error discrimination coincides with the unambiguous discrimination. For choice of m smaller than $m_0 + 1/2$ the success probability copies that of the usual Grover's search, and for m larger it becomes slightly advantageous. If the choice of m falls in the region $[m_0, m_0 + 1]$, in contrast to the unambiguous discrimination scheme where the probability drops towards zero, we do not have any considerable drop in probability showing that minimum-error discrimination is in this sense superior to the unambiguous discrimination scheme. Furthermore, considering only integer m, none of the discrimination schemes can be perfect.

4 Conclusion

We have introduced the concept of programmable search database (see fig. 1) employing (in a programmable way) Grover's oracles to search over an unstructured databases (like a phone book). It enables us to choose query (either name, or phone number) and search for its complement (phone number or name, respectively) from the unstructured database. Because of the symmetry of the programmable search database for any query the complexity is the same as for Grover's algorithm but offers a lot of flexibility. Moreover, this construction works also for higher degree of searchable items (like mailing address, e-mail, etc.). We believe this note clarifies how the Grover algorithm might actually be used for searching a quantum database, especially with more degrees of freedom within which one might want to search. Although we have not addressed the question of how the database would be physically constructed, this note provides an outlook on what one should consider —the symmetry of the oracle, if implemented, would make the search more universal.

In the second note we have discussed the performance of Grover's search algorithm when the size of the database is unknown, but the resources (probe state and oracles) are available at user's disposal. We have found that the measurement point has to be chosen carefully (even if the guess is almost precise), as in a small range between the points of perfect discrimination, the success probability can drop significantly (see fig. 2). This feature holds for unambiguous approach and therefore minimum error might be favored more if the size of the database is not known exactly. Minimum-error discrimination seems to be more practicable as it not only overcomes the pit near $m_0+1/2$ but it also works in the presence of small errors. Moreover, it might be applied more easily, as the bound for unambiguous discrimination can be hard to reach. Finally, as for the number of steps smaller than m_0 it copies the usual success probability for Grover's search we see that the measurement in the computational basis performs the minimum error discrimination. The unambiguous discrimination, although very interesting from the theoretical point of view, is to large extent impractical.

The two presented notes cover only a small set of directions of interest where only partial results are known. For example we still do not know what an actual realization might look like —quite possibly it will be a subroutine in a larger algorithmic application [2]. Other interesting directions to pursue are geometric analysis of Grover's search [15] or quantum searches under decoherence [16,17].

This work was supported by projects APVV-0808-12 (QIMABOS) and COST Action MP1006. M.Z. acknowledges the support of RAQUEL and GAČR project P202/12/1142. D.R. acknowledges the support of Fulbright Visiting Scholar Program.

References

1. L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
2. A. Ambainis, SIAM J. Comput. **37**, 210 (2007).
3. C.H. Bennett, E. Bernstein, C. Brassard, U. Vazirani, SIAM J. Comput. **26**, 1510 (1997).
4. M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
5. N. Brunner, S. Pironio, A. Acin, N. Gisin, A.A. Méthot, V. Scarani, Phys. Rev. Lett. **100**, 210503 (2008).
6. M.M. Wolf, D. Perez-Garcia, Phys. Rev. Lett. **102**, 190504 (2009).
7. A. Chefles, A. Kitagawa, M. Takeoka, M. Sasaki, J. Twamley, J. Phys. A **40**, 10183 (2007).
8. X. Wu, R. Duan, Phys. Rev. A **78**, 012303 (2008).
9. C. Zalka, Phys. Rev. A **60**, 2746 (1999).
10. M. Sedlák, Acta Phys. Slovaca **59**, 653 (2009).
11. A. Chefles, S.M. Barnett, Phys. Lett. A **250**, 223 (1998).
12. A.S. Holevo, J. Multivar. Anal. **3**, 337 (1973).
13. S.M. Barnett, S. Croke, J. Phys. A **42**, 062001 (2009).
14. M. Ban, K. Kurokawa, R. Momose, O. Hirota, Int. J. Theor. Phys. **36**, 1269 (1997).
15. C. Cafaro, S. Mancini, Physica A **391**, 1610 (2012).
16. N. Shenvi, K.R. Brown, K.B. Whaley, Phys. Rev. A **68**, 052313 (2003).
17. O. Regev, L. Schiff, *Impossibility of a Quantum Speed-Up with a Faulty Oracle*, in *Proceedings of the 35th International Colloquium on Automata, Languages and Programming*, Vol. **1** (2008) p. 773.