Algebraic, Geometric and Complexity Aspects of Quantum Search Algorithms

by
Christos Konstandakis

Submitted to the School of Electrical and Computer Engineering
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Electrical and Computer Engineering
at the
TECHNICAL UNIVERSITY OF CRETE
7th May 2018

Dedicated to
Angelina, Alexandra, Melina and Dimitris

Acknowledgements

It is both an honour and a pleasure to acknowledge my debt to my supervisor, Prof. Demosthenes Ellinas.

This thesis would not have been possible without his insight, encouragement, patience, friendship and generosity.

I am grateful to Dr. Peter Jarvis for his interest in my work and our fruitful discussions.

I gratefully acknowledge the scholarships received towards my PhD studies from Technical University of Crete.

Jury

3-member Commitee
Demosthenes Ellinas (Supervisor), Professor
Antonios Manoussakis, Associate Professor
Minos Petrakis, Associate Professor
Examiners
Dimitris Angelakis, Associate Professor
Minos Garofalakis, Professor
Mihalis Kolountzakis, Professor
Jiannis Pachos, Professor

Algebraic, Geometric and Complexity Aspects
of Quantum Search Algorithms

by
Christos Konstandakis
Submitted to the School of Electrical and Computer Engineering
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Electrical and Computer Engineering
at the
TECHNICAL UNIVERSITY OF CRETE

Abstract

Quantum search algorithm determines k marked items in an otherwise unstructured set (database), of size N by performing Order(SQRT(N/k)) trials. Hence a quadratic reduction of search complexity is achieved compared to Order(N/k) trials required by any classical algorithm. The quantum algorithm exploits successfully basic ingredients of Quantum Mechanics such as, linear superpositions and quantum entanglement of state vectors in multiple tensorial products of Hilbert spaces, unitary dynamics, projective measurements and the probabilistic interpretation of the outcomes. It stands as a landmark procedure and a computational primitive within the field of Quantum Information Algorithms. This Thesis undertakes research on the original quantum search scheme and proposes novel quantum algorithms that exceed existing search complexity limits. The work is organized along the algebraic, geometrical and complexity aspects characterizing the quantum search field.

Initially the so called oracle matrix algebra is introduced as a special SU(2) isomorphic algebra embedded in SU(N) algebra, determined by the oracle Boolean function that marks the target vectors in the database Hilbert space. Formulating search via oracle algebra reveals that Bloch's vector search trajectories are spherical geodesics, hence the complexity reduction has geometric origin. Within the same algebraic setting a toy model relaxation of the unitarity of the model leading to an open quantum system search algorithm is introduced. Searching is now carried out by a completely positive trace preserving map (CPTP), the investigation of which allows to address questions of complexity vs. accuracy trade off, and to provide answers summarized in the form of a new search strategy.

Utilizing oracle algebra's representation theory a novel scheme of collective quantum search is put forward. Many quantum searche(r)s can be joined in two modes: either by concatenation or by merging their Boolean functions and database Hilbert spaces. While concatenation complexity Tconc, leads to no improvements, merging quantum searches, say n of them, leads to complexity: Tconc=Order(SQRT(n)) Tmerg. Hence collective search speeds up

finding items by a factor quadratic in the number of searches participating. Between the all n merging to all n concatenating joining schemes all other possible interpolating joining schemes are investigated. They provide all intermediate values of complexity reductions, as is shown analytically by means of the theory of partitions, Young tableaux, and majorization theory.

Relying on unitary dilation theory of CP maps, it is next shown that the parametric quantum search algorithm introduced before admits a unitarization (unitary dilation) a la quantum walk (QW), at the expense of introducing auxiliary quantum coin-qubit spaces. QW, a proverbial model of quantum random walk with quadratic enhancement of the diffusion range in comparison to that of classical random walk, hence of similar to search quadratic complexity reduction, is shown to enable quantum search simulation. QW dynamics is generated by a Hamiltonian representing multiparticle long-range interacting qubits. The QW-Quantum Search construct is finally shown to give rise to a double lane quantum search algorithm.

Finally the Thesis addresses the fast counting problem: Counting the size of a set requires as many counts as set's cardinality, say N. Employing single item search algorithm of N dimensional database and the entanglement developed between any two parts of database space during search leads to fast counting. Demonstrating the periodic projectivity of reduced density matrix ensuing by decoupling fraction of qubits from database state and monitoring entanglement measures, being periodically vanishing with period Order(SQRT(N)), leads to quadratic speed up of counting. By rigging marked item initial probability a hyper-quadratic acceleration of counting is achieved.

Introduction

Contents

Background topics

The subject matter of this Thesis contains, elaborates and introduces concepts and methods belonging to various wider background topics of Quantum Information Science. What follows is a brief introduction to three such basic topics within which the problems of the Thesis are addressed. Specifically we deal with the topics: Quantum Algorithms and Quantum Search Algorithms, Quantum Walks and Quantum Entanglement.

Quantum Algorithms and Quantum Search Algorithms: Quantum Mechanics as a theoretical framework that holds some enhanced possibilities for computational processes has been suggested in the early 1980s, [1], [2]. The potential computational profits could be relied on two types of parallelism: the *quantum register parallelism* (n qubits can hold 2^n complex amplitudes), and the *quantum processing parallelism (e.g. a* 2 queries classical problem can by solved by a single query to a quantum black-box processor, [3]). Quantum state vector superpositions in a single Hilbert space distributed by non-local quantum gates to multiple Hilbert spaces in the form of *quantum entanglement* constitute a unique *quantum resource* which could be tapped to create computational advantages in classical algorithms. Quantum algorithms designate a new research area initiated about 30 years ago by quantum formulating classical query tasks and demonstrating polynomial [4],[5], as well as exponential [6], reductions of classical complexities. The culmination of this effort was a quantum algorithm that could achieved exponential speed up of the problem of factorization of integers [7], a notoriously exponentially hard classical problem. Since then quantum algorithms constitute a vibrant research field comprising by hundreds of algorithms [8],[9]-[14], that has become a pillar of Quantum Science and Technology.

The quantum search algorithm and its numerous other variations and generalizations form a special class of quantum algorithms with a polynomial

search complexity reduction wrt the classical rivals. Specifically the original Grover's algorithm seeks to determine k marked items in a unstructured database set of size N. The unitary search operator constructed to act on $\mathcal{H} \approx \mathbb{C}^N$ the database Hilbert space requires $\mathcal{O}(\sqrt{\frac{N}{k}})$ quires to the classical oracle i.e. it is quadratically faster than the classical algorithm that needs $\mathcal{O}(\frac{N}{k})$ queries.

Quantum Walks : Quantum walks (QW) [15, 16, 18, 17], are a quantum versions of random walk walks (CRW) with the additional task to outperform CRW in the spreading rates. Given the order $\mathcal{O}(\sqrt{N})$ of the diffusion range of a CRW achieved after N steps, one can show that the analogous QW spreads over a range of order $\mathcal{O}(N)$. Again a quadratic overhead of the figure of merit of the quantum version in comparison to the classical version of a task is achieved, similarly to the quantum search case. Further QW evolve by means of maps operating on the density matrix of a "walker system". Such maps are characterized as been completely positive and trace preserving (CPTP) maps [19], with special case the ones having commuting unitary generators. Unitary dilations of such CPTP maps are possible and non unique unitary versions of them, in extension of the original "walker" Hilbert space by auxiliary spaces, the "quantum coin" Hilbert space.

Quantum Entanglement: Within the standard formalism of Quantum Mechanics by means of *state vector spaces* and their *tensor products*, modelled by various types of Hilbert spaces and by means of *quantum observables* modelled by bounded linear operators acting on these spaces in various specific representations of them e.g. of matricial or of analytic type, the quantum entanglement shows up as a lack of decomposition of a tensor product state vector under the restriction of local-only action on it by various operators of interest. This local action restriction is both *physically imposed* and *operationally useful*. Quantifiers (e.g. [20]) measuring the entanglement developed between two or more particle states is a central topic in the field of quantum information algorithms. Such quantifiers are various functionals in the form of classical or quantum entropy function of the marginalized version of the total system density matrix/operator. Examples are the so called linear entropy, the von Neumann entropy and the quantum Renyi entropy [21]. Entanglement constitutes a form of quantum correlation developed between parts of a larger quantum system. Provided that the scientific consensus is considering it as a raison d' etre for various complexity reductions in computational algorithms, namely treating as a kind resource for achieving various tasks, measuring and monitoring entanglement is important aspect of algorithmic complexity.

References

[1] Y. Manin, *Classical computing, quantum computing, and Shor's factoring algorithm*, Seminaire Bourbaki, **41** (1998-1999), **862**, 375-404 (2000). The appendix translates an excerpt about quantum computing from a 1980 paper (in Russian).

[2] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982)

[3] D. Deutsch, Proc. R. Soc. London, Ser. A **400**, 97 (1985)

[4] D. Deutsch, D and R. Jozsa, Proc. R. Soc. London, Ser. A **439**, 553 (1992)

[5] E. Bernstein and U. Vazirani, ACM Symposium on Theory of Computing ACM, New York, pp. 11-20 (1993)

[6] D. R. Simon, SIAM J. Comput. **26**, 1474, (1997)

[7] P. W. Shor, SIAM J. Comput. **26**, 1484, (1997)

[8] Quantum Algorithm Zoo, https://math.nist.gov/quantum/zoo/

[9] A. Montanaro, *Quantum algorithms: an overview*, npj Quantum Information **2 ,**15023 (2016)

[10] A. Childs and W. van Dam, *Quantum algorithms for algebraic problems*, Rev. Mod. Phys. **82**, 1–52 (2010)

[11] D. Bacon and W. Dam, *Recent progress in quantum algorithms*, Commun. ACM **53**, 84–93 (2010).

[12] A. Bleicher, *Quantum Algorithms Struggle Against Old Foe: Clever Computers*, Quantam Magazine, https://www.quantamagazine.org/quantum-computers-struggle-against-classical-algorithms-20180201/

[13] M. Santha, *Quantum walk based search algorithms*, Theory Appl. Model. Comput. **4978**, 31-46 (2008)

[14] M. Mosca, *Computational Complexity* 2303–2333, (2012)

[15] J. Kempe, *Quantum random walks - an introductory overview*, Contemporary Physics. **44** (4), 307-327 (2003)

[16] A. Nayak and A. Vishwanath: *Quantum walk on a line.* DIMACS Technical Report No 2000-43 (2001)

[17] A. Ambainis, J. Kempe and A. Rivosh: *Coin make quantum walks faster*, In: Proceedings of 16th ACM-SIAM SODA, pp. 1099–1108 (2005).

[18] D. Aharonov, A. Ambainis, J. Kempe, U. Vazirani: *Quantum walks on graphs*. In: Proceedings of 33th STOC, pp. 50–59. ACM, New York (2001)

[19] K. Kraus, *States, Effects and Operations*, (Springer, Berlin 1983)

[20] G. Vidal and R. F. Werner, *Computable measure of entanglement*, Phys. Review A, **65**, 032314 (2004).

[21] K. Zyczkowski, I. Bengtsson, *Geometry of Quantum States: An Introduction to Quantum Entanglement*, (Cambridge Univ. Press, 2006).

Summary of Thesis' Articles

The Thesis includes the following papers five papers the content of which is analysed subsequently first thematically and and then individually for each one of them:

i) D. Ellinas and Ch. Konstandakis, *Matrix Algebra for Quantum Search Algorithm: Non Unitary Symmetries and Entanglement*, in Proceedings of 10th Conference Quantum Communication, Measurement and Computing (QCMC), Brisbane, Australia, 19-23 July 2010, Eds. T. Ralph, P. K. Lam. AIP Conf. Proc. 1363.

ii) D. Ellinas and Ch. Konstandakis, *Parametric Quantum Search Algorithm by CP maps: algebraic, geometric and complexity aspects*, Journal of Physics A: Mathematical & Theoretical, **46**, 415303-41530 (2013).

iii) D. Ellinas and Ch. Konstandakis, *Faster Together: Collective Quantum Search*, Entropy, **17**, 4838-4862 (2015).

iv) D. Ellinas and Ch. Konstandakis, *Parametric Quantum Search Algorithm as Quantum Walk: A Quantum Simulation*, Reports on Mathematical Physics **77** (1), 105-128 (2016).

v) D. Ellinas and Ch. Konstandakis, *Fast Counting Fuelled by Entanglement: Quantum Search new Harness*,
pp. 10, submitted for publication, 2018.

Algebraic, Geometric and Complexity Aspects: Results

According to its title this Thesis concerns research work on aspects of the theory of quantum search algorithms categorized as algebraic, geometric and complexity aspects. Subsequently the finding results of the Thesis are summarized per aspect category and cross reference to the respective papers of the Thesis are provided. Then a non technical analysis of the content of

each paper is provided, followed by a Technical Appendix where a number of technical summaries of some key topics of the articles are presented.

Algebraic aspects

• Algebraic reformulation of quantum search algorithm in terms of the so called *oracle algebra*, an $SU(2)$ isomorphic matrix algebra embedded in $SU(N)$, is introduced. (Paper I).

• Relaxation of unitarity of quantum search algorithm and a unitary preconditioning are introduced via CPTP maps. This preconditioning changes in effect the symmetry of the map from $SU(2)$ to $U(1) \oplus U(1)$. (Paper II).

• The problem of counting the number of elements of finite set S in the quantum setting is proposed, achieving counting in quadratically less counts than the cardinality of S, by employing Grover's algorithm reformulated in terms of A_f. Entropy-based and $SU(2)$-algebra-element based quantum measurements is shown to lead to evaluation of the period of entangelment variation. This period finding task provides operational ways to fast cardinality determination. (Paper V).

Geometric aspects

• The searching Bloch vector tracing the Bloch sphere is not rigid and is shown to have an axial sysmetry, the *azimuthal symmetry.* The search complexity reduction is shown to be byproduct of the fact that searching trajectories are *spherical geodesic* motions of the density's matrix vector on the Bloch sphere. In the open system parametric quantum search generalization the Bloch sphere is deformed to an *ellipsoid* in $\mathbb{R}^3$, and the parameter manifold of the invariant search density matrix is determined by a *cross curve cylinder* (Paper II).

• Characterizations are given for parametric search map via a *tetrahedron* spanned by a vector formed by the eigenvalues of the matrix implementing the affine transformation induced by the CP search map. (Paper II).

• The parametric quantum serach-QW relation when the QW in taken to be on a *complete graph,* is shown to lead a the double lane quantum search algorithm, a duplication of the original algorithm. (Paper IV).

Complexity aspects

• Quantum search with rigged marked item probability leads to *hyper-quadratic* acceleration and deceleration of complexity below classical value are achieved. (Paper V).

• Introduce novel collective models of quantum search by joining n independent searches by union domains of their Boolean oracle functions and sum of Hilbert spaces (*merging*), instead of acting separately (*concatenation*), then reduction of search complexity by factor $\mathcal{O}(\sqrt{n})$ is achieved

(Paper III). Joining schemes are described by Young diagrams tableaux of partitions and majorization theory.

• *Complexity versus accuracy* trade-off for the parametric search model and its robustness is revealed for sets of parameter values. That robustness enables the formulation of a novel search strategy, which determines the infima of database sizes over which the algorithm performs accurately. (Paper II).

Paper I

An algebraic reformulation of the quantum search algorithm associated to a k-valued oracle function, is introduced in terms of the so called *oracle matrix algebra* A_f, by means of which a Bloch sphere-like description of search is obtained. Motivated by the symmetry of search operator U_G being determined up a unitary $SU(2)$ matrix in A_f we turn the closed search system to an open quantum system driven by a CPTP map E_V, (for details c.f. Paper II). That extension formalizes the presence of quantum noise like effect. Next decomposing the total system state to two sub-systems with $n-2$ and 2 qubits respectively, we obtained the 2 qubit system reduced density matrix. Both these two actions renders the density to be a mixed state. Finally we introduce a negativity-like criterion for entanglement in bipartite systems based on L_1-norm, which indicates entanglement. This criterion also bridges the Paper I with a similar criterion in Paper V, c.f. fig. 3.

Paper II

A toy model relaxation of the unitarity of a quantum search algorithm would lead to an open quantum systems modelling search. Implementing this idea a χ parametric quantum search is introduced and investigated mathematically via a one-parameter family of CPTP maps by introducing the framework of oracle matrix algebra. Particular values of χ lead to three special examples $\mathcal{E}_S, \mathcal{E}_V, \mathcal{E}_W$ of the generic CPTP map. An detail investigation of the decision tree of the possible choices for the possible search map and the respective complexity vs. accuracy trading are provided. In short the ensuing parametric search is shown to be conditionally as fast as the original algorithm. Main finding: set G_2 is determined such that if $\chi \in G_2$, the evolved density matrix $\mathcal{E}_V^m(\rho_s)$ is projective and the algorithm is successful.

Next the paper proceeds to suggest a general quantum search strategy valid for *any positive* χ, and summarizes the findings in the form of demarcation of fast-search domains in the (χ,database size) plane for various numbers k of marked items. Turning to geometric aspects of quantum search first the papers deal with the original unitary algorithm demonstrating the geodesic character of search orbits on the Bloch sphere as well a novel axial

symmetry designated *azimuthal symmetry* of the algorithm.

In addition to those algebraic and complexity issues the question of geometrical consequences of the parametric - open system like - quantum search is addressed. Motivated by the *state-observable duality* (density operator-observable operator trace inner product duality on any Hilbert state space), the density matrix and the CPTP search map are shown to be represented in a modified geometrical setting. In accordance to the general theory in which any density matrix is characterized by its Bloch vector lying in the surface of the (Bloch) sphere on in the interior of the (Bloch) ball, the parametric CPTP map is shown to induce an affine transformation on the search Bloch vector that moves it from the sphere to an ellipsoid lying in the interior of the Bloch ball. As to the dual object, viz. the CPTP search map, it is shown that it is characterize by a matrix implementing affine transformations on the Bloch vector. The positivity and complete positivity conditions imposed on the map induce general constrains on the eigenvalue vector of its associated matrix to be lying inside a tetrahedron or on its faces or edges. Focusing specifically on map E_V, the optimally nearest noise free ($\chi = 0$), search map, it is shown that by varying the free parameter χ, its representing point spans a line segment on one of the edges of the tetrahedron. The resulting geometric modifications for the dual state-observable pair can be inspected in figures 8, and 10, which display respectively the Bloch vector ellipsoid and the search map tetrahedron.

Paper III

This work utilizes the underlying algebraic structure of search algorithm and its matrix representation theory so that the algorithm is treated as a computational unit able to be composed in two different ways, to be called *merging* and *concatenation*. Consider n quantum searches, each targeting a single item, that join the domains of their classical oracle functions and direct sum their Hilbert spaces (merging), instead of acting independently (concatenation). E.g. considering joining of two searches in Hilbert spaces H_1, H_2 with dimensions N_1, N_2 :

a) in the form of *concatenation*, i.e. embed their database vectors into a larger space $H_1 \oplus H_2$ of dimension $N_1 + N_2$, we define the new marked item $|x_{conc}\rangle = |x\rangle_{N_1} \oplus |\emptyset\rangle_{N_2} + |\emptyset\rangle_{N_1} \oplus |x\rangle_{N_2}$, where we denote by $|\emptyset\rangle_{N_{1,2}}$ the respective null vectors with all their components being zero and by $|x\rangle_{N_{1,2}}$ the corresponding marked items in H_1, H_2.

b) in the form of *merging*, one considers the quantum search in Hilbert space H_{merg} which is spanned by all database vectors of H_1, H_2 and there are two marked items: $|x\rangle_{N_1}, |x\rangle_{N_2}$.

Definition: Complexity functions $T_{merg}^{(N_1,\ldots,N_n)} = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N_1+\cdots+N_n}{n}} \right\rfloor, T_{conc}^{(N_1,\ldots,N_n)} =$

$\left\lfloor \frac{\pi}{4}\sqrt{N_1} \right\rfloor + \cdots + \left\lfloor \frac{\pi}{4}\sqrt{N_n} \right\rfloor$.

Notation : $T^{(c)} \equiv T_{merg}^{(N_1,...,N_n)}$ the continuous function wrt its arguments $N_1, ..., N_n$.

The main resulting is the following

Proposition: For arbitrary positive integers (database sizes) $\{N_i\}_{i=1}^n$, it holds that $\sqrt{n}T_{merg}^{(c)} < T_{conc}^{(c)} \leq nT_{merg}^{(c)}$.

Moreover, if N_i are: a) consecutive terms of the unbounded sequence $\left\{N_i = 2^i\right\}_{i=1}^n$ then $T_{conc} = \mathcal{O}(\sqrt{n})T_{merg}$; b) terms of a bounded sequence of positive integers with $p = \sup\{N_i\}_{i=1}^n$, $q = \inf\{N_i\}_{i=1}^n$, then $\frac{T_{con}}{Tmerg} \in \Theta(n)$, i.e. $n\lambda^{-1}T_{merg} < T_{conc} \leq n\lambda T_{merg}$, with $\lambda = \frac{\left\lfloor \frac{\pi}{4}\sqrt{p} \right\rfloor}{\left\lfloor \frac{\pi}{4}\sqrt{q} \right\rfloor}$.

This main result of collective search is scrutinized in all intermediated joining schemes, where among n searches k are merged and the rest are left concatenated, via partitioning databases into distinct groups of merged algorithms and then concatenating the resulting groups. Specifically the logistics of joining schemes is carried out via Young diagrams and tableaux of partitions, as well as majorization theory, and it is investigated by introducing two important distinctions, the *Conjugate Partition Criterion* (CPC) and the *Threshold Partition Criterion* (TPC).

Paper IV

The work of this paper is to investigate the inter-relation of Grover's quantum search algorithm with the proverbial quantum walk (QW) algorithm (see Technical Appendix for details, and references therein), and to show in particular that a new version of quantum search can be simulated quantum mechanically by a QW. The suggested simulation is based on the fact that the two algorithms share the same computational advantage i.e. $\mathcal{O}(\sqrt{x})$, where $x = \#items, x = \#steps$, for search and QW respectively. Motivated by the open system quantum search of Paper II, investigating a U_G unitary evolution operator that randomly fluctuates between unitary operators that eventually lead to a optimally unitary CPTP E_V, we ask the following question. Given the fact that the completely positive trace preserving map admits a unitarization i.e. a non-unique unitary dilation in a extended space, and given that a QW on e.g. $\mathbb{Z}$ or $\mathbb{Z}_N$, is a unitary CPTP map that admits a specific QW-ish quantum dilation, (see Technical Appendix for details), the question addressed is how to show that a parametric open quantum search algorithm admits, hence is equivalent to, a QW type unitary dilation. Also what are the consequences, especially in terms of the three target-aspects of this Thesis, from this inter-relation between quantum search and QW.

In more details, the unitary random search map (c.f. Paper II), $\mathcal{E}_V =$

$\sum_{k=0}^{s} q_k Ad(V_k J_s V_k^\dagger J_{x^\perp}) \equiv \sum_{k=0}^{s} q_k Ad(\widetilde{V}_k)$, for $s = 1$ and $q_0 = q_1 = 1/2$, may be unitarized as a QW i.e. $\mathcal{E}_V(\rho) = Tr_c Y_V(\rho_c \otimes \rho) Y_V^\dagger$, where the unitary dilation operator $Y_V : H_c \otimes \mathcal{V}_x \to H_c \otimes \mathcal{V}_x$, reads $Y_V = \sum_k (P_k \otimes \widetilde{V}_k)(Q \otimes 1_{\mathcal{V}_x})$. Here one identifies the "search system" $\mathcal{V}_x$ with the "walker" system and the "coin" space $H_c \approx \mathbb{C}^2$, with coin density matrix $\rho_c = |c\rangle \langle c|$ with $|c\rangle$ a basis vector in "coin space", and the non unique reshuffling matrix Q s.t. $Q \circ Q^*$ is uni-stohastic with entries $q_k = \langle k| \ Q \circ Q^* \, |c\rangle$. The latter implies that the parametric quantum search can be simulated by a QW.

Next, the paper proceed to show that there's a Hamiltonian generator for the unitary Y_V,describing a long range interacting quantum chain model. The model describe an interaction of a quantum system with a Hilbert space, designated as the "search system" or the "walker system", with a set of n qubits, forming a kind of bath of "coin qubits". Tracing out $n \geq 1$ of these bath coins leads to the evolution map $\mathcal{E}_V$, for the walker system at the time step n, i.e. $\mathcal{E}_V^n$. This identification then implies that the number of steps in the search picture equals the number of qubit coins in the QW picture.

Finally the paper shows, by building upon works in QW on complete graphs, that a QW with graph-node conditional unitary reshuffling matrix and after choosing step operator from node to node to be the swap operator between the nodes, would lead graph QW the even steps of which viz. W_q^{2k}, simulate the quantum search step operator U_G^k i.e. $W_q^{2k} = U_G^{\dagger k} \otimes U_G^k$; hence the name "double lane quantum search". In conclusion, the even steps of specially constructed full graph (non unitary) QW, at an extra cost of two additional queries to the oracle, simulate the quantum unitary search algorithm, at each of its coin-walker subspaces. Hence it would serve operationally as a quantum search duplicator.

Paper V

Fast counting is a novel method to address the problem of counting the number of elements of given finite set S in the quantum setting, achieving counting in quadratically less than N counts, where N equals the cardinality of S , by casting the counting problem in the language of quantum algorithms. This work shows fast counting to be possible by employing Grover's search algorithm reformulated mathematically in terms of oracle matrix algebra by treating set S as a search-able database with no additional structure.

We assume, as a rule of the game, that the number N is known to a search-algorithm builder which is solicited to set up a quantum search procedure with a single marked item in a database of size N: The output of searching, expressed by the quantum entanglement developed between two arbitrary parts of database space, in the form of a sequence wrt to iteration number, can be utilized for fast counting. Indeed it is shown that entan-

glement quantified by various measures have a *periodic vanishing behavior* during specific moments of searching, with a period of order $\mathcal{O}(\sqrt{N})$ for $N \gg 1$. Hence a quantum measurement of the entanglement enables the determination of cardinality N quadratically faster than classical counting.

In more concrete terms the main result is expressed by saying that quantum search can alternatively be harnessed to quadratically accelerate the finding the size of a set by mining the multi-particle entanglement built among database qubits in the course of search. This is accomplished by demonstrating and exploiting the periodic projectivity of the reduced density matrix ensuing by de-coupling a fraction of qubits from the total database state. The effect is quantified by showing that a general set of entanglement measures are vanishing periodically at identical moments during search, with period $\mathcal{O}(\sqrt{N})$ wrt the number of iterations which are identified with counts of cardinality.

Looking only for positions of zeros for an entanglement measure, it suffices to employ an indication function that equals zero if entanglement vanishes, so that the number search steps between zeros can me counted and identified with the counting of set S cardinality. I the particular case in which $N-2$ qubits have been de-coupled from total database state, the criterion which has been introduced in paper I for the existence of entanglement in bipartite systems, can be used. In addition to a synchronized vanishing of entropy measures, the papers also show that the monotonic behavior of the entropy functions is also synchronized i.e. they have interval of the same increasing/decreasing tendency separated by vanishing points. Detecting length of intervals with common monotonicity allows to determine fast the periodicity of its variation and hence again fast counting ensues.

Beyond the quadratic speed up of counting, it is shown that by rigging the initial probability of the marked item, (stemmed either by prior information or guess about the item), a hyper-quadratic shortening of the classical counting complexity of the cardinality is achieved.

Technical Appendix

i) *Oracle algebra* $\mathcal{A}_f$
Given a set with N elements, find $1 \leq k \ll N$ marked elements from this set, via a black box (an oracle) that answers queries. The black box can be described by an oracle Boolean function $f : \{1, 2, ..., N\} \rightarrow \{0, 1\}$, introduced as the characteristic function of subset $I \subset \{1, 2, ..., N\}$ of marked items.

Definition: Let a Boolean function $f : \{1, 2, ..., N\} \rightarrow \mathbb{Z}_2$, and the orthogonal vectors $|x\rangle = \frac{1}{\sqrt{\nu}} \sum_{i=1}^{N} f(i) |i\rangle$ and $\left|x^{\perp}\right\rangle = \frac{1}{\sqrt{\nu^{\perp}}} \sum_{i=1}^{N} (1 - f(i)) |i\rangle$, with $\nu = \sum_{i=1}^{N} f(i)$, and $\nu^{\perp} = \sum_{i=1}^{N} (1 - f(i))$, which generate the space $H_2 \equiv \mathcal{V}_x =$

span$\{|x\rangle, |x^{\perp}\rangle\} \approx \mathbb{C}^2$, and the unit element $\Sigma_0 = |x\rangle\langle x| + |x^{\perp}\rangle\langle x^{\perp}|$. The oracle algebra is defined as the vector space $\mathcal{A}_f = \{M \in \mathbb{C}^{N\times N}; M\Sigma_0 M^{\dagger} = \Sigma_0\}$, generated by the elements $\Sigma_1 = |x\rangle\langle x^{\perp}| + |x^{\perp}\rangle\langle x|$, $\Sigma_2 = -i|x\rangle\langle x^{\perp}| + i|x^{\perp}\rangle\langle x|$ and $\Sigma_3 = |x\rangle\langle x| - |x^{\perp}\rangle\langle x^{\perp}|$, with $u(2)$ algebra commutation relations $[\Sigma_\alpha, \Sigma_b] = 2i\Sigma_c$ (cyclically), and $[\Sigma_0, \text{everything}] = 0$, i.e. $\mathcal{A}_f \approx u(2)$, oracle algebra is isomorphic to $u(2)$ matrix algebra.

A S-dimensional matrix representation of $\mathcal{A}_f$ is provided by the algebra homomorphism $\pi_S : \mathcal{A}_f \to Mat(H_S)$, where $H_S = span\{|i\rangle\}_{i=1}^{S}$. Explicitly, any element $A \in\in \mathbb{C}^{N\times N}$ is embedded in $\mathcal{A}_f$, by a S-dim matrix $\pi_S(A) = \pi_S(\Sigma_0)A\pi_S(\Sigma_0^{\dagger})$.

ii) *Quantum search with rigged marked item probability*

Define $\mathcal{D}_M = \{\rho \in \mathcal{M}_M(\mathbb{C}); \rho^{\dagger} = \rho, \rho > 0, Tr\rho = 1\}$. Let $\{p_j\}_{j=1}^{N}$ be the initial distribution of items-vector in database Hilbert space. Mark a single item $|x\rangle$ with probability $p_x \equiv p \in (0,1)$, so that the initial vector $|\widetilde{s}\rangle = \sum_{j=1}^{N}\sqrt{p_j}|j\rangle$ equals $|\widetilde{s}\rangle = (\cos\widetilde{\alpha})|x\rangle + (\sin\widetilde{\alpha})|x^{\perp}\rangle$, where $|x^{\perp}\rangle = \frac{1}{\sqrt{1-p}}\sum_{j\neq x}\sqrt{p_j}|j\rangle$, and $\widetilde{\alpha} = \cos^{-1}(\sqrt{p})$. Operating m times on the initial state $\pi_N(\widetilde{\rho}_s) = |\widetilde{s}\rangle\langle\widetilde{s}|$, with search operator $\pi_N(\widetilde{U_G}) = \exp(i\widetilde{\theta}\pi_N(\Sigma_2))$, where $\widetilde{\theta} = \pi - 2\widetilde{\alpha}$, yields a state that projects on target item $\pi_N(\widetilde{\rho}_x^{(n)}) = |x\rangle\langle x|$, with probability

$$\widetilde{p}(m) = Tr\left[\pi_N(\widetilde{\rho}^{(n)}(m))\pi_N(\widetilde{\rho}_x^{(n)})\right] = \cos^2(\widetilde{\alpha} - m\widetilde{\theta}).$$

At m-th step the density matrix is

$$\begin{aligned}\pi_N(\widetilde{\rho}^{(n)}(m)) &\equiv \widetilde{U_G}^{m}\pi_N(\widetilde{\rho_s}^{(n)})\widetilde{U_G}^{m\dagger} \\ &= \frac{1}{2}\left(\pi_N(\Sigma_0) + \widetilde{s}_1(m)\pi_N(\Sigma_1) + \widetilde{s}_3(m)\pi_N(\Sigma_1)\right)\end{aligned}$$

with $\widetilde{s}_1(m) \equiv \langle\Sigma_1\rangle = -\sin(2m\widetilde{\theta} - 2\widetilde{\alpha})$, $\widetilde{s}_3(m) \equiv \langle\Sigma_3\rangle = \cos(2m\widetilde{\theta} - 2\widetilde{\alpha})$, where $\langle\Sigma_{1,3}\rangle = \pi_S(\widetilde{\rho}^{(s)}\Sigma_{1,3})$ the mean values of the algebra generators, abbreviated to $\widetilde{s}_i \equiv \langle\Sigma_i\rangle$. The first time when $\widetilde{p}(m) = 1$, equals

$$m = \widetilde{m}(p) = \frac{\widetilde{\alpha}}{\widetilde{\theta}} = \frac{\cos^{-1}(\sqrt{p})}{\sin^{-1}(2\sqrt{p - p^2})}$$

Initial and target states are unitarily related i.e. $|\widetilde{s}\rangle = \pi_N(\widetilde{R})|x\rangle \equiv \exp(-i\widetilde{\alpha}\pi_N(\Sigma_2))|x\rangle$. The evolved state $|\widetilde{s}^{(m)}\rangle = \pi_N(\widetilde{U_G}^{m})|\widetilde{s}\rangle$, projects on the target state with probability $\widetilde{p}(m) = |\langle x|\widetilde{s}^{(m)}\rangle|^2$, determined exclusively by the xx- matrix element of the combined unitary operators $\pi_N(\widetilde{U_G}^{m}\cdot\widetilde{R})$, explicitly $\widetilde{p}(m) = \langle x|[\pi_N(\widetilde{U_G}^{m}\cdot\widetilde{R}) \circ \pi_N(\widetilde{U_G}^{m}\cdot\widetilde{R})^*]|x\rangle$, i.e. by the xx-matrix element of its element-wise product with its complex conjugate. This suggests that any unitary transformation on the initial vector $|\widetilde{s}\rangle \to V|\widetilde{s}\rangle$ that accepts the

marked vector as fixed point up to a phase i.e. $V|x\rangle = e^{i\phi}|x\rangle$, gives an equal complexity search algorithm; such transformations belong to $U(1)\otimes U(N-1)$ group, hence the algorithm's search evolution orbit $\left|\widetilde{s}^{(m)}\right\rangle$ belongs to the $U(N)/U(1)\otimes U(N-1) = CP^{N-1}$ Grassmannian space (see also the hidden subgroup problem aspects of Grover's algorithm [1]).

The asymptotic limit when $0 < p \ll 1$ and $N \to \infty$, yields $\widetilde{\theta}(p) = \mathcal{O}(p^{\frac{1}{2}})$ and $\widetilde{m}(p) = \mathcal{O}(\frac{\pi}{4\sqrt{p}})$. Some indicative choices of probability p would provide new possibilities for search complexity and associated counting time. The following cases of p are interesting for $\widetilde{p}(\widetilde{m}(p)) = 1$:
a) in general for $0 < p \ll 1$, we obtain $\widetilde{m} \approx \mathcal{O}(1/\sqrt{p})$;
b) for $p = 1/N$ and $N \gg 1$ we obtain the standard optimal result $\widetilde{m} \approx \mathcal{O}(\frac{\pi}{4}\sqrt{N})$;
c) For quadratically larger item probability $p = 1/\sqrt{N}$ and $N \gg 1$, we obtain a quadratic speed up of search complexity $\widetilde{m} \approx \mathcal{O}(\frac{\pi}{4}N^{1/4})$;
d) slowing down parameter $\widetilde{m}$ below its classical value (with $p = 1/N$), is also possible: e.g. the choice $p = 1/N^2$ yields $\widetilde{m} \approx \mathcal{O}(N)$, while if $p = 1/N^3$ then $\widetilde{m} \approx \mathcal{O}(N\sqrt{N})$.

iii) *CPTP maps*

Let a finite dimensional Hilbert space H and let the set of endomorphisms $End(H)$. A *positive* map $\mathcal{E} : End(H) \to End(H)$, gives $\mathcal{E}(X) \geq 0$ for any positive element $X \in End(H)$. Given a (normalized) element $|\Psi\rangle \in H$, its rank one projection operator is $\rho_\Psi = |\Psi\rangle\langle\Psi|$. Let P be the set of all such ρ_Ψ elements. Let further $\mathcal{D} = convex\ hull(P)$ be the set of density matrices $\rho \in \mathcal{D}$, where any ρ is positive, Hermitian and of unit trace. Those elements describe the *state* of a quantum system in H.
A completely positive trace preserving (CPTP) map $\mathcal{E} : \mathcal{D} \to \mathcal{D}$, transforms density matrices into themselves, namely $\mathcal{E}(\rho)$ is positive, Hermitian and trace one matrix. Additionally it is *completely positive*, namely for any $n \in \mathbb{N}$, the extension map $id_n\otimes\mathcal{E}$ acting on $M_n\otimes\mathcal{D}$, where M_n is the algebra of square matrices of dimension n, is again positive [2, 3].
There are two possible ways to represent a CPTP map $\mathcal{E}$. One is the *operator sum representation (OPS):* there is a set of operators $\{S_i\}_{i=1}^n$, (the so called Kraus generators), with the normalization $\sum_{i=1}^n S_i^\dagger S_i = \mathbf{1}$, such that $\mathcal{E}(\rho) = \sum_{i=1}^n S_i \rho S_i^\dagger$. Operator Sum Representation has a unitary freedom (the unitary equivalence of Kraus generators)[2], namely, for two sets of Kraus generators $\{S_i\}_{i=1}^n$ and $\{S'_i\}_{i=1}^n$, the equality $\mathcal{E}(\rho) = \sum_{i=1}^n S_i \rho S_i^\dagger = \sum_{i=1}^n S'_i \rho S_i'^\dagger$ holds iff there is a unitary matrix $U = [u_{kl}]$ such that, $S'_i = \sum_{l=1}^n u_{il} S_l$.
The second representation is the *unitary dilation representation (UDL):* let an auxiliary Hilbert space H_A of some finite dimension and let a quantum system with state space H_A, and let ρ_A its density matrix, then there is a unitary operator V acting on $H_A\otimes H$ such that $\mathcal{E}(\rho) = Tr_A V(\rho_A\otimes\rho)V^\dagger$,

where Tr_A is the partial trace with respect to the auxiliary space $H_A[2,\,4]$. The interilation between OPS and UDL representations is given by chosing $\rho_A = |a\rangle\langle a|$ for some basis vector in H_A, and then obtain for the Kraus generators $S_i = \langle i|U|a\rangle$, i.e. they are located in the a column of unitary U.

iv) *Spherical geodesic distance, Fubini-Study distance in the (Bloch) sphere S^2 and the projective plane CP , and the transition probability between two states of quantum search.*

Oracle algebra is endowed with the trace inner product $\langle\cdot,\cdot\rangle = A_f \times A_f \to \mathbb{R}$, defined for any two elements $x, y \in A_f$, as $\langle x, y\rangle := Tr(xy^\dagger)$. By virtue of this product the success probability reads $\widetilde{p}(m) = |\left\langle x|\widetilde{s}^{(m)}\right\rangle|^2 = \left\langle\widetilde{\rho}^{(m)},\widetilde{\rho}_x\right\rangle$ (for simplicity, $\pi_S(\widetilde{\rho}^{(s)}(m))$ is abbreviated to $\widetilde{\rho}^{(s)}$, whith $S = 2^s$) and is written in terms of 3-vectors $\overrightarrow{s}^{(m)}$ and $\overrightarrow{s}^{(x)}$ as

$$\begin{aligned}\widetilde{p}(m) &= Tr(\widetilde{\rho}^{(s)}\widetilde{\rho}_x) = \frac{1}{2} + 2\,\overrightarrow{s}^{(m)} \cdot \overrightarrow{s}^{(x)} \\ &= \frac{1}{2} + 2\cos d_{S^2}(\overrightarrow{s}^{(m)} \cdot \overrightarrow{s}^{(x)}).\end{aligned}$$

Function d_{S^2} appeared about stands for the spherical geodesic distance between two points determined by radii $\overrightarrow{\alpha}$ and $\overrightarrow{\beta}$ on a sphere S^2, and is the distance of the shortest path along sphere's surface from $\overrightarrow{\alpha}$ to $\overrightarrow{\beta}$, lying along a great circle, and equals $d_{S^2} = \cos^{-1}(\overrightarrow{\alpha} \cdot \overrightarrow{\beta})$, (for previous works regarding the relation of quantum search to geodesics see [5], [6]; also for geometric aspects of quantum theory and quantum states, see respectively [7] and [8]). Distance d_{S^2}, $(0 \leq d_{S^2} \leq \pi)$ is determined by the success probability

$$\begin{aligned}d_{S^2}(\overrightarrow{s}^{(m)} \cdot \overrightarrow{s}^{(x)}) &= \cos^{-1}(\widetilde{p}(m) - 1/2) \\ &= \cos^{-1}(\frac{1}{4}(1 - D_{FS}(|x\rangle, \left|\widetilde{s}^{(m)}\right\rangle))),\end{aligned}$$

where in the last equation the Fubini–Study distance D_{FS} appears. The Fubini-Study distance $D_{FS}(\widetilde{|\psi_1\rangle}, \widetilde{|\psi_2\rangle})$ between two $U(1)$ rays

$$\widetilde{|\psi_i\rangle} = \{e^{i\delta_i}|\psi_i\rangle\,|0 \leq \delta_i < 2\pi, |\psi_i\rangle \in H\}$$

of the complex projective plane $CP \approx SU(2)/U(1)$, corresponding to vectors $|\psi_i\rangle \in H$, $i = 1, 2$, in Hilbert space H, is defined as

$$D_{FS}(\widetilde{|\psi_1\rangle}, \widetilde{|\psi_2\rangle}) = \inf_{\delta} ||\,|\psi_1\rangle - e^{i\delta}|\psi_2\rangle\,||^2$$

and is equal to

$$D_{FS}(\widetilde{|\psi_1\rangle}, \widetilde{|\psi_2\rangle}) = 2(1 - |\langle\psi_1|\psi_2\rangle|^2)$$

(see e.g. [9]). Identifying $|\psi_2\rangle \equiv \widetilde{U}_G^m |\widetilde{s}\rangle \equiv \left|\widetilde{s}^{(m)}\right\rangle$, and $|\psi_1\rangle \equiv |x\rangle$, the 'transition probability' between these vectors $\widetilde{p}^{(m)} = |\left\langle \widetilde{s}^{(m)}|x\right\rangle|^2$, is obtained.

Referring to the three related sequences by $\widetilde{p}(m)$, $d_{S^2;m}$, $D_{FS;m}$, $m = 0, 1, 2, ...$ pertinent to the algorithm that are associated with the success probabilities and with the two geodesic distances in the Bloch sphere S^2 and the projective plane CP respectively, we remark, echoing ref. [7], that the introduction of spherical and projective geometry in our context illustrates how the notions of probability and distance become interlinked, once quantum search algorithm is formulated in a geometric manner. The geodesic distances with respect to the $d_{S^2;m}$ and $D_{FS;m}$ metrics determine the transition probability between the two states and vice versa.

v) *Measures of Entanglement*

Let a bipartite quantum system in $H_t = H_1 \otimes H_2 \approx \mathbb{C}^m \times \mathbb{C}^n$ with total density matrix $\rho_t \in \mathcal{D}(H_t)$. The reduced density matrix $Tr_{1,2}\rho_t = \rho_{2,1} \in \mathcal{D}(H_{2,1})$, can be used to quantify the quantum entanglement between the two subsystems. If ρ stand either for ρ_1 or ρ_2 the the quantum Renyi entropy is a family of entropic measurement of quantum entanglement labelled by a non negative parameter $\alpha \neq 1$, $S_\alpha(\rho) = \frac{1}{1-\alpha} \log Tr(\rho^\alpha)$. The quantum von Neumann entropy $S_{vN}(\rho) = \lim_{\alpha \to 1} S_\alpha(\rho) = -Tr(\rho \ln \rho)$,is a limiting case obtain via spectral decomposition of the reduced density matrix/operator ρ. The so linear entropy $S_L(\rho) = 1 - Tr(\rho^2)$, is often used. [10].

Additional entanglement measures:

Definition (Wooters): Let $|\Phi\rangle$ be a pure state of a pair of qubits, and $|\Phi^*\rangle = (\sigma_2 \otimes \sigma_2)|\Phi\rangle$, where $|\Phi^*\rangle$ is the complex conjugate of $|\Phi\rangle$ in the standard basis $|00\rangle, |11\rangle, |01\rangle, |10\rangle$, the *concurrence* of the state $|\Phi\rangle$ is defined to be the non negative number $C(\Phi) = |\langle\Phi|\Phi^*\rangle|$ [11].

Corollary: Let ρ the density matrix of a bipartite system, and

$$\widetilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$$

and let also $\lambda_1 > \lambda_2 > \lambda_3 > \lambda_4$ the eigenvalues of the Hermitian operator $R = \sqrt{\sqrt{\rho}\widetilde{\rho}\sqrt{\rho}}$, in decreasing order. Then, the concurrence for the density matrix ρ, equals

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}.$$

vi) *Partitions and Young diagrams*

If λ is a partition of a non negative integer k, we write $\lambda \vdash k$, and $\lambda = (\lambda_1, ..., \lambda_k)$ is a sequence of non negative integers λ_i for $i = 1, 2, ..., k$, such that $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_k \geq 0$ with $\sum_{i=1}^k \lambda_i = k$. The partition λ is said to be of weight $|\lambda| = k$ and length $l(\lambda)$, where $\lambda_i > 0$ for all $i \leq l(\lambda)$, and $\lambda_i = 0$ for all $i > l(\lambda)$. In specifying λ, the trailing zeros, that is those $\lambda_i = 0$, are often omitted, and the non-zero λ_i are called the *parts* of λ. Obviously, the length of a partition equals to the number of its parts. By way of illustration, if $k = 10$, we regard $(4, 2, 2, 1, 1, 0, 0, 0, 0)$ and $(4, 2, 2, 1, 1)$ as the same

partition λ, for which it holds that $|\lambda| = 10$ and $l(\lambda) = 5$. Each partition of weight $|\lambda| = k$, and length $l(\lambda)$ defines a Young diagram consisting of $|\lambda|$ boxes arranged in $l(\lambda)$ left-adjusted rows of lengths from top to bottom $\lambda_1, ..., \lambda_{l(\lambda)}$ (in the English convention). Young lattice is a partially ordered set consisted of all Young partitions, ordered by inclusion of their Young diagrams. The notation follows in large part that of [12].

vii) *Quantum Random Walks* ([13, 14], and references therein)

Remark: The formalism of QW starts with the construction of a unitary step operator for the composite coin-walker system which evolves its total density matrix and subsequently the coin system is decoupled by performing the map of partial trace, modelling mathematically in this way the classical coin tossing. The resulting CPTP map acts on the walker density matrix only. The initial unitary step operator, by reasoning backwards, is identified with the unitary dilation of the CP map. Composition of the step CP map acting on the initial walker density matrix generates the current step walker density matrix from which by performing projection quantum measurements the sequence of the occupation probabilities for the site of the walker space/lattice is generated. This formalism serves as prototype for the quantum search algorithm and its inter-relation with the QW algorithm, the topic of Paper IV.

Quantum Walk on Integers. Exact dynamics: Let a random walker hopping on the lattice of integers $\mathbb{Z}$. Let $\mathcal{H}_w = span\{|m\rangle ; m \in \mathbb{Z}\} \approx l_2(\mathbb{Z})$, be the walker's Hilbert space on which step operators $E_\pm = e^{\pm i\widehat{\Phi}}$, and position operator L, (that form the Euclidean Lie algebra $ISO(2)$, see [14]), act on the canonical basis respectively as $|m\rangle \rightarrow E_\pm |m\rangle = |m \pm 1\rangle$, and $|m\rangle \rightarrow L|m\rangle = m|m\rangle$. Walker's position is decided by coin tossing. On the coin Hilbert space $\mathcal{H}_c = span\{|+\rangle = heads, |-\rangle = tails\} \approx l_2(\{+,-\})$, act the projection operators $P_\pm = |\pm\rangle\langle\pm|$, Coin-walker systems are described by the respective density matrices ρ_c, ρ_w acting on the total space $\mathcal{H}_c \otimes \mathcal{H}_w$. The classical random walk (CRW), is described by the step unitary operator $V_{cl} = P_+ \otimes E_+ + P_- \otimes E_-$, via the action $\rho_c \otimes \rho_w \rightarrow \mathcal{E}^k_{cl}(\rho_w) = Tr_c[V^k_{cl}(\rho_c \otimes \rho_w)V^{k\dagger}_{cl}]$, which reproduces the kth step classical probability distribution as $\langle m|\mathcal{E}^k_{cl}(\rho_w)|m\rangle \equiv p^k_{cl}(m)$.

The so called U quantization rule of CRW introduces the transformation $V_{cl} \rightarrow V_q = V_{cl}U \otimes \mathbf{1}_w$, where U is unitary (reshuffling) matrix in coin space. The QW density matrix at $k-$th step $\rho_w \rightarrow \mathcal{E}^k_q(\rho_w)$ reads,

$$\mathcal{E}^k_q(\rho_w) = Tr_c[V^k_q(\rho_c \otimes \rho_w)V^{k\dagger}_q],$$

with occupation probabilities being obtained from the diagonal element of the non-diagonal evolved density matrix $p^k_q = \langle m|\mathcal{E}^k_q(\rho_w)|m\rangle$.

The marked difference between CRW and QWs is the quadratic enhancement of the diffusion rate in the quantum case exemplified by the standard deviation of a QW being $\mathcal{O}(t)$ after t step contrary to the standard $\mathcal{O}(\sqrt{t})$

result of CRW. This quantum effects is attributed to the non-diagonal reshuffling matrix U the necessary existence of which modifies classical evolution operator, c.f. $V_{cl} \rightarrow V_q U \otimes \mathbf{1}_w \equiv V_q$, rendering V_q to a form of entanglement creating operator (compare to the Bell states generation case and circuit [14]), between coin and walker state vectors. The reshuffling $U = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \in SO(2)$, employed depends on angle θ to be estimated. The dual space $\mathcal{H}_w^* = span\{|\phi\rangle ; \phi \in [0, 2\pi), \frac{d\phi}{2\pi}\} \approx L_2([0, 2\pi), \frac{d\phi}{2\pi})$, is the eigenspace of step operators $E_\pm |\phi\rangle = e^{\pm i\widehat{\Phi}} |\phi\rangle = e^{\pm i\phi} |\phi\rangle$, and the phase operator $\widehat{\Phi}$, is employed to compute the evolution operator as $V_q = \int_0^{2\pi} \{M(\phi;\theta) \otimes |\phi\rangle \langle\phi|\} \frac{d\phi}{2\pi}$, where $M(\phi;\theta) = \begin{pmatrix} e^{i\phi}\cos\theta & e^{-i\phi}\sin\theta \\ -e^{i\phi}\sin\theta & e^{-i\phi}\cos\theta \end{pmatrix}$. The final result is summarized next:

Proposition : *QW's k-th step evolution unitary operator reads*

$$V_q^k = \begin{pmatrix} \mathcal{A}_k & \mathcal{B}_k \\ -\mathcal{B}_k^\dagger & \mathcal{A}_k^\dagger \end{pmatrix},$$

where $\mathcal{A}_k(\widehat{\Phi};\theta)$, $\mathcal{B}_k(\widehat{\Phi};\theta)$, *with* $\mathcal{A}_k = \cos\theta e^{i\widehat{\Phi}} U_{k-1}(\cos\theta\cos\widehat{\Phi}) - U_{k-2}(\cos\theta\cos\widehat{\Phi})$ *and* $\mathcal{B}_k = \sin\theta e^{-i\widehat{\Phi}} U_{k-1}(\cos\theta\cos\widehat{\Phi})$. ($U_k$ the second kind Chebyshev polynomial of order k).

References

[1] S.J. Lomonaco and L.H. Kauffman, Quantum Inf. Process, **6**, 461-476, (2007)

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge Univ. Press, 2000).

[3] M. D. Choi, Linear Algebra Appl. **10** 285(1975)

[4] W. F. Stinespring, *Positive Functions on C * - algebras*, Proc. Amer. Math. Soc. **6**, 211, (1955).

[5] J. J. Alvarez and C. Gomez, "*A comment on Fisher Information and quantum algorithms*", arXiv:quant-ph/9910115 (2000).

[6] A. Miyake and M. Wadati, "*Geometric strategy for the optimal quantum search*", Phys. Rev. A**64**, 042317 (2001).

[7] D. C. Brody and L. P. Hughston "*Geometric Quantum Mechanics*", J. Geom. Phys. **38** 19(2001)

[8] K. Zyczkowskiand W. Słomczynski, "*The Monge metric on the sphere and geometry of quantum states*", J. Phys. A: Math. Gen. **34** 6689–6722(2001)

[9] D. Ellinas, "*On coherent states and q-deformed algebras*", Proc. of Intern. Symp. Coherent States: Past, Present and Future , Oak Ridge USA, 1993. Eds. D.H. Feng. J.R. Klauder and M.R. Strayer, (World Sci. Singapore 1994). p. 139-151.

[10] K. Zyczkowski, I. Bengtsson, *Geometry of Quantum States: An Introduction to Quantum Entanglement*, Cambridge Univ. Press, (2006).

[11] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998)

[12] I. G. MacDonald, *Symmetric functions and Hall polynomials*, Calderon Press, Oxford, 1979; 2nd edition 1995.

[13] D. Ellinas and P. D. Jarvis, *Maximum Likelihood Parameter Estimation via Reluctant Discrete Quantum Walk,* manuscript 2018

[14] D. Ellinas and I. Smyrnakis, *Quantum Rules and Quantum Simulation of Asymptotics*, Physical Review A **76**, 022333, 2007.

Matrix Algebra for Quantum Search Algorithm: Non Unitary Symmetries and Entanglement*

Demosthenes Ellinas and Christos Konstandakis

Department of Sciences, Mathematical Physics and Quantum Information MΦQ Research Unit
Technical University of Crete GR 731 00 Chania Crete Greece

Abstract. An algebraic reformulation of the quantum search algorithm associated to a *k*-valued oracle function, is introduced in terms of the so called *oracle matrix algebra*, by means of which a Bloch sphere like description of search is obtained. A parametric family of symmetric completely positive trace preserving (CPTP) maps, that formalize the presence of quantum noise but preserves the complexity of the algorithm, is determined. Dimensional reduction of representations of oracle Lie algebra is introduced in order to determine the reduced density matrix of subsets of qubits in database. The L1 vector-induced norm of reduced density matrix is employed to define an index function for the quantum entanglement between database qubits, in the presence of non invariant noise CPTP maps. Analytic investigations provide a causal relation between entanglement and fidelity of the algorithm, which is controlled by quantum noise parameter.

Keywords: Quantum search algorithm, quantum noise, quantum maps, entanglement
PACS: 03.67.Lx, 89.70.+c

THE ORACLE MATRIX ALGEBRA

Introduction. Let the set $D=\{1,2,...,N\}$, subset $I\subset D$, |I|=k, and the oracle function f defined as the characteristic function of I with k elements. Let the Hilbert space $l_2(D)$ the vector $|x\rangle=\frac{1}{\sqrt{\nu}}\sum_{i=1}^{N}f(i)|i\rangle$, determined by the wanted items and its orthogonal complement $|x^{\perp}\rangle=\frac{1}{\sqrt{\nu^{\perp}}}\sum_{i=1}^{N}(1-f(i))|i\rangle$, with $\nu=\sum_{i=1}^{N}f(i)$ and $\nu^{\perp}=\sum_{i=1}^{N}(1-f(i))$ normalization factors. The generators of oracle algebra A_f are $\Sigma_1=|x\rangle\langle x^{\perp}|+|x^{\perp}\rangle\langle x|$, $\Sigma_2=-i|x\rangle\langle x^{\perp}|+i|x^{\perp}\rangle\langle x|$, $\Sigma_3=|x\rangle\langle x|-|x^{\perp}\rangle\langle x^{\perp}|$, and $\Sigma_0=|x\rangle\langle x|+|x^{\perp}\rangle\langle x^{\perp}|$. They span the vector space of the oracle algebra $A_f=\{\alpha\Sigma_0(f)+\beta\Sigma_1(f)+\gamma\Sigma_2(f)+\delta\Sigma_3(f),\alpha,\beta,\gamma,\delta\in\mathbf{R}\}\approx u(2)$, and satisfy the commutation relations $[\Sigma_a,\Sigma_b]=2i\varepsilon_{abc}\Sigma_c$, $[\Sigma_0,everything]=0$.

*Proceedings 10th Conference Quantum Communication, Measurement and Computing (QCMC) Brisbane, Australia, 19-23 July 2010, Eds. T. Ralph, P. K. Lam. AIP Conf. Proc. **1363**

Representation Theory: There are two matrix representations, i) the 2 dimensional $\pi_2 : A_f \to Lin(H_2)$, ii) the N dimensional reducible one $\pi_N : A_f \to Lin(H_N)$.

Reduction of oracle algebra elements:

Lemma 1: Let $N = 2^n, 0 < M \equiv 2^m < N$. For any Σ_a element the algebra is valid that $Tr_m \pi_N(\Sigma_a) = c_M \pi_{N/M}(\Sigma_a)$, where $c_M = M\sqrt{v_{N/M-k}/v_{N-k}}$, and $Tr_m \equiv Tr^{\otimes m}$.

GROVER'S QUANTUM SEARCH ALGORITHM

The problem: Find $1 \leq k < N$ marked items from the set $D = \{1, 2, ..., N\}$. Let the oracle function f introduced as the characteristic function of subset $I \subset D$ of marked items. The initial vector and the density matrix is chosen to be $|s\rangle = \sqrt{1/N}\sum_{i=1}^{N}|i\rangle$, i.e. $|s\rangle = \sqrt{k/N}\,|x\rangle + \sqrt{(N-k)/N}\,|x^{\perp}\rangle$
and $\rho_s = |s\rangle\langle s| = 1/2\,\pi_N(\Sigma_0) - (N-2k)/2N\,\pi_N(\Sigma_3) + \sqrt{k(N-k)}/N\,\pi_N(\Sigma_1)$. The unitary search map equals $U_G = -J_s U J_x U^{\dagger} = \exp(i\theta\pi_N(\Sigma_2))$, $\theta = \arcsin(2\sqrt{k(N-k)}/N)$, and $U \in SU(2)$ is an unspecified matrix, manifesting the $SU(2)$ symmetry of the algorithm. For $a = \arccos(\sqrt{k/N})$, and l a positive integer, it holds that $\rho^l := U_G^l \rho_s (U_G^l)^{\dagger} = 1/2\pi_N(\Sigma_0) - 1/2\sin(2l\theta - 2a)\pi_N(\Sigma_1) + 1/2\cos(2l\theta - 2a)\pi_N(\Sigma_3)$, therefore ρ^l lies on the (Σ_1, Σ_3) plane.

Complexity : The success probability is obtained by projecting (with respect to the trace inner product of matrices), the time evolved density matrix to the density matrix of the wanted items i.e. $p_l = Tr(U_G^l \rho_s (U_G^l)^{\dagger} |x\rangle\langle x|) = \cos^2(l\theta - a)$. For $N>>1$ it approaches 1, when the repetition number, which equals the number of calls to the oracle, is of the order $l = O(\sqrt{N/k})$ [1].

NON UNITARY SYMMETRIES OF THE ALGORITHM

Definition 1 : Let the density matrix ρ of search algorithm, with projection probability on the marked item $p_x = Tr(\rho|x\rangle\langle x|)$. The family of CPTP maps $E_{(\lambda,t)}$ parametrized by λ and t, is an invariant family of maps if for any λ and t, it preserves this probability, i.e. is valid that $p_x = Tr(\rho|x\rangle\langle x|) = Tr(E_{(\lambda,t)}(\rho)|x\rangle\langle x|)$.

The action of CPTP maps on two dimensional density matrices ρ, is geometrically described by an affine transformation induced on the Bloch vector of ρ. The rotations and translations of such an affine transformation are parametrized by real parameters λ's and *t*'s respectively[2]. Here we consider $E_{(\lambda,t)}$ to formalized a kind of quantum noise interfering in quantum searching, and the map is taken to act on the projection of the density matrix on the 2D projection of the subspace spanned by $|x>$ and $|x^{\perp}>$. Below the exact form of maps $E_{(\lambda,t)}$ are determined by specifying geometrically the range of their parameters.

Proposition 1 : The set of all invariant CPTP maps is $E=\{E_{(\lambda,t)},\lambda_1,\lambda_2,\lambda_3,t_1,t_2,t_3\in \mathbf{R}^6 / t_1=t_3=0,\lambda_1=\lambda_3 \textbf{and} 1/\lambda_1^2+t_2^2/\lambda_2^2=1\}$, and is characterized by parameters *t*'s and λ's. Geometrically the set E, for any given t_2, is the intersection of the cylinder with cross curve $1/\lambda_1^2+t_2^2/\lambda_2^2=1$ with the plane $\lambda_1=\lambda_3$.

QUANTUM NOISE IN SEARCH ALGORITHM

Noise: Let the *N*-dimensional database consisting of projective density matrices, and let the single conjugate action of unitary search operator on the initial ρ_s, i.e. the map $\rho_s \to U_G \rho_s U_G^{\dagger}$. Denote by *Ad* the adjoint action i.e AdX(h)=XhX †. Then $\rho_s \to AdU_G(\rho_s)=Ad(UJ_{|s\rangle}U^{\dagger}J_{|x^{\perp}\rangle})(\rho_s)=Ad(J_{U|s\rangle}J_{|x^{\perp}\rangle})(\rho_s)$. Assuming now that the unspecified U unitary operator, due to the presence of quantum noise, is replaced by a CPTP map with Kraus generator e.g. R_0 and R_1 parametrized by a noise control parameter, we obtain the CPTP search map

$$E_R(\rho_s)=1/2\sum_{i=0,1}Ad(R_iJ_{|s\rangle}R_i^{\dagger}J_{|x^{\perp}\rangle})(\rho_s)=1/2\sum_{i=0,1}Ad(J_{R_i|s\rangle}J_{|x^{\perp}\rangle})(\rho_s).$$

Let $U=U_{\pi/4}$ for concreteness, and let this rotation matrix be corrupted by an external 2D environment via the Hamiltonian coupling [3],
$H_R=H_{\pi/4}+H_{env}=\pi/4\,\pi_N(\Sigma_2)\otimes\pi_N(\Sigma_0)+\chi/2(\pi_N(\Sigma_0)-\pi_N(\Sigma_3))\otimes\pi_N(\Sigma_2)$. Then the CPTP map E_R which replaces the $U_{\pi/4}$ is
$\rho\to Tr_{env}(U_R\rho\otimes|0\rangle\langle 0|U_R^{\dagger})\equiv E_R(\rho)=\sum_{j=0,1}R_j\rho R_j^{\dagger}$, where $U_R=\exp(-iH_R)$. The set of Kraus generators [4], is given by $R_i=\langle i|U_R|0\rangle, i=0,1$, where
$R_0=(\cos(\mu(\chi))\pi_N(\Sigma_0)+i\chi/2\,\delta(\chi)\pi_N(\Sigma_2))\exp(-i\chi/2\,\pi_N(\Sigma_2))$, and
$R_1=\pi/4\,\delta(\chi)\exp(-i\chi/2\,\pi_N(\Sigma_2))$, with $\delta(\chi)=\sin(\mu(\chi))/\mu(\chi)$,
with $\mu(\chi)=\sqrt{\chi^2/4+\pi^2/16}$, and $\chi\geq 0$ the noise parameter. Further we approximate the nonunitary $R_{0,1}$ by their nearest unitaries $V_{0,1}$,with respect to Frobenius norm, i.e.
$V_0=(R_0R_0^{\dagger})^{-1/2}R_0=\exp(i\varphi(\chi)\pi_N(\Sigma_2))$, and
$V_1=(R_1R_1^{\dagger})^{-1/2}R_1=\exp(-i\chi/2\,\pi_N(\Sigma_2))$ where $\varphi(\chi)=\psi(\chi)-\chi/2$, and $\psi(\chi)$ is the

solution of equation $[\cos^2\mu(\chi)+\chi^2/4\delta^2(\chi)]\cos^2(\psi(\chi))=\cos^2(\mu(\chi))$. This leads to the new search CPTP map $\rho_s \to E_V(\rho_s)=1/2\sum_{i=0,1} Ad(J_{V_i|s\rangle}J_{|x^\perp\rangle})(\rho_s)$. After *l* steps we obtain $E_V^l(\rho_S)=1/2\,\pi_N(\Sigma_0)+s_1\pi_N(\Sigma_1)+s_3\pi_N(\Sigma_3)$, with Bloch components $s_1=-1/2\cos^l(2l\psi(\chi))\sin(2l\psi(\chi)-2l\chi-2\alpha+2l\theta)$, $s_2=0$, and $s_3=1/2\cos^l(2l\psi(\chi))\cos(2l\psi(\chi)-2l\chi-2\alpha+2l\theta)$.

For a figure of merit we choose the radial fidelity function, $f_r(\chi,l):=1/2\,Tr(E_V^m(\rho_s)|x\rangle\langle x|)=1/4(1+\cos^l(2\psi(\chi))\cos T)$, where $T=2(l\psi(\chi)-l\chi-\alpha+l\theta)$ [5].

Remark: Noise map E_V, although not an invariant map, still it retains algorithm's density matrix on the (Σ_1,Σ_3) plane. This motivates its choice as tool to probe the quantum noise-quantum entanglement relation in the context of the algorithm

QUANTUM ENTANGLEMENT IN QUANTUM SEARCH

Lemma 2: Let the 1 norm $\|A\|_1=\max_{1\le j\le n}\sum_{i=1}^{m}|a_{ij}|$. If ρ_a and ρ_b, are 2x2 real density matrices, it is valid that $\|\rho_a\|_1\ge 1, \|\rho_b\|_1\ge 1$ and $\|\rho_a\otimes\rho_a\|_1\ge 1$.

Next, we introduce a negativity-like [6], criterion for entanglement in bipartite systems, based on 1-norm and Lemma 2. Let the reduction e.g. from *n* qubits to 2 qubits ($M=2^{n-2}$). Then the reduce density matrix reads

$$\rho_4\equiv\pi_4(E_V^l(\rho_s))=Tr_{n-2}(\pi_N(E_V^l(\rho_s)))=c_{n-2}(1/2\,\pi_4(\Sigma_0)+s_1\pi_4(\Sigma_1)+s_3\pi_4(\Sigma_3))$$

Let $\rho_4^{T_2}$ be the partial transpose in the second space of the bipartite reduced matrix ρ_4.

Criterion: Let $\mathcal{N}=-1+\|\rho_4^{T_2}\|_1$,(c.f. [6]) and check whether $\mathcal{N}<0$. If yes, then $\rho\neq\rho_a\otimes\rho_b$, therefore there is an indication for the existence of entanglement.

Analytic studies corroborated by numerical results employing the above Criterion verify the causal relation between entanglement of database qubits and accuracy (radial fidelity) of a successful algorithm of complexity $O(\sqrt{\frac{N}{k}})$, for various values of the noise parameter [5].

REFERENCES

1. L. Grover , "Quantum mechanics helps in searching for needle in a haystack," Phys. Rev. Lett. **78**, 325-328 (1997)
2. C. King and M. B. Ruskai, "Minimal Entropy of States Emerging from Noisy Quantum Channels", *IEEE Trans. Info. Theory* **44** 192-209 (1998).
3. I. L. Chuang and Y. Yamamoto, "Creation of a persistent bit using error correction," *Phys. Review A,* **55**, 114-127 (1997).
4. K. Kraus, States, Effects and Operations, Springer, 1983.

5. D. Ellinas and Ch. Konstandakis, «Quantum Noise and Information in Quantum Search Algorithm», in *Quantum Communication Measurement and Computation, (QCMC 2004),* edit by S.M. Barnett, et. al. *AIP Conference Proceedings* **734**(1) American Institute of Physics Inc., Melville, NY, 2004 pp. 179-182; and to appear.
6. G. Vidal and R. F. Werner, "Computable measure of entanglement", *Phys. Review A,* **65**, 032314 (2004).

Parametric quantum search algorithm by CP maps: algebraic, geometric and complexity aspects

2013 J. Phys. A: Math. Theor. 46 415303

(http://iopscience.iop.org/1751-8121/46/41/415303)

IOP Publishing Journal of Physics A: Mathematical and Theoretical

J. Phys. A: Math. Theor. **46** (2013) 415303 (27pp) doi:10.1088/1751-8113/46/41/415303

Parametric quantum search algorithm by CP maps: algebraic, geometric and complexity aspects

Demosthenes Ellinas and Christos Konstandakis

Technical University of Crete, Department of Electronic and Computer Engineering, Mathematical Physics and Quantum Information MΦQ Research Unit, GR 731 00 Chania, Crete, Greece

E-mail: ellinas@ece.tuc.gr and konstandakis@science.tuc.gr

Received 13 March 2013, in final form 19 August 2013
Published 1 October 2013
Online at stacks.iop.org/JPhysA/46/415303

Abstract

A toy model relaxation of the unitarity of a quantum search algorithm is introduced and the resulting parametric quantum search is investigated mathematically via a one-parameter family of completely positive trace preserving maps by introducing the oracle algebra (an SU(2) isomorphic matrix algebra). The parametric search is shown to be conditionally as fast as the original algorithm. Geometrically, it is related to spherical geodesics which exhibit an azimuthal symmetry, while its search map and density matrix enjoy geometric and structural symmetries.

PACS number: 03.67.Lx

(Some figures may appear in colour only in the online journal)

1. Introduction

After Deutsch, Jozsa, Simon, and Shor presented their quantum algorithms for solving, in polynomial time, i.e. exponentially faster than any classical rival, the problems of distinguishing between two or exponentially many cases and integer factorization, respectively, great interest arose in finding other problems for which quantum algorithms could outperform the best known classical algorithms (see e.g. [6]). One of these problems is usually described as 'searching an unsorted database'. Classically, this searching cannot be done in less than $\mathcal{O}(N)$ queries, where N is the number of entries of the database, but in 1996 Grover invented a quantum algorithm which solves this problem with quadratic speed-up, namely with the complexity $\mathcal{O}(\sqrt{N})$. Moreover, in [3, 4] Grover's algorithm was proved to be optimal. Grover's algorithm has various other important applications, e.g., it can be used for estimating the mean and median of a set of numbers, solving the collision problem, finding global and local minima, element distinctness, and solving 3-satisfiability in $\mathcal{O}(\sqrt{2}^n \mathrm{poly}(n))$ steps (see e.g. [38]). Notice also that Grover's algorithm is most useful when N is very large.

A number of investigations have been carried out which relax some of the premises of the original algorithm concerning either the classical oracle (see e.g. [7, 8]) or the unitarity of the model (see e.g. [9, 10]. This situation paves the way to thinking of a reformulation of the quantum search algorithm in the framework of generalized open systems of quantum mechanics, in which system states are described by density operators, and transformations are implemented by non-unitary positive maps [11, 12, 14]).

The main goal of the present work sets is to introduce a novel version of a search algorithm in which the unitarity has been relaxed and replaced by a map that searches in the space of density matrices. Moreover, this map constitutes a continuous deformation of the unitary operator of the original algorithm, and it is parametrized by a single real parameter. The resulting *parametric quantum search algorithm* (PQSA) is investigated thoroughly, and a number of important aspects concerning its geometric and algebraic structure are brought out; finally a novel search protocol operating with *completely positive trace preserving maps* (CPTP or CP maps) is introduced, which manages to preserve complexity, so that under the conditions specified in detail, both the original and the parametric search algorithm share the same complexity.

The outline of the present work is as follows. In the first part of the paper, we first rephrase the algorithm in the language of the *oracle algebra* (see below). Relaxation of unitarity is then introduced by replacing the norm-preserving search operator by a CPTP map, parametrized by a real parameter (to be referred to hereafter as 'the noise parameter'). To bring the CPTP map 'closer' to the original unitary, a unitary precondition is subsequently introduced, which replaces its Kraus generators by their *nearest* unitary matrix. This preconditioning in effect changes the symmetry of the map from $SU(2)$ to $U(1) \oplus U(1)$. Further, the complexity versus accuracy trade-off is investigated. Studying the algorithm's angular fidelity, its robustness is revealed for a specific set of values for the parameter. In turn, this robustness enables the formulation of a novel search strategy. This strategy determines the infima of the database sizes, over which the algorithm now performs accurately with the complexity $\mathcal{O}(\sqrt{N})$.

In the second part of the paper, two geometric aspects of the algorithm are investigated: one for the original unitary algorithm and one for the parametric CP map algorithm. In the former case the azimuthal symmetry of the searching Bloch vector is revealed via oracle algebra formalism; in the latter case characterizations are provided for the search CP map via a tetrahedron, and for the density matrix via a positional symmetry of its elements. In the appendix the $N =$eight-dimensional matrix representation of the oracle algebra generators for the case of the $k = 2$ marked item is provided. Conclusions and prospects are offered at the end.

2. Fast search via the oracle algebra

The problem. Given a set Δ with N elements, find $1 \leqslant k \ll N$ marked elements from this set, via a black box (an oracle) that answers queries. The black box can be described by an oracle function f, introduced as the characteristic function of subset $I \subset \Delta$ of marked items.

A short description of the solution. The fast quantum search algorithm uses the matrix $U_G = -UJ_sU^\dagger J_x$ to search for $1 \leqslant k \ll N$ items/vectors $\{|j\rangle \mid 1 \leqslant j \leqslant k\}$ among N orthonormal others, that span the complex Hilbert space $H_N = \text{span}\{|i\rangle\}_{i=1}^N$ of an unsorted quantum database $D = \{|i\rangle\}_{i=1}^N$ (see the discussion in [22]). Here U is a general $U(N)$ unitary matrix, and $J_s = \mathbf{1} - 2|s\rangle\langle s|, J_x = \mathbf{1} - 2|x\rangle\langle x|$ are reflection operators with respect to the vectors $|s\rangle$ and $|x\rangle$, where $|s\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^N |i\rangle$ is the uniform superposition state of all database vectors, and $|x\rangle = \frac{1}{\sqrt{k}} \sum_{j=1}^k |j\rangle$ the uniform superposition of all marked vectors [1–5]. We denote by

$\mathcal{G}$ the class of unitary search operators U_G with various unitary U, $\left|x^{\perp}\right\rangle = \frac{1}{\sqrt{N-k}} \sum_{j=1}^{k} |j\rangle$ the uniform superposition of all unmarked vectors, and $\mathcal{V}_x = \text{span}\{U|x\rangle, U\left|x^{\perp}\right\rangle\} \approx C^2$, where $U \in U(N)$ such that $\mathcal{V}_x = \text{span}\{|x\rangle, \left|x^{\perp}\right\rangle\}$. Grover proved that the marked item $|x\rangle \in D$ can be found by applying U_G on $|s\rangle$ only for $\mathcal{O}(\sqrt{N/k})$ times, i.e. the quantum search algorithm is quadratically faster than any classical rival, since any classical search requires $\mathcal{O}(N/k)$ trials for finding the target.

The oracle algebra. Next, we reconsider the algorithm from an algebraic viewpoint, and to this end, we define the matrix oracle algebra [23]. Let the set $\Delta = \{1, 2, \ldots N\}$, a subset $I \subset \Delta$, and the oracle function f be the characteristic function of I with k elements, defined as $f(i) = 1$ for $i \in I$, and $f(i) = 0$ for $i \notin I$. Let also the Hilbert space $l_2(D) \equiv H_N$, the vector

$$|x\rangle = \frac{1}{\sqrt{\nu}} \sum_{i=1}^{N} f(i)\,|i\rangle\,,$$

and its orthogonal vector

$$|x^{\perp}\rangle = \frac{1}{\sqrt{\nu^{\perp}}} \sum_{i=1}^{N} (1 - f(i))\,|i\rangle\,,$$

with $\nu = \sum_{i=1}^{N} f(i)$, and $\nu^{\perp} = \sum_{i=1}^{N}(1 - f(i))$. Next, we introduce the following operators Σ_0, Σ_1, Σ_2, Σ_3, as the generators of oracle algebra A_f

$$\Sigma_1 = |x\rangle\langle x^{\perp}| + |x^{\perp}\rangle\langle x|,\ \Sigma_2 = -i|x\rangle\langle x^{\perp}| + i|x^{\perp}\rangle\langle x|,$$
$$\Sigma_3 = |x\rangle\langle x| - |x^{\perp}\rangle\langle x^{\perp}|,\ \Sigma_0 = |x\rangle\langle x| + |x^{\perp}\rangle\langle x^{\perp}|.$$

Definition. *We define as the matrix oracle algebra A_f with respect to the characteristic function f of $I \subset \Delta$, the set $A_f = \{A : A = \alpha\Sigma_0(f) + \beta\Sigma_1(f) + \gamma\Sigma_2(f) + \delta\Sigma_3(f)\}$ where $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ are arbitrary real.*

Remark. Due to the fact that $\Sigma_{0,1,2,3}$ fulