REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
MAR 2012	Journal Article Post Print	OCT 2009 – SEP 2011

4. TITLE AND SUBTITLE

GROVER'S SEARCH ALGORITHM WITH AN ENTANGLED DATABASE STATE

5a. CONTRACT NUMBER
IN-HOUSE QIS0PROJ

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Paul M. Alsing; Nathan McDonald

5d. PROJECT NUMBER
QIS0

5e. TASK NUMBER
PR

5f. WORK UNIT NUMBER
OJ

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

AFRL/RITA
525 Brooks Road
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/RITA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TP-2012-002

12. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA #: 88ABW-2011-1380
DATE CLEARED: 15 MAR 2011

13. SUPPLEMENTARY NOTES
2011 Defense Security and Sensing Conference, Orlando, FL, 25-29 Apr 2011; Proc. of SPIE Vol. 8057, 80570R (2 May 2011).

14. ABSTRACT
Grover's oracle based unstructured search algorithm is often stated as "given a phone number in a directory, find the associated name. This paper examines an amplitude amplification algorithm in which the user encodes the directory (e.g. names and telephone numbers) into an entangled database state, which at a later time can be queried on one supplied component entry (e.g. a given phone number t0) to find the other associated unknown component (e.g. name x0). For N=2^n names x with N associated phone numbers t , performing amplitude amplification on a subspace of size N of the total space of size N^2 produces the desired state $|x0\rangle|t0\rangle$ in $\sqrt{N}$ steps. We discuss how and why sequential (though not concurrent parallel) searches can be performed on multiple database states. Finally, we show how this procedure can be generalized to databases with more than two correlated lists (e.g. $|x\rangle|t\rangle|s\rangle|r\rangle$ …).

15. SUBJECT TERMS
quantum computing, Grover's search algorithm, quantum algorithms

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			PAUL M. ALSING
U	U	U	UU	18	19b. TELEPHONE NUMBER (*Include area code*) N/A

Grover's search algorithm with an entangled database state

Paul M. Alsing*[a], Nathan McDonald[a]
[a]Air Force Research Laboratory, Information Directorate, 525 Brooks Rd, Rome, NY 13441

ABSTRACT

Grover's oracle based unstructured search algorithm is often stated as "given a phone number in a directory, find the associated name." More formally, the problem can be stated as "given as input a unitary black box U_f for computing an unknown function $f:\{0,1\}^n \rightarrow \{0,1\}$ find $x=x_0$ an element of $\{0,1\}^n$ such that $f(x_0)=1$, (and zero otherwise). The crucial role of the externally supplied oracle U_f (whose inner workings are unknown to the user) is to change the sign of the solution $|x_0\rangle$, while leaving all other states unaltered. Thus, U_f depends on the desired solution x_0. This paper examines an amplitude amplification algorithm in which the user encodes the directory (e.g. names and telephone numbers) into an entangled database state, which at a later time can be queried on one supplied component entry (e.g. a given phone number t_0) to find the other associated unknown component (e.g. name x_0). For $N=2^n$ names $|x\rangle$ with N associated phone numbers $|t\rangle$, performing amplitude amplification on a subspace of size N of the total space of size N^2 produces the desired state $|x_0\rangle|t_0\rangle$ in $\sqrt{N}$ steps. We discuss how and why sequential (though not concurrent parallel) searches can be performed on multiple database states. Finally, we show how this procedure can be generalized to databases with more than two correlated lists (e.g. $|x\rangle|t\rangle|s\rangle|r\rangle\ldots$).

Keywords: quantum computing, Grover's search algorithm, quantum algorithms

1. INTRODUCTION

In addition to Shor's factorization algorithm[1], Grover's search algorithm[2] is another highly recognized quantum algorithm, being widely taught in many texts on quantum computation,[3,4] and serves as a benchmark for nascent physical implementations of quantum computers[5]. Grover's search algorithm (GSA) considers the following scenario[6], suppose you have a large table T[0…N-1] of N entries for which you would like to find some element z_0. More precisely, you wish to find an integer x_0 such that $0 \le x_0 < N$ and $T[x_0]= z_0$, provided that such an x_0 exists. If the table is sorted the problem can be solved in a time $O(\log N)$. However, in many interesting problems, ordering or structuring the data may not be possible or practical, and one must resort to the brute force method of exhaustively searching through all the data until the result is found (or to determine if it even exists). Classically, there is no algorithm that succeeds with probability greater than ½ without searching through more than half the entries of T. Grover[1] described his algorithm as finding a needle in the haystack, and equivalently as finding the associated name in a telephone book when one is supplied with a given telephone number (in which the telephone book is sorted on the names, but random on the telephone numbers). Grover's quantum unstructured search algorithm can solve this problem on a quantum computer in expected time in $O(\sqrt{N})$. The GSA has also been shown to be optimal[6], implying that a quantum algorithm cannot achieve faster than a quadratic speedup over its classical counterpart.

The GSA utilizes an *oracle*, which computes a function $f(x)$ of the input x, but whose inner workings is unknown and unavailable to the user. The Grover search problem can be stated formally[3] as

The Grover Search Problem

Input: A black box (oracle) U_f for computing an unknown function $f:\{0,1\}^n \rightarrow \{0,1\}$.

Problem: Find an input $x_0 \in \{0,1\}^n$ such that $f(x_0)=1$ and $f(x\neq x_0)=0$.

In the above, f is the classical function which evaluates to "yes" on the needle and "no" on the more abundant pieces of hay in the haystack. U_f is the unitary representation of f which acting on x encoded into a quantum multi-qubit state $|x\rangle$, performs the reversible operation

Quantum Information and Computation IX, edited by Eric Donkor, Andrew R. Pirich, Howard E. Brandt,
Proc. of SPIE Vol. 8057, 80570R · © 2011 SPIE · CCC code: 0277-786X/11/$18 · doi: 10.1117/12.883092

$$U_f|x\rangle\otimes|y\rangle=|x\rangle\otimes|y\oplus f(x)\rangle, \tag{1}$$

where $|y\rangle$ is a single auxiliary qubit and $\oplus$ denotes binary (mod 2) addition. (Note: from now on we will often write the tensor products of state $|x\rangle\otimes|y\rangle$ simply as $|x\rangle|y\rangle\equiv|x,y\rangle$).

As is well known, and as will be explicitly illustrated below, U_f requires knowledge of the solution x_0 in order to be explicitly constructed[4]. This is why the oracle U_f is part of the input to the GSA, and it has to be supplied externally to the user performing the search. Recently, there has been interest in developing algorithms that would dispense with the Grover oracle U_f and encode the search list directly into a quantum database state which can be initially constructed (e.g. an encoding of a telephone book), and subsequently searched at a later time (e.g. given a telephone number, find the associated name). Xu *et al.*[7] have designed such an $O(\sqrt{N})$ algorithm based on adiabatic quantum computing (AdQC) and experimentally demonstrated its operation on a two qubit "telephone book" in an NMR quantum computer. In their work, only the names were encoded into the quantum database state, while the telephone numbers were encoded as classical integers. The goal of this paper is enunciate a quantum search algorithm (QSA), analogous in spirit to Xu *et al.*[7], but in the usual quantum circuit model paradigm (i.e. an explicit unitary operator approach vs the Hamiltonian approach of AdQC).

In the following, we briefly recall the GSA in a now standard form that elucidates its functionality and its generalization to quantum amplitude amplification (QAA) algorithms. In addition, we illustrate the GSA on a simple two qubit search, explicitly constructing the Grover oracle U_f revealing its dependence on the solution x_0. We then briefly describe the non-oracle AdQC database search of Xu *et al.*[7] and describe why it succeeds. We illustrate their algorithm (as their paper does) on a simple telephone book search example. Next, we turn to the main portion of this paper, in which we detail a QSA where both the names and telephone numbers are encoded into a quantum database state. For $N=2^n$ names $|x\rangle$ with N associated phone numbers $|t\rangle$ we show how our QSA performs amplitude amplification on a subspace of size N of the total Hilbert space of size N^2, and produces the desired target state $|x_0\rangle|t_0\rangle$ in $O(\sqrt{N})$ steps given a randomly chosen telephone number t_0. We further discuss how and why sequential (though not concurrent parallel) searches can be performed on multiple database states. Finally, we show how this procedure can be generalized to databases with more than two correlated lists (e.g. $|x\rangle|t\rangle|s\rangle|r\rangle\ldots$).

2. GROVER'S SEARCH ALGORITHM

2.1 The Grover iteration and the phase kickback or solution tagging operation

The essential operation in Grover's algorithm is the Grover iteration[3]

$$G=U_{\psi^\perp}U_f \tag{2}$$

composed of two functionally distinct unitary components (i) U_f, the phase kickback (PK) or "solution tagging" operation, and (ii) $U_{\psi^\perp}$, the inversion about the mean (IAM). The phase kickback unitary operation works as follows

$$U_f|x\rangle\otimes|-\rangle=U_f|x\rangle\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}=|x\rangle\otimes\frac{|0\oplus f(x)\rangle-|1\oplus f(x)\rangle}{\sqrt{2}}=(-1)^{f(x)}|x\rangle\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}=(-1)^{f(x)}|x\rangle\otimes|-\rangle \tag{3}$$

where we have used (1) with $|y\rangle=H|1\rangle\equiv|-\rangle=(|0\rangle-|1\rangle)/\sqrt{2}$ with the Hadamard operator $H=\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\Big/\sqrt{2}$ which also maps $H|0\rangle\equiv|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$. In the first equality of (3), U_f acts on both terms of $|y\rangle$ simultaneously (quantum parallelism). Explicitly working out both cases $f(x_0)=1$ and $f(x\neq x_0)=0$ yields two results that can be encapsulated into the single statement given by the rightmost expression. This is the famous phase kickback[2,3,4] in which the evaluation of the function f is stored in the quantum phases $e^{i\theta}$ (here, with $\theta\in\{0,\pi\}$). Since the single auxiliary qubit $|y\rangle=|-\rangle$ is returned to its initial state after the PK operation, one often abbreviates (3) to

$$U_f|x\rangle=(-1)^{f(x)}|x\rangle \tag{4}$$

with the understanding that the required auxiliary qubit $|y\rangle$ is implied. The net result of U_f is that the sought after solution state $|x_0\rangle$ is flagged with a -1, while all other states $|x \neq x_0\rangle$ are unchanged. An explicit matrix realization[4] of the unitary operator U_f is shown in Fig. 1 for the case of two qubits with solution state $x_0 = 2$ in the decimal representation, corresponding to 10 in the binary representation. (From now on we will primarily use the decimal representation x∈{0,1,…,N-1} on n qubits, where $N=2^n$). Figure 1 illustrates the assertion that one needs to know the solution x_0 in order to construct the oracle U_f.

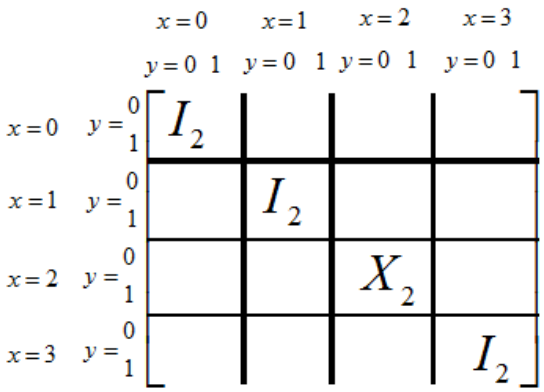


Fig.1 Explicit construction of the unitary phase kickback operator U_f^{xy} for the case of two qubits labeled by the decimal x∈{0,1,2,3} (↔{00,01,10,11}, binary) representation. In this example, the solution state is $x_0 = 2$ (binary, 10), X_2 denotes the 2x2 Pauli σ_x bit-flip matrix and I_2 denotes the 2x2 unit matrix. The superscript xy on U_f^{xy} denotes that the PK operation acts upon the 3-qubit state $|x\rangle \otimes |y\rangle$, where y is a single qubit auxiliary state.

In Fig.1, the x= x_0=2 diagonal block of U_f^{xy} contains the 2x2 Pauli bit-flip matrix denoted as X_2 which flips the single auxiliary y qubit. All other x≠x_0 diagonal blocks U_f^{xy} contain the 2x2 identity matrix, denoted as I_2, which leaves the y qubit unaltered. The superscript xy on U_f^{xy} denotes that the PK operation acts upon the 3-qubit states $|x\rangle \otimes |y\rangle$, and the net effect is to multiply the state $|x_0\rangle \otimes |-\rangle$ by the phase factor -1, leaving all other states unaltered. Since there are N=4=2^2 qubits in this example, there are 4 block diagonals in which to place the bit-flip operator X_2. The choice of which specific diagonal block is X_2 placed is determined by the solution state x_0. Formally, the PK operation has the form $U_f^{xy} = |x_0\rangle\langle x_0| \otimes X_2^y + \sum_{x \neq x_0} |x\rangle\langle x| \otimes I_2^y$ that explicitly illustrates this point. Thus, the construction of the PK operator requires knowledge of the solution state x_0. This is the primary reason why U_f^{xy} is given as an "input" to the GSA, and is considered as an *externally provided* oracle.

2.2 The inversion about the mean operation

The second unitary in the Grover iterate (2) is the inversion about the mean operation, given by

$$U_{\psi^\perp} = H^{\otimes n} U_{0^\perp} H^{\otimes n} \tag{5}$$

where $H^{\otimes n}$ takes the n-qubit initial state $|0\rangle$ to the unbiased, equal amplitude product state $|\psi\rangle = 1/\sqrt{N} \sum_{x=0}^{N-1} |x\rangle \equiv \prod_{i=0}^{N-1} H|0\rangle_i$ (the n-fold tensor product of $H|0\rangle_i$ of all qubits). For n-qubits, we will denote this for simplicity as

$$H|0\rangle = |\psi\rangle . \tag{6}$$

The operator $U_{0^\perp}$ is defined as

$$U_{0^\perp}|0\rangle = |0\rangle,$$
$$U_{0^\perp}|x \neq 0\rangle = -|x \neq 0\rangle. \quad (7)$$

Note that $U_{0^\perp}$ does not require knowledge of the solution state x_0; it simply flips the sign of all states except the standard initial state x=0. $U_{0^\perp}$ therefore, has the representation $U_{0^\perp} = |0\rangle\langle 0| - |1\rangle\langle 1| - \ldots - |N-1\rangle\langle N-1| = 2|0\rangle\langle 0| - I_N$ where we have used the completeness relation $I_N = \sum_{x=0}^{N-1} |x\rangle\langle x|$, with I_N being the NxN unit matrix. Thus, using (6) we can express $U_{\psi^\perp}$ in (5) as

$$U_{\psi^\perp} = 2|\psi\rangle\langle\psi| - I_N. \quad (8)$$

A straightforward calculation[3,4] reveals that $U_{\psi^\perp}$ maps the amplitudes c_x of arbitrary quantum state $|\varphi\rangle = \sum_x c_x |x\rangle$ according to $c_x \mapsto 2\bar{c} - c_x$ where $\bar{c} = \sum_x c_x / N$ is the average of all the quantum amplitudes c_x. This is easily seen since $\text{Avg} \equiv |\psi\rangle\langle\psi|$ is the matrix with each entry taking the value 1/*N*, that maps an arbitrary quantum vector $|\varphi\rangle$ to a vector whose every component is $\bar{c}$. Thus, $U_{\psi^\perp}$ performs an inversion of each quantum amplitude c_x about its mean value $\bar{c}$.

2.3 The Grover iteration as an effective rotation operator

The essence of the GSA is that U_f acts simply in a 2-dimensional basis which we denote as the 2D column vector (where T = transpose) $|f_i\rangle_{i\in\{1,2\}} \equiv \left[|\psi\rangle_{bad}, |\psi\rangle_{good}\right]^T$, and $U_{\psi^\perp}$ acts simply in a different basis denoted as $|g_i\rangle_{i\in\{1,2\}} \equiv \left[|\psi\rangle, |\bar{\psi}\rangle\right]^T$, defined and motivated as follows. We can decompose the state $|\psi\rangle$ (assuming the existence of only a single solution x_0 for simplicity of exposition) as (using repeated index summation convention)

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x\neq x_0} |x\rangle + \frac{1}{\sqrt{N}} |x_0\rangle = \frac{\sqrt{N-1}}{\sqrt{N}} \left(\frac{1}{\sqrt{N-1}} \sum_{x\neq x_0} |x\rangle \right) + \frac{1}{\sqrt{N}} |x_0\rangle \equiv \cos\theta |\psi_{bad}\rangle + \sin\theta |\psi_{good}\rangle \equiv \psi_i |f_i\rangle;\ \sin\theta \equiv \frac{1}{\sqrt{N}}. \quad (9)$$

$|\bar{\psi}\rangle$ is defined as the 2-dimensional state orthogonal to $|\psi\rangle$ defined as

$$|\bar{\psi}\rangle \equiv -\sin\theta |\psi_{bad}\rangle + \cos\theta |\psi_{good}\rangle. \quad (10)$$

The action of U_f and $U_{\psi^\perp}$ in these bases are given as

$$U_f \begin{bmatrix} |\psi_{bad}\rangle \\ |\psi_{good}\rangle \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} |\psi_{bad}\rangle \\ |\psi_{good}\rangle \end{bmatrix} = \begin{bmatrix} |\psi_{bad}\rangle \\ -|\psi_{good}\rangle \end{bmatrix};\ U_{\psi^\perp} \begin{bmatrix} |\psi\rangle \\ |\bar{\psi}\rangle \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} |\psi\rangle \\ |\bar{\psi}\rangle \end{bmatrix} = \begin{bmatrix} |\psi\rangle \\ -|\bar{\psi}\rangle \end{bmatrix}, \quad (11)$$

and the bases are related by a simple rotation R in a 2D plane

$$\begin{bmatrix} |\psi\rangle \\ |\bar{\psi}\rangle \end{bmatrix} \equiv R \begin{bmatrix} |\psi_{good}\rangle \\ |\psi_{bad}\rangle \end{bmatrix} \equiv \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} |\psi_{bad}\rangle \\ |\psi_{good}\rangle \end{bmatrix} \Leftrightarrow |f_i\rangle = R_{ij} |g_j\rangle. \quad (12)$$

From (11) we see that in their respective bases, both U_f and $U_{\psi^\perp}$ act as the 2x2 Pauli phase-flip operator $Z_2 = \sigma_z$. The application of a single Grover iteration G can now be carried out in matrix-vector form as

$$\begin{aligned} |\psi^{(1)}\rangle = G|\psi\rangle = \psi_i U_{\psi^\perp} U_f |f_i\rangle = \psi_i U_{\psi^\perp} \left(U_f\right)_{ij} |f_j\rangle = \psi_i U_{\psi^\perp} \left(U_f\right)_{ij} \left(R^{-1}\right)_{jk} |g_k\rangle = \psi_i \left(U_f\right)_{ij} \left(R^{-1}\right)_{jk} U_{\psi^\perp} |g_k\rangle \\ = \psi_i \left(U_f\right)_{ij} \left(R^{-1}\right)_{jk} \left(U_{\psi^\perp}\right)_{kl} |g_l\rangle \\ = \psi_i \left(U_f\right)_{ij} \left(R^{-1}\right)_{jk} \left(U_{\psi^\perp}\right)_{kl} R_{lm} |f_m\rangle \\ \equiv \psi_i G_{im} |f_m\rangle \\ \equiv \psi_m^{(1)} |f_m\rangle, \end{aligned} \quad (13)$$

with

$$\psi_m^{(1)} = \psi_i \, G_{im} = [\cos\theta, \sin\theta] \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{bmatrix} = [\cos 3\theta, \sin 3\theta], \tag{14}$$

which rotates $|\psi\rangle$, with small initial angle $\theta \sim 1/\sqrt{N}$ from the non-solution $|\psi_{bad}\rangle$, to the new angle 3θ lying incrementally closer to the solution state $|\psi_{good}\rangle$. After k successive Grover iterations $|\psi^{(k)}\rangle = G^k |\psi\rangle$, repeated applications of (14) yields $\psi_m^{(k)} = [\cos(2k+1)\theta, \sin(2k+1)\theta]$, i.e. $|\psi^{(k)}\rangle = \cos(2k+1)\theta |\psi_{bad}\rangle + \sin(2k+1)\theta |\psi_{good}\rangle$. The GSA is terminated under the condition (for $N \gg 1$) that $\pi/2 = (2k+1)\theta \sim 2k\theta \sim 2k/\sqrt{N}$ or $k \sim \lfloor \pi\sqrt{N}/4 \rfloor$ (where $\lfloor x \rfloor$ denotes *floor*(x), the nearest integer less than x). This is the famous quadratic speedup of the GSA over the classical brute force unstructured search. With these approximations, we have $\sin(2k\theta + \theta) \sim \cos\theta = \sqrt{N-1}/\sqrt{N}$ and $\cos(2k\theta + \theta) \sim -\sin\theta \sim -1/\sqrt{N}$, yielding $|\psi^{(k)}\rangle = -\sin\theta |\psi_{bad}\rangle + \cos\theta |\psi_{good}\rangle \sim -1/\sqrt{N} |\psi_{bad}\rangle + \sqrt{N-1}/\sqrt{N} |\psi_{good}\rangle$. The ratio of the probability to find the good state solution to the bad state non-solution upon a (von Neumann) measurement of the state $|\psi^{(k)}\rangle = G^{(k)} |\psi\rangle$ is

$$\frac{P(\text{good})}{P(\text{bad})} = \frac{\sin^2\theta}{\cos^2\theta} \sim \left(\frac{\sqrt{N-1}/\sqrt{N}}{1/\sqrt{N}} \right)^2 \sim N \, . \tag{15}$$

In other words, the initial amplitude $\sin\theta$ of finding the solution has undergone an *amplitude amplification* by a factor of $\cot\theta \sim \sqrt{N}$, significantly increasing the probably to detect upon measurement of the final state.

3. THE ADQC NON-ORACLE VARIANT OF THE GSA BY XU ET AL.[7]

In this section, we briefly review essential ingredients of the adiabatic quantum computing, non-oracle variant of the GSA by Xu *et al.*[7]. The motivation of these authors was to circumvent the construction of U_f^{xy} (see Fig.1) by the agent conducting the search (the searcher) that would require, as discussed in the previous section, his/her explicit knowledge of the sought after solution state $|x_0\rangle$. They accomplished this goal by encoding both the names and telephone numbers (the example Grover originally suggests) into a database state, which can be constructed and stored at some point in the past, and interrogated later in the future when a random telephone number is given, and the associated name is sought. To perform this database search, they utilized the adiabatic quantum computing methodology.

Briefly, in adiabatic quantum computing (AdQC) the emphasis is on the construction of a time dependent Hamiltonian $H(t)$ whose (time-ordered) exponentiation yields a time varying unitary evolution $U(t)$. The crucial mathematical result is that if the evolution is slow enough (i.e $H(t)/(dH(t)/dt)$ "sufficiently" small to avoid undesirable level crossings) the physical system remains in the instantaneous ground state $|\psi_0(t)\rangle$. Thus, one constructs a Hamiltonian of the form $H(t) = [1\text{-}s(t)]\, H_i + s(t)\, H_p$, where H_i is the initial Hamiltonian at time $t=0$ whose ground state is known and easy to achieve physically, and H_p is the problem Hamiltonian whose ground state at time $t=T$ is the solution to the search problem. The monotonic function $s(t)$ satisfies the simple requirements that $s(0)=0$ and $s(T)=1$, as we adiabatically switch from H_i to H_p over the course of the evolution $t=[0,T]$.

Xu *et al.*[7] chose $H_i = g\sum_{i=0}^{N-1} X_i$, where g is some arbitrary coupling constant and X_i is the Pauli bit-flip operator for the ith qubit. Since $X_i |\pm\rangle_i = \pm |\pm\rangle_i$, the ground state of H_i is readily given by the equal amplitude product state $|\psi_0(0)\rangle = 1/\sqrt{N} \prod_{i=0}^{N-1} |-\rangle_i$. The innovation of Xu *et al.*[7] was to encode the telephone book database into the diagonal database operator D given by

$$D = \sum_{i=0}^{N-1} \mathrm{v}_i \, |i\rangle\langle i| \, , \tag{16}$$

where the name i is encoded into the quantum state $|i\rangle$ and the corresponding telephone number v_i is encoded into an (classical) integer. The encoding of the telephone book (the database consisting of a two lists, one of names and the other of corresponding telephone numbers, each of which may be chosen as a random permutation of the integers [0,…,N-1]) takes place at some time in the past, and the state D is stored and saved until searching is requested. Upon the selection of a randomly chosen telephone number v_{i^*} one constructs the problem Hamiltonian H_p as

$$H_p = \left(\sum_{i=0}^{N-1} \mathrm{v}_i |i\rangle\langle i| - \mathrm{v}_{i^*} I_N \right)^2 = \left(D - \mathrm{v}_{i^*} I_N \right)^2 . \tag{17}$$

The action of D on an arbitrary computational state $|i\rangle$ is given by $D|i\rangle = \mathrm{v}_i |i\rangle$. Consequently, the action of H_p on the same state $|i\rangle$ is given by

$$H_p |i\rangle = \left(D - \mathrm{v}_{i^*} I_N \right)^2 |i\rangle = \left(\mathrm{v}_i - \mathrm{v}_{i^*} \right)^2 |i\rangle = 0 \left| i^* \right\rangle = 0 \text{ iff } i = i^* , \tag{18}$$

indicating that the ground state of H_p is given by the state $\left| i = i^* \right\rangle$, i.e. the sought for quantum state that was associated with the (randomly) selected name v_{i^*} in the quantum database operator D. The rest of the paper by Xu *et al.*[7] details an experimental implementation of this scheme in an NMR setting. In particular, the application of the unitary evolution $U(t)$ is given by usual Trotter expansion of chopping up the Hamiltonian $H(t)$ in piecewise constant terms $H(\bar{t})$ over small time intervals $[t, t+\Delta t]$ and implementing $U(t) = \prod_k e^{-iH(\bar{t}_k)\Delta t}$ which is accurate to second order in Δt. The key idea of this approach is to encode the database into a quantum state, and then subsequently search on one subspace of the system (e.g. telephone numbers) which is indexed to the sought after item in the other subspace of the system (i.e. the corresponding names).

4. GSA WITH AN ENTANGLED DATABASE STATE

4.1 General amplitude amplification

It is well known[3,6] that the Grover iteration (2) can be extended to the more general case

$$G = U_{\psi^\perp} U_f = A U_{0^\perp} A^\dagger U_f , \tag{19}$$

where A is the operator that takes the standard initial state $|0\rangle$ on n qubits to an initial "guess" state, often taken to be the equal amplitude, unbiased state $|\psi\rangle = 1/\sqrt{N} \sum_{x=0}^{N-1} |x\rangle$,

$$A|0\rangle = A \begin{bmatrix} 1 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 1/\sqrt{N} \\ 1/\sqrt{N} \\ \vdots \\ \vdots \\ 1/\sqrt{N} \end{bmatrix} = |\psi\rangle \quad \Rightarrow \quad A = \begin{bmatrix} \left(\\ \left| \psi \right\rangle \\ \left(\end{array} \right) \left(\right) & \cdots & \left(\right) \\ \left(\right) \end{bmatrix} . \tag{20}$$

From left hand side of (20), we see that the initial state $|0\rangle$ picks out the first column of A, which is $|\psi\rangle$. The rest of the columns of A can be chosen arbitrarily, only under the restriction that A is unitary $AA^\dagger = I_\mathrm{N}$, requiring that all columns (and all rows) are mutually orthonormal. Note that in standard Grover iteration (2) $A = H^{\otimes n}$. Further, $A|0\rangle = |\psi\rangle$ ensures that $U_{\psi^\perp} = A U_{0^\perp} A^\dagger = 2|\psi\rangle\langle\psi| - I_N$ is again the inversion about the mean operator (8).

4.2 The quantum database state and the subspace phase kickback operation

We now develop a quantum database state $|\psi_{db}\rangle$, this time in the quantum circuit model approach in which we explicitly state the unitary evolution operators (vs the AdQC approach, in which the focus is on the constructed Hamiltonians). Again we utilize the example of a telephone directory database. We will encode *both* the names and the telephone numbers into quantum states, and illustrate our implementation explicitly with the example utilizing n=2 qubits for the

names and n=2 qubits for the telephone numbers, while concurrently developing formulas for an arbitrary number n of qubits. We consider the case of $N=2^n$ (name, telephone number) pairs $\{x_i, t_i\}_{i\in[0,\ldots,N-1]}$. The quantum database state $|\psi_{db}\rangle$ is given by

$$|\psi_{db}\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|x_i\rangle_x \otimes |t_i\rangle_t , \tag{21}$$

which is, in general, an entangled state between the name and telephone component states.
Note that $|\psi_{db}\rangle$ is an N-dimensional vector in a N^2 dimensional Hilbert space, where the most general state is given by

$$|\Psi\rangle = \frac{1}{\sqrt{N^2}}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} a_{ij}|i\rangle_x \otimes |j\rangle_t \equiv \frac{1}{\sqrt{N^2}}\sum_{k=0}^{N^2-1} b_k |k\rangle_{xt} \in \boldsymbol{H}_x \otimes \boldsymbol{H}_t , \tag{22}$$

where $\boldsymbol{H}_x$ and $\boldsymbol{H}_t$ are the N-dimensional Hilbert spaces of the names and telephone numbers, respectively. In (21) and (22) we use a subscript notation to denote which Hilbert space the ket belongs $|i\rangle_x \in \boldsymbol{H}_x$, $|j\rangle_t \in \boldsymbol{H}_t$ and $|k\rangle_{xt} \in \boldsymbol{H}_x \otimes \boldsymbol{H}_t$. Let us consider the specific example of n=2, $N=2^n$ =4, and utilize the decimal representation of the states (i.e. $\{x_i, t_i\}_{i\in[0,1,2,3]}$). Consider a telephone directory and corresponding database state given by

$$\begin{array}{cccc} & \text{names} & \text{telephone \#s} & \\ \{x_i,t_i\}_{i\in[0,1,2,3]} = & 0 & 2 & \\ & 1 & 3 & \Rightarrow |\psi_{db}\rangle = \frac{1}{\sqrt{4}}\left(|0\rangle_x|2\rangle_t + |1\rangle_x|3\rangle_t + |2\rangle_x|0\rangle_t + |3\rangle_x|1\rangle_t\right) \\ & 2 & 0 & \\ & 3 & 1 & \end{array} \tag{23}$$

$$= \frac{1}{\sqrt{4}}\left(|2\rangle_{xt} + |7\rangle_{xt} + |8\rangle_{xt} + |13\rangle_{xt}\right), \text{ where } |x_i\rangle_x|t_i\rangle_t \mapsto |Nx_i + t_i\rangle_{xt} .$$

Note that while we have ordered the names in (23) sequentially, the two lists of names and telephone numbers can in general be chosen as random permutations of the integers [0,1,…,N-1]. Our rational for constructing the database state $|\psi_{db}\rangle$ is simple. Given the telephone directory (the database) we, as the eventual searcher (database interrogator), can encode this classical information into the quantum state $|\psi_{db}\rangle$ and store it for subsequent interrogation. Suppose at a later time, we select (or are provided with) a random telephone number t^*, and desire to find the associated corresponding name x^*. We can then construct the phase kickback, *telephone number* tagging operator $U_f^{t^* y}$ utilizing the known information of the selected telephone number t^*. For example, if t^*=2, the operator $U_f^{t^* y}$ would have the form given in Fig.1 (with x now replaced by t^*). Note that $U_{f_{t^*}}^{ty}$ acts on the ty-subspace (indicated by the superscript) of telephone numbers t and the auxiliary qubit y, and *not* on the x-subspace of names, on which we are seeking the associated name x^*. Thus, in the full $2N^2$-dimensional Hilbert space of $\boldsymbol{H}_x^{(N)} \otimes \boldsymbol{H}_t^{(N)} \otimes \boldsymbol{H}_y^{(1)}$ (where the superscript denotes the dimension of the Hilbert space) the *telephone number* tagging operator has the following form, and operational PK effect

$$U_{f_{t^*}}^{xty} = I_N^x \otimes U_{f_{t^*}}^{ty} \qquad \text{where} \qquad f_{t^*}(t) = \delta_{t,t^*} = \begin{cases} 1 & t = t^* \\ 0 & t \neq t^* \end{cases},$$

$$I_N^x \otimes U_{f_{t^*}}^{ty}|x\rangle_x \otimes |t\rangle_t \otimes \left(\frac{|0\rangle_y - |1\rangle_y}{\sqrt{2}}\right) = |x\rangle_x \otimes \left\{(-1)^{f_{t^*}(t)}|t\rangle_t \otimes \left(\frac{|0\rangle_y - |1\rangle_y}{\sqrt{2}}\right)\right\} = (-1)^{f_{t^*}(t)}|x\rangle_x \otimes |t\rangle_t \otimes \left(\frac{|0\rangle_y - |1\rangle_y}{\sqrt{2}}\right). \tag{24}$$

Note that $U_{f_t^*}^{t,y}$ performs an effective sign flip on states $|x\rangle_x \otimes |t^*\rangle_t$ for *all* values of x. Due to the tensor product nature of the component states, a PK sign flip on $|t^*\rangle_t$ produces an effective PK sign flip on $|x\rangle_x \otimes |t^*\rangle_t$, which includes the sought after state $|x^*\rangle_x \otimes |t^*\rangle_t$. We now proceed to construct the Grover iteration in this approach.

4.3 Encoding the database into the quantum database state

From (20) we need to construct a unitary operator $A \equiv A^{xt}$ such that $A|0\rangle_x \otimes |0\rangle_t \equiv A|0\rangle_{xt} = |\psi_{db}\rangle_{xt}$.

$$A|0\rangle_x \otimes |0\rangle_t \equiv A|0\rangle_{xt} = |\psi_{db}\rangle_{xt}. \tag{25}$$

This is most easily accomplished if we perform a *relabeling* of the indices of the *xt* component states in the lower, rightmost line of (23) so that we bring them to the first N entries of the N^2 database vector, i.e. $|\psi_{db}\rangle = 1/\sqrt{4}\left(|2\rangle_{xt} + |7\rangle_{xt} + |8\rangle_{xt} + |13\rangle_{xt}\right) \rightarrow \quad 1/\sqrt{4}\left(|0'\rangle_{xt} + |1'\rangle_{xt} + |2'\rangle_{xt} + |3'\rangle_{xt}\right) \equiv |\psi'_{db}\rangle$, which we will call the *prime frame*, which we denote by primes on the component values. In the prime frame, the database state has the form $|\psi'_{db}\rangle = 1/\sqrt{4}\,[1,1,1,1,0,\ldots,0]^T$ and we seek a unitary operator A' with the property that $A'|0'\rangle_{xt} = |\psi'_{db}\rangle_{xt}$. Though there is much freedom in choosing such an A', the simplest, most direct (though non-unique) choice that we adopt here, is to choose $A' = H_N \equiv H^{\otimes n}$, the n-fold tensor product of 2x2 single quibt Hadamard unitaries. In the prime frame A' takes the block diagonal direct sum form,

$$A' = H_N \oplus I_{N^2-N}, \tag{26}$$

(see Fig. 2), in which I_{N^2-N} is the (N^2-N) x (N^2-N) identity matrix acting on those states $|i\rangle_x \otimes |j\rangle_t$ not in $|\psi'_{db}\rangle_{xt}$.

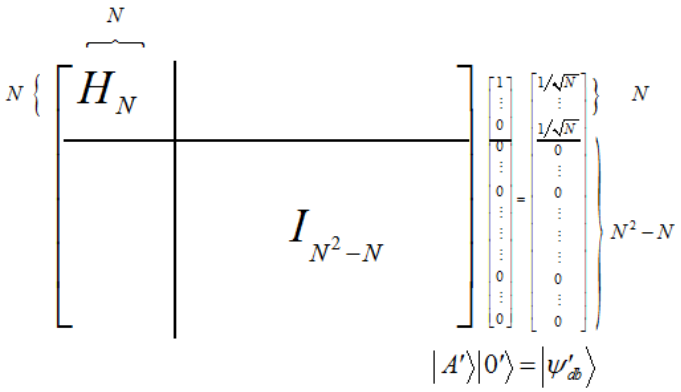


Fig.2 Form of the unitary A' operator, effecting the operation $A'|0'\rangle_{xt} = |\psi'_{db}\rangle_{xt}$, in the *prime index ordering* for which the N^2-dimensional primed database vector $|\psi'_{db}\rangle_{xt}$ has equally weighted values in the first N components. H_N is the n-fold tensor product single quibt 2x2 Hadamard unitaries. I_{N^2-N} is the (N^2-N) x (N^2-N) identity matrix operating on those states $|i\rangle_x \otimes |j\rangle_t$ not in $|\psi'_{db}\rangle_{xt}$. A' has the block-diagonal direct sum form $A' = H_N \oplus I_{N^2-N}$.

We can transform A' back to the original unprimed frame by a series of N^2 x N^2 unitary operations $S_{i,j} \equiv S_{i,j}^{xt}$ that swaps rows i and j of any matrix. In our particular example (23) where $|\psi_{db}\rangle = 1/\sqrt{4}\left(|2\rangle_{xt} + |7\rangle_{xt} + |8\rangle_{xt} + |13\rangle_{xt}\right)$ we have

$$\begin{aligned}
&|\psi_{db}\rangle = \frac{1}{\sqrt{4}}\left(|2\rangle_{xt} + |7\rangle_{xt} + |8\rangle_{xt} + |13\rangle_{xt}\right) \equiv \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|k_i\rangle_{xt}; \quad \{k_0,k_1,k_2,k_3\} = \{2,7,8,13\} \\
&|\psi'_{db}\rangle = \frac{1}{\sqrt{4}}\left(|0'\rangle_{xt} + |1'\rangle_{xt} + |2'\rangle_{xt} + |3'\rangle_{xt}\right) \equiv \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i'\rangle_{xt}, \\
&\Rightarrow A = \prod_{i=0}^{N-1} S_{i',k_i} A' = S_{0',2} S_{1',7} S_{2',8} S_{3',13} A', \qquad \left(S_{i,j}\right)_{k,l} = \begin{cases} 1 & (k,l) \in \{(i,j),(j,i)\} \\ 0 & \text{otherwise} \end{cases}
\end{aligned} \tag{27}$$

which is illustrated in Fig. 3. The swap operators $S_{i,j}$ acting on a quantum state vector effectively performs a Pauli bit-flip operation X_2 between the ith and jth components, and therefore, acting on a matrix, $S_{i,j}$ swaps the ith and jth rows. Note that we perform the row swaps from the prime to the unprimed frame beginning with the largest value of $i' = N$, backwards to smallest value $i' = 0$.

4.4 Construction of the Grover iteration

The construction of the Grover iteration is most clearly described in the prime frame. However, in the numerical examples discussed below, the simulations are carried out in the unprimed frame. As a (common) slight abuse of notation, we will drop the explicit labeling of the auxiliary y qubit (leaving it implied) that is necessary to perform the PK operation in the telephone number subspace. We will denote this unitary operator simply as $U^t_{f_t^*}$ enacting the effective conditional sign flip $U^t_{f_t^*}|t\rangle_t = (-1)^{f_t^*(t)}|t\rangle_t$ analogous to (4). We shall further write the full

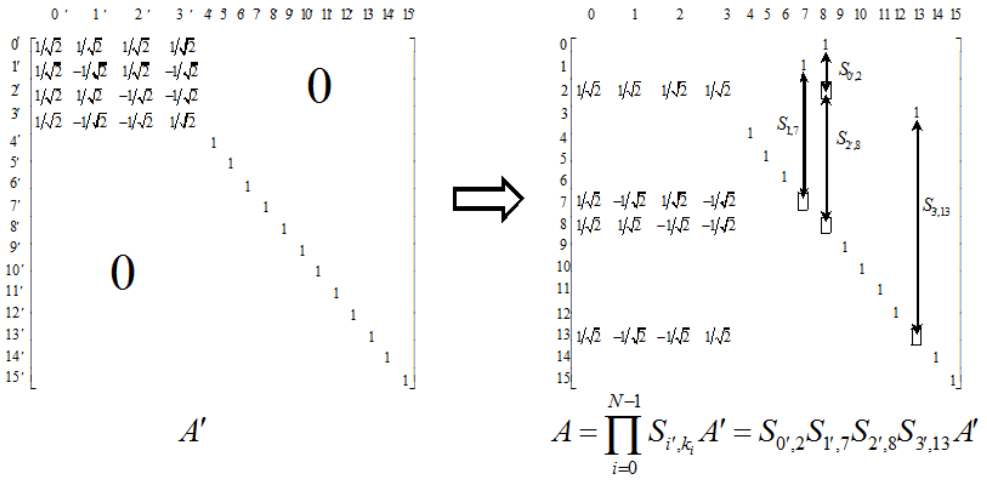


Fig.3: Successive row swapping operations to transform A' in the prime frame to A in the unprimed frame for the specific telephone database example in (27).

N^2 x N^2 operator in (24) acting on xt vectors as $U^{xt}_{f_t^*} = I^x_N \otimes U^t_{f_t^*}$. This matrix is block-diagonal in form, which each block consisting of the N x N sub-matrix telephone number tagging operator $U^t_{f_t^*}$. Formally $U^{xt}_{f_t^*}$ takes the form

$$U^{xt}_{f_t^*} = I^x_N \otimes U^t_{f_t^*} = \bigoplus_{i=0}^{N-1} U^t_{f_t^*} = \underbrace{U^t_{f_t^*} \oplus \cdots \oplus U^t_{f_t^*}}_{N}, \tag{28}$$

which is the tensor product of the N x N matrix $U^t_{f_t^*}$ acting in the N-dimensional t-subspace, for a given value of x (for which there N possibilities), with the identity matrix I^x_N in the x-subspace. The direct product form of (28), and presence of I^x_N in the x-subspace indicates that $U^t_{f_t^*}$ transforms $|x\rangle_x \otimes |t^*\rangle_t \mapsto -|x\rangle_x \otimes |t^*\rangle_t$ (leaving all other states unchanged), unbiasedly for *all* value of x, not just for the sought for value x=x^*.

Turning to the N^2 x N^2 inversion about the mean (IAM) operator $U^{xt}_{\psi^\perp}$ we note that both the states $|0'\rangle_{xt}$ and $|0\rangle_{xt}$ in the prime and unprimed frame, respectively, take the form of the vector $[1,0,\ldots,0]^T$. Therefore, the operator $U'^{xt}_{0^\perp}$ has the analogous operational effect as in (7)

$$
\begin{aligned}
U'^{xt}_{0^\perp} &= |0'\rangle_{xt\ xt}\langle 0'| - |1'\rangle_{xt\ xt}\langle 1'| - \ldots - |N'-1'\rangle_{xt\ xt}\langle N'-1'| = 2|0'\rangle_{xt\ xt}\langle 0'| - I_{N^2}, \\
U'^{xt}_{0^\perp}|0'\rangle_{xt} &= |0'\rangle_{xt}, \\
U'^{xt}_{0^\perp}|k'\neq 0'\rangle_{xt} &= -|k'\neq 0'\rangle_{xt},
\end{aligned}
\tag{29}
$$

where use has been made of the completeness relation $I_{N^2} = \sum_{k=0}^{N-1} |k\rangle_{xt\ xt}\langle k|$, with I_{N^2} the N^2xN^2 unit matrix. Further, in the unprimed frame $U^{xt}_{0^\perp}$ has the exact same form as $U'^{xt}_{0^\perp}$ without the primes. In both the primed and unprimed frame we can construct $U'^{xt}_{0^\perp}$ or $U^{xt}_{0^\perp}$ independent of knowledge of t^* and x^*.

Using the fact that $A'|0'\rangle_{xt} = |\psi'_{db}\rangle_{xt}$ yields

$$
\begin{aligned}
U'^{xt}_{\psi^\perp} &= 2|\psi'_{db}\rangle_{xt\ xt}\langle\psi'_{db}| - I_{N^2}, \\
&\equiv \left(2|\psi'_{db}\rangle_{xt\ xt}\langle\psi'_{db}| - I_N\right) \oplus \left(-I_{N^2-N}\right), . \\
&= U'^{(N)}_{\psi^\perp} \oplus \underbrace{\left((-I_N)\oplus\ldots\oplus(-I_N)\right)}_{N-1}.
\end{aligned}
\tag{30}
$$

It is important to note that $|\psi'_{db}\rangle_{xt\ xt}\langle\psi'_{db}|$ is the averaging operator (see the discussion following (8)) *only* on the first N components of a primed quantum state vector, with the effect of averaging only the components of the database state. Even in the unprimed frame where the N components of $|\psi_{db}\rangle_{xt}$ are spread out over the N^2 possible positions, $|\psi_{db}\rangle_{xt\ xt}\langle\psi_{db}|$ still performs an average only on the N components of $|\psi_{db}\rangle_{xt}$. Thus the N x N matrix $U'^{(N)}_{\psi^\perp} \equiv 2|\psi'_{db}\rangle_{xt\ xt}\langle\psi'_{db}| - I_N$ performs an inversion about the mean operation on the first N components of an N^2 component primed xt quantum state vector. (The superscript on $U'^{(N)}_{\psi^\perp}$ denotes the dimension of the subspace on which it acts). The full Grover iteration (19) is then given by

$$
\begin{aligned}
G^{xt} &= U^{xt}_{\psi^\perp} U^{xt}_{f^{t^*}}, \\
&= A^{xt} U^{xt}_{0^\perp} A^{xt\dagger} U^{xt}_{f^{t^*}}, \\
&= \left(2|\psi_{db}\rangle_{xt\ xt}\langle\psi_{db}| - I_{N^2}\right)\left(I^x_N \otimes U^t_{f^{t^*}}\right),
\end{aligned}
\tag{31}
$$

which we illustrate in Fig. 4 in the prime frame (for clarity) acting on $|\psi'_{db}\rangle_{xt}$.

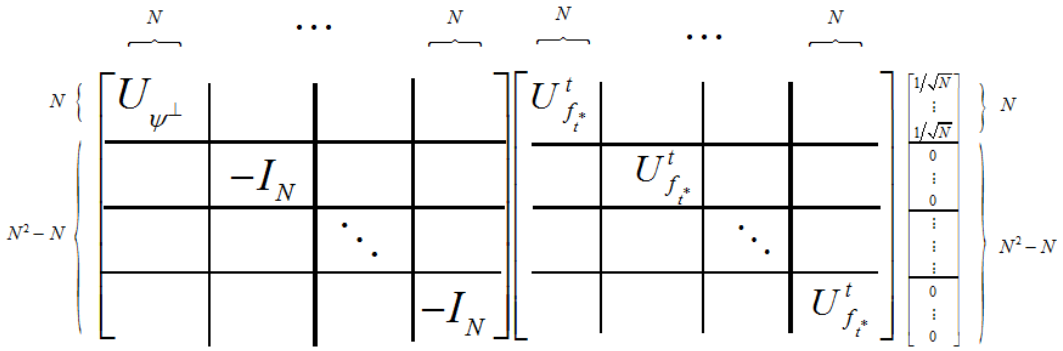


Fig.4: Illustration of the action $G'^{xt} = U'^{xt}_{\psi^\perp} U'^{xt}_{f^{t^*}} = \left(2|\psi_{db}\rangle_{xt\ xt}\langle\psi_{db}| - I_{N^2}\right)\left(I^x_N \otimes U^t_{f^{t^*}}\right)$, the Grover iteration (31) in the primed frame, acting on the $|\psi'_{db}\rangle_{xt}$, the primed database state. Note that in each NxN

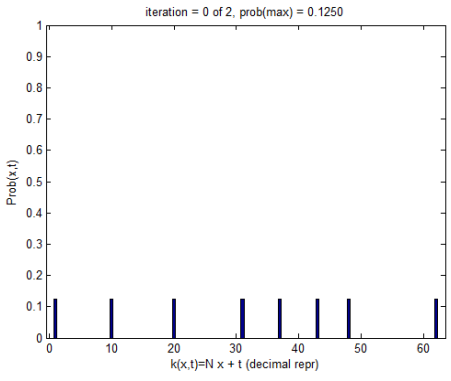
block $U^{t}_{f^{t^*}}$ performs a sign flip $U^{t}_{f^{t^*}}\left|t\right\rangle_t = (-1)^{f^{t^*}(t)}\left|t\right\rangle_t$ conditioned on the selected telephone number t^*, independent of the value of x. The operator $U'^{(N)}_{\psi^\perp} \equiv 2\left|\psi'_{db}\right\rangle_{xt\ xt}\left\langle\psi'_{db}\right| - I_N$ (where we have suppressed the subscripts in the figure) performs an inversion about the mean on the N components of $\left|\psi'_{db}\right\rangle_{xt}$.

The net effect of (31) is that on the first N components of the primed database state $\left|\psi'_{db}\right\rangle_{xt}$, we affect a Grover iteration of the original form in (2). On the later N^2-N components of $\left|\psi'_{db}\right\rangle_{xt}$ we perform the operation $\left|x \neq x^*\right\rangle_x \otimes \left|t^*\right\rangle_t \mapsto -\left|x \neq x^*\right\rangle_x \otimes \left|t^*\right\rangle_t$ in each N x N block, followed by the multiplication by the N x N identity matrix I_N. However, since the latter N^2-N components of $\left|\psi'_{db}\right\rangle_{xt}$ are initially zero (which we will generalize below), they remain zero after the Grover iteration. Thus, after $k \sim \left\lfloor \pi\sqrt{N}/4 \right\rfloor$ Grover iterations, the amplitude of the state $\left|x^*\right\rangle_x \otimes \left|t^*\right\rangle_t$ lying somewhere in the first N (of the N^2) components of $\left|\psi'_{db}\right\rangle_{xt}$ the will be driven to a magnitude $\sqrt{N-1}/\sqrt{N} \sim O(1)$ (see the discussion following (14)) with probability $O(1-1/N)$ for detection upon measurement.

4.5 Numerical simulations of algorithm

In Fig. 5 we show a simulation for the case of n=3 qubits where a pair of arrays of names and telephones of size N=2^n=8 are chosen as random permutations of [0,1,…,N-1]. In the code, the database state $\left|\psi_{db}\right\rangle_{xt} = 1/\sqrt{N}\sum_{k=0}^{N-1}\left|k\right\rangle_{xt}$ is constructed in the unprimed frame, and from the specific collection of N indices $\{k\}_{\text{db}}$ in the database state, we construct A in (27) from A', as discussed in (26) and illustrated in Fig. 3. This allows us to construct $U^{xt}_{\psi^\perp}$. We next generate a random telephone number t^* and use it to construct the specific PK telephone tagging operator $U^{xt}_{f^{t^*}}$. Subsequently, we assemble the Grover iteration $G^{xt} = U^{xt}_{\psi^\perp}\, U^{xt}_{f^{t^*}}$ and apply it for $\left\lfloor \pi\sqrt{N}/4 \right\rfloor = 2$. In Fig. 5 note that only N=8 of the total N^2=64 probabilities are non-zero throughout the whole evolution, corresponding to the N=8 non-zero amplitudes of the database state $\left|\psi_{db}\right\rangle_{xt}$.

name: x	telephone # t
3	7
4	5
5	3
0	1
$x^*=1$ ←	$t^*=2$
6	0
7	6
2	4



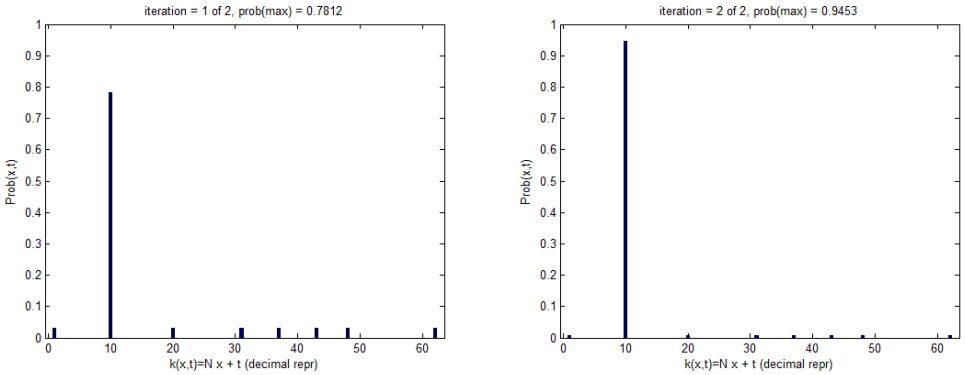


Fig.5: Grover iterations (31) for n=3 qubits (N=2^3=8) with a randomly selected telephone number t^*=2. The plots (left to right) show the probabilities (amplitude squared) for the $\{0,1,\lfloor \pi\sqrt{N}/4 \rfloor = 2\}$ iterations. The abscissa is the combined xt index k=Nx+t ranging from 0 to N^2-1=63. The Grover iterations acts on the $|\psi_{db}\rangle_{xt}$ and drives it towards the state $|k^* = 10\rangle = |x^* = 1\rangle_x \otimes |t^* = 2\rangle_t$ with near unit probability. Note that only N=8 of the total N^2=64 probabilities are non-zero throughout the whole evolution, corresponding to the N=8 non-zero amplitudes of the database state $|\psi_{db}\rangle_{xt}$.

5. CONSIDERATIONS AND EXTENSIONS

5.1 Initial state

It is illuminating to consider the action of our Grover iteration G^{xt} on initial states $|\psi_{init}\rangle_{xt}$ other than the constructed database state $|\psi_{db}\rangle_{xt}$. In general, the normalized initial state could be written in the form

$$|\psi_{init}\rangle_{xt} = \sqrt{p}\,|\psi_{db}\rangle_{xt} + \sqrt{1-p}\,|\psi_{ndb}\rangle_{xt}, \tag{32}$$

where $|\psi_{ndb}\rangle_{xt}$ denotes a normalized non-database state, i.e. the state formed by all components *not* in the database state $|\psi_{db}\rangle_{xt}$. In (32), $p = |\langle\psi_{db}|\psi_{init}\rangle|^2$ is the probability to find the initial state in the database state. After the $\lfloor \pi\sqrt{N}/4 \rfloor$ of G^{xt} the final state is approximately

$$|\psi_{final}\rangle_{xt} \sim \sqrt{p}\,|x^*\rangle_x |t^*\rangle_t + \sqrt{1-p}\,|\psi_{ndb}\rangle_{xt}, \tag{33}$$

which implies there is only a probability p to detect the sought after solution state $|x^*\rangle_x |t^*\rangle_t$. Thus, as long as p≥1/2, the form the GSA presented here does better than its classical $O(N/2)$ exhaustive search.

The initial state (32) might occur as an imperfect attempt to construct the desired database state $|\psi_{db}\rangle_{xt}$. A simpler state to form, is the N^2 equal amplitude state $|\psi_{N^2}\rangle_{xt} \equiv 1/\sqrt{N^2}\sum_{k=0}^{N^2-1}|k\rangle_{xt} = H_x^{\otimes n} \otimes H_t^{\otimes n}|0\rangle_x \otimes |0\rangle_t$ since the last equality shows that we can form this state directly by the application of 2n-fold tensor product of Hadamards $H_x^{\otimes n} \otimes H_t^{\otimes n}$ acting on the tensor product of the n-qubit standard name-state $|0\rangle_x$ and the n-qubit standard telephone-state $|0\rangle_t$. However, from (32) and (33) such an initial state renders the GSA worse than classical exhaustive search since there are N^2-N non-database states each with probability $1/\sqrt{N^2}$ that are unchanged by the Grover iteration G^{xt} for a total probability for the detection of $|\psi_{ndb}\rangle_{xt}$ upon measurement given by 1-1/N. The initial probability of p=1/N to find $|\psi_{N^2}\rangle_{xt}$ in the

state $|\psi_{db}\rangle_{xt}$ remains the final probability to find $|\psi_{final}\rangle_{xt}$ in the solution state $|x^*\rangle_x|t^*\rangle_t$. Figure 6 illustrates though that G^{xt} the does act only on the N-component state $|\psi_{db}\rangle_{xt}$ buried within N^2 sized initial state $|\psi_{N^2}\rangle_{xt}$.

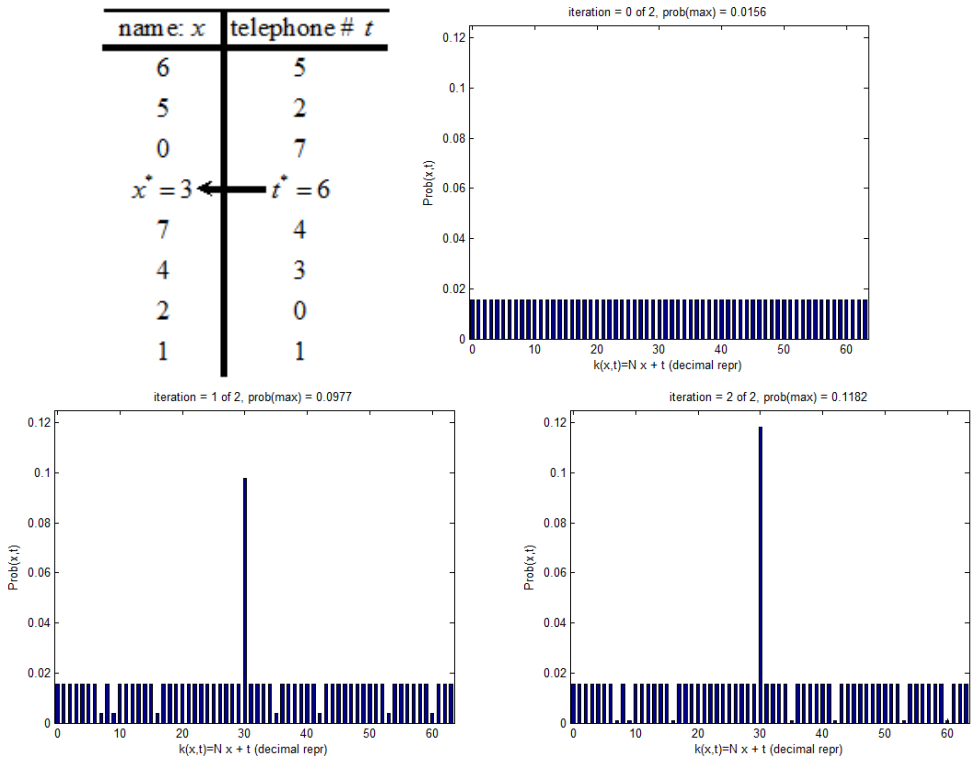


Fig.6: Grover iteration (31) for n=3 qubits (N=2^3=8) with a randomly selected telephone number t^*=6 with initial state $|\psi_{init}\rangle = |\psi_{N^2}\rangle_{xt} \equiv 1/\sqrt{N^2}\sum_{k=0}^{N^2-1}|k\rangle_{xt}$. The plots (left to right) show the probabilities (amplitude squared) for the $\{0,1,\lfloor \pi\sqrt{N}/4 \rfloor = 2\}$ iterations. The abscissa is the combined xt index k=Nx+t ranging from 0 to N^2-1=63. The Grover iterations acts upon the $|\psi_{db}\rangle_{xt}$ portion of $|\psi_{init}\rangle_{xt} = \sqrt{p}\,|\psi_{db}\rangle_{xt} + \sqrt{1-p}\,|\psi_{ndb}\rangle_{xt}$ where $p = 1/\sqrt{N^2} = 1/N$, and drives it towards the state $|k^* = 30\rangle = |x^* = 3\rangle_x \otimes |t^* = 6\rangle_t$ with probability p=1/8. Note that all N^2=64 probabilities are non-zero throughout the whole evolution, but only the N=8 amplitudes of the database state $|\psi_{db}\rangle_{xt}$ are acted upon by G^{xt} (compare with Fig. 5). Because the amplitudes in $|\psi_{ndb}\rangle_{xt}$ are unchanged by G^{xt} using the initial state, $|\psi_{init}\rangle = |\psi_{N^2}\rangle_{xt}$ yields inferior performance when compared to classical exhaustive search.

5.2 Sequential vs concurrent searches with a generalized database state

Since the essence of the above variation of the GSA is to implement the Grover iterations in an N-dimensional subspace of a larger N^2 dimensional Hilbert space (of xt-states) it is natural to inquire if multiple independent Grover search could be executed in M<N independent subspaces concurrently. The answer is unfortunately no, for a reason illuminated by the form the our current algorithm. Consider $|\Psi_{DB}\rangle = 1/\sqrt{M}\sum_{m=0}^{M-1}|\psi_{db}^{(m)}\rangle_{xt} = 1/\sqrt{M\,N}\sum_{m=0}^{M-1}\sum_{i=0}^{N-1}|x_i^{(m)}\rangle_x \otimes |t_i^{(m)}\rangle_t$ an M database state encoded containing $MN < N^2$ elements. We assume that a given pair $(x_i^{(m)}, t_i^{(m)})$, the state $|x_i^{(m)}\rangle_x \otimes |t_i^{(m)}\rangle_t$ appears in one and only one database state $|\psi_{db}^{(m)}\rangle_{xt}$. The crucial operation is the t-subspace PK operation $U_{f_{t^*}}^{xt}$ (28),

which is applied independent of the *x*-subspace $U^{xt}_{f^*_t} = I^x_N \otimes U^t_{f^*_t} = \bigotimes_{i=0}^{N-1} U^t_{f^*_t} = \underbrace{U^t_{f^*_t} \otimes \cdots \otimes U^t_{f^*_t}}_{N}$. Suppose M=2, and we attempted to apply two simultaneous NxN PK operations $U^t_{f^*_{t_1}}$ and $U^t_{f^*_{t_2}}$ given two separate telephone numbers (t^*_1, t^*_2) for two different database states $\left|\psi^{(1)}_{db}\right\rangle_{xt}$ and $\left|\psi^{(2)}_{db}\right\rangle_{xt}$. This would imply that we would have to implement an operator of the form $U^{xt}_{f^*_{t_1} f^*_{t_2}} = \underbrace{U^t_{f^*_{t_1}}}_{N} \oplus \underbrace{U^t_{f^*_{t_2}}}_{N} \oplus \underbrace{U_{N^2-2N}}_{N^2-2N}$ (where in the prime frame, $U^t_{f^*_{t_1}}$ acts on the first N components of $\left|\Psi_{DB}\right\rangle$ consisting of $\left|\psi^{(1)}_{db}\right\rangle_{xt}$, $U^t_{f^*_{t_2}}$ acts on the second N components of $\left|\Psi_{DB}\right\rangle$ consisting of $\left|\psi^{(2)}_{db}\right\rangle_{xt}$ and U_{N^2-2N} is some arbitrary unitary operator acting on the remaining zero valued N^2-N components of $\left|\Psi_{DB}\right\rangle$). However, the construction of such a PK operation requires some specific knowledge of the *x*-subspace (i.e. about location of sought for solutions $\{x^*_1, x^*_2\}$), and therefore would not of the *x*-egalitarian tensor product form $I^x_N \otimes U^t_{f^*_{t_1} f^*_{t_2}}$, where now $U^t_{f^*_{t_1} f^*_{t_2}}$ acts solely in the *t*-subspace, independent of the values of *x*.

The best approach is to apply $I^x_N \otimes U^t_{f^*_{t_1}}$ and its appropriate averaging operator $U^{xt}_{\psi^\perp_1} = \left(2\left|\psi^{(1)}_{db}\right\rangle_{xt\ xt}\left\langle\psi^{(1)}_{db}\right| - I_{N^2}\right)$ until we converge $\left|\psi^{(1)}_{db}\right\rangle_{xt}$ to the solution $\left|x^*_1\right\rangle_x \otimes \left|t^*_1\right\rangle_t$, and then repeat the process applying $I^x_N \otimes U^t_{f^*_{t_2}}$ and its appropriate averaging operator $U^{xt}_{\psi^\perp_2} = \left(2\left|\psi^{(2)}_{db}\right\rangle_{xt\ xt}\left\langle\psi^{(2)}_{db}\right| - I_{N^2}\right)$ until we converge $\left|\psi^{(2)}_{db}\right\rangle_{xt}$ to the solution $\left|x^*_2\right\rangle_x \otimes \left|t^*_2\right\rangle_t$. The case of M=2 is illustrated in Fig. 7, in the prime frame, where $\left|\psi^{(1)}_{db}\right\rangle_{xt}$ occupies

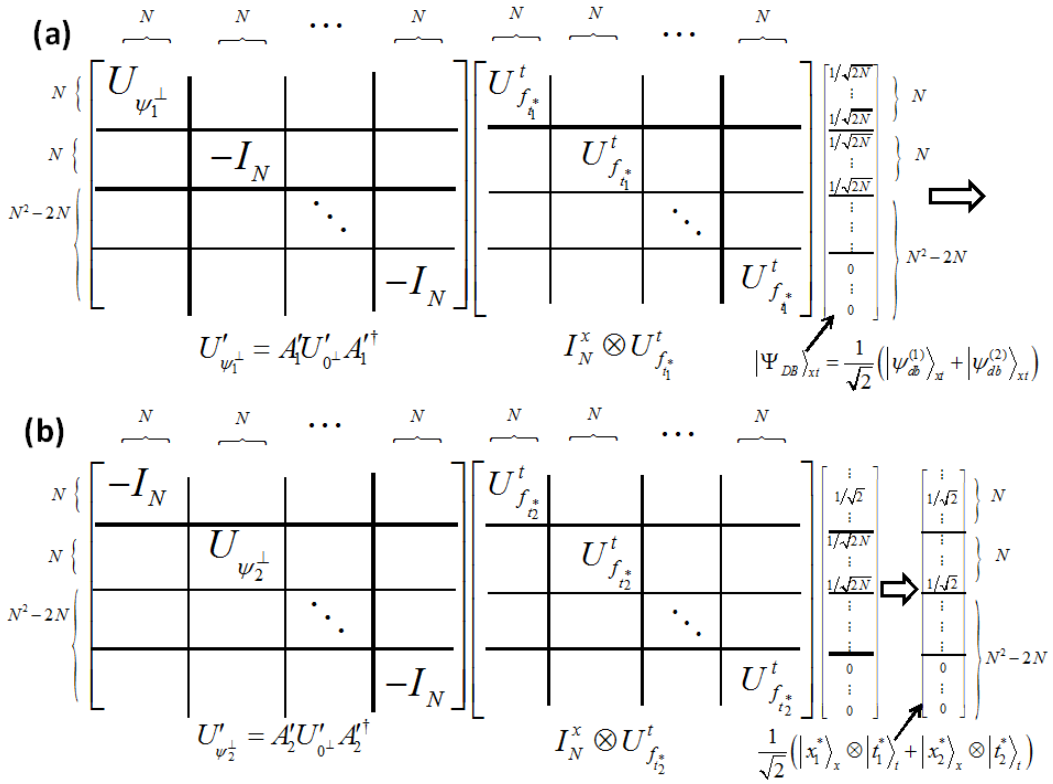


Fig.7: Illustration of the sequential GSA in M=2 separate N-dimensional subspaces, illustrated in the prime frame. The two N-dimensional subspaces $\left|\psi^{(1)}_{db}\right\rangle_{xt}$ and $\left|\psi^{(2)}_{db}\right\rangle_{xt}$ occupy the first and second set of N components of the

joint database state $|\Psi_{DB}\rangle = \left(|\psi_{db}^{(1)}\rangle_{xt} + |\psi_{db}^{(2)}\rangle_{xt}\right)/\sqrt{2}$. (a) Given two telephone number (t_1^*, t_2^*) for the two databases $|\psi_{db}^{(1)}\rangle_{xt}$ and $|\psi_{db}^{(2)}\rangle_{xt}$, the operations $U_{f_{t_1^*}}^{xt} = I_N^x \otimes U_{f_{t_1^*}}^t$ and $U_{\psi_1^\perp}^{xt} = \left(2|\psi_{db}^{(1)}\rangle_{xt\ xt}\langle\psi_{db}^{(1)}| - I_{N^2}\right)$ (the same in Fig. 4) drive $|\Psi_{DB}\rangle \to \left(|x_1^*\rangle_x \otimes |t_1^*\rangle_t + |\psi_{db}^{(2)}\rangle_{xt}\right)/\sqrt{2}$. (b) Subsequently, constructing $U_{f_{t_2^*}}^{xt} = I_N^x \otimes U_{f_{t_2^*}}^t$ and using $U_{\psi_2^\perp}^{xt} = \left(2|\psi_{db}^{(2)}\rangle_{xt\ xt}\langle\psi_{db}^{(2)}| - I_{N^2}\right)$ drives the solution to $|\Psi_{DB}\rangle \to \left(|x_1^*\rangle_x \otimes |t_1^*\rangle_t + |x_2^*\rangle_x \otimes |t_2^*\rangle\right)/\sqrt{2}$.

components 0 to *N*-1 of $|\Psi_{DB}\rangle$, and $|\psi_{db}^{(2)}\rangle_{xt}$ occupies components *N* through 2*N*-1. Since both $|\psi_{db}^{(1)}\rangle_{xt}$ and $|\psi_{db}^{(2)}\rangle_{xt}$ have been encoded sometime in the past into separate N-dimensional subspaces, we know operators A_1' and A_2' that encode $|\psi_{db}^{(1)}\rangle_{xt}$ into the first *N* components of $|\Psi_{DB}\rangle$ in the prime frame, and encode $|\psi_{db}^{(2)}\rangle_{xt}$ into the second *N* components. Hence we know how to construct the averaging operators $U_{\psi_1^\perp}^{xt} = A_1' U_{0^\perp}' A_1'^\dagger$ and $U_{\psi_2^\perp}^{xt} = A_2' U_{0^\perp}' A_2'^\dagger$ that act on the first and second set of *N* components respectively in $|\Psi_{DB}\rangle$. The net effect of the sequential GSA as illustrated in Fig. 7 is to drive $|\Psi_{DB}\rangle$ to the joint solution $|\Psi_{final}\rangle = \left(|x_1^*\rangle_x \otimes |t_1^*\rangle_t + |x_2^*\rangle_x \otimes |t_2^*\rangle\right)/\sqrt{2}$, with probability 1/*M* to measure a specific solution $|x_m^*\rangle_x \otimes |t_m^*\rangle_t$, m∈{1,2}. Statistically, this is equivalent to performing two separate GSA on two separate database states $|\psi_{db}^{(1)}\rangle_{xt}$ and $|\psi_{db}^{(2)}\rangle_{xt}$ as originally discussed in Section 4.4 above and illustrated in Fig. 4. The only advantage of performing sequential GSA as illustrated in Fig. 7 is to continue using the original database state $|\Psi_{DB}\rangle$, without re-creating it for subsequent subspace searches.

5.3 Formation of the initial state

Once the telephone book database is given, the quantum database state is constructed via (25) from the unitary operator *A* and the standard initial state $|0\rangle_x \otimes |0\rangle_t \equiv |0\rangle_{xt}$ by $A|0\rangle_{xt} = |\psi_{db}\rangle_{xt}$. In this section we briefly show that the initial database state $|\psi_{db}\rangle = 1/\sqrt{N}\sum_{i=0}^{N-1}|x_i\rangle_x \otimes |t_i\rangle_t$ given in (21) can also be constructed in O(log N) = O(n) cascaded stages (using $N=2^n$ for simplicity), where parallel operations can be utilized at each stage This assertion rests on the following observation. Consider two arbitrary states $|\phi\rangle$ and $|\varphi\rangle$. Define the states $|\pm\rangle = (|\phi\rangle \pm |\varphi\rangle)/\sqrt{2}$ and the Hadamard operator defined on these two states as $H_{\phi,\varphi} = |+\rangle\langle\phi| + |-\rangle\langle\varphi|$ with the effect $H_{\phi,\varphi}|\phi\rangle = |+\rangle$ and $H_{\phi,\varphi}|\varphi\rangle = |-\rangle$. A simple calculation shows that $H_{\phi,\varphi}H_{\phi,\varphi}^\dagger = \left(|\phi\rangle\langle\phi| + |\varphi\rangle\langle\varphi|\right) + \langle\phi|\varphi\rangle|+\rangle\langle-| + \langle\varphi|\phi\rangle|-\rangle\langle+|$, which is the identity operator $I_{\phi,\varphi} = |\phi\rangle\langle\phi| + |\varphi\rangle\langle\varphi|$ on the subspace of these two states if and only if $|\phi\rangle$ and $|\varphi\rangle$ are orthogonal, i.e. $\langle\varphi|\phi\rangle = 0$. In other words, $H_{\phi,\varphi}$ takes the form of the usual Hadamard operator $\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$ if the rows and columns are labeled by the orthogonal states $|\phi\rangle$ and $|\varphi\rangle$. Since each of the component *x*-*t* states $|x_i\rangle_x \otimes |t_i\rangle_t$ in $|\psi_{db}\rangle$ are orthogonal (and known since we are initially encoding the telephone directory database), we can construct the necessary $H_{\phi,\varphi}$ to combine them pair wise in a logarithmic number of stages to successively construct $|\psi_{db}\rangle$. This is illustrated in Fig. 8 for the database state $|\psi_{db}\rangle = 1/\sqrt{4}\left(|0\rangle_x|2\rangle_t + |1\rangle_x|3\rangle_t + |2\rangle_x|0\rangle_t + |3\rangle_x|1\rangle_t\right)$ given in (23).

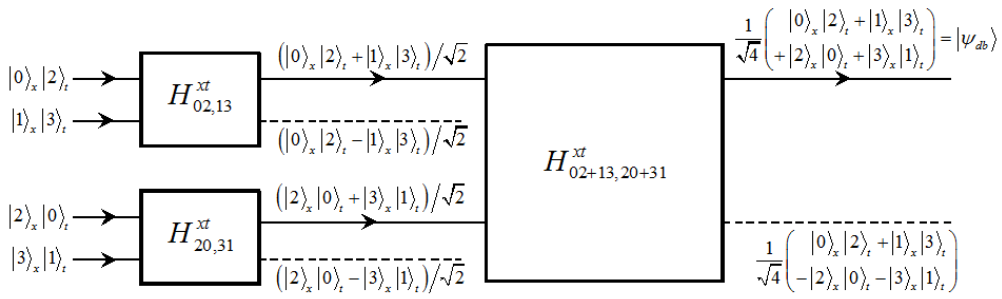


Fig.8: Construction of database state $|\psi_{db}\rangle=1/\sqrt{4}\left(|0\rangle_x|2\rangle_t+|1\rangle_x|3\rangle_t+|2\rangle_x|0\rangle_t+|3\rangle_x|1\rangle_t\right)$ by successive Hadamard-type operations on successive pairs of orthogonal states (see text) for the case of n=2 qubits, i.e. two $N=2^2=4$ dimensional subspaces to represent the name (x-states) and telephone number (t-states) subspaces respectively. For general, $N=2^n$ dimensional x- and t-subspaces, the first (leftmost) stage has $N/2$ gates H^{xt} acting on known (since one is encoding the telephone directory database) pairs of orthogonal input states $|i\rangle_x\otimes|j\rangle_t$ and $|i'\rangle_x\otimes|j'\rangle_t$ acting in parallel. At each subsequent stage (moving rightwards) half the number of Hadamard gates are constructed and used to form further superpositions of orthogonal input states, which successively constructs $|\psi_{db}\rangle$ after O(log N)=O(n) stages.

6. SUMMARY AND CONCLUSIONS

The focus of this paper was to illustrate a variant of Grover's algorithm for the case of a k=2 indexed database state of the form $|\psi_{db}\rangle_{xt}=1/\sqrt{N}\sum_{i=0}^{N-1}|x_i\rangle_x\otimes|t_i\rangle_t$. The rationale our approach was to avoid the requirement that the oracle, implementing the phase kickback operation, has to be supplied to the searcher of the database by an external agent (as in the original formulation of the GSA). Instead, our variant of the GSA was designed so that the searcher could initially encode the database state and subsequently search it at a later time, without having to know the sought-for result in order to construct the phase kickback operator.

The variant of the GSA discussed in this work can easily be extended to multi-indexed databases states of the form $|\psi_{db}\rangle_{xtsr\ldots}=1/\sqrt{N}\sum_{i=0}^{N-1}|x_i\rangle_x\otimes|t_i\rangle_t\otimes|s_i\rangle_s\otimes|r_i\rangle_r\cdots$. If this generalized database state is encoded in the past, then a later time a chosen subspace component (e.g. the t-subspace telephone number as illustrated in this paper) can be searched on through the construction of a phase kickback operation $U_f^t=I_N^x\otimes U_f^t\otimes I_N^s\otimes I_N^r\cdots$ on that subspace, implementing $f(t^*)=1$ and $f(t\neq t^*)=0$ for a given t^*, producing the result $U_f^t|x_i\rangle_x\otimes|t_i\rangle_t\otimes|s_i\rangle_s\otimes|r_i\rangle_r=|x_i\rangle_x\otimes(-|t_i\rangle_t)\otimes|s_i\rangle_s\otimes|r_i\rangle_r$. $=-|x_i\rangle_x\otimes|t_i\rangle_t\otimes|s_i\rangle_s\otimes|r_i\rangle_r$ For a k-component database state (i.e. k different index states $|x_i\rangle_x,|t_i\rangle_t,|s_i\rangle_s,|r_i\rangle_r,\ldots$), general amplitude amplification as given in (19) $G=U_{\psi^\perp}U_f=AU_{0^\perp}A^\dagger U_f$ can be used to perform an $O(\sqrt{N})$ Grover search algorithm in the N dimensional subspace of a general N^k dimensional Hilbert space. Again, A is the unitary operator that takes the standard state $|0\rangle_{xtsr\ldots}$ to the database state $|\psi\rangle_{xtsr\ldots}$. The utility of this approach depends upon the ease and efficiency of constructing the operator A. and hence the quantum database state $|\psi\rangle_{xtsr\ldots}$. Similar work along the lines of a quantum Grover search upon multi-index states has been considered by Pang *et al.*[8].

DISCLAIMER: Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of AFRL.

References

[1] Shor, P. "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 124-134 (1994).

[2] Grover, L.K., "Quantum mechanics helps in searching for a needle in a haystack," Phys. Rev. Lett. 79(2), 325-328 (1997).

[3] Kaye, P., Laflamme, R. and Mosca, M., [An Introduction to Quantum Computing], Oxford University Press, New York, 152-178 (2007).

[4] Yanofsky, N.S., and Mannucci, M.A., [Quantum Computing for Computer Scientists], Cambridge University Press, New York, 195-204 (2008).

[5] P. Walther, K.J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Apselmeyer and A. Zeilinger, "Experimental one-way quantum computing," Nature 434, 169-176 (2005); K.A. Brickman, P.C. Haljan, P.J. Lee, M. Acton, L. Deslauriers, and C. Monroe, "Implementation of Grover's quantum search algorithm in a scalable system," Phys. Rev. A. 72, 050306(R) (2005); Bhattacharya, N., van Linden van den Heuvell, H. B. & Spreeuw, R. J. C. "Implementation of quantum search algorithm using classical Fourier optics," Phys. Rev. Lett. 88, 137901 (2002).

[6] Boyer., Brassard, G., Hoyer, P. and Tapp, A., "Tight bounds on quantum searching," arXiv:quant-ph/9605034 (1996).

[7] Xu, N., Zhu, J., Peng, X., Zhou, X. and Du, J., "A non-oracle quantum search algorithm and its experimental implementation," arXiv:0809.0664 [quant-ph], (2008).

[8] Pang, C.Y., Zhou, Z.W. and Guo, G.C. "Quantum discrete cosine transformation for image compression," arXiv:quant-ph/0601043, (2006).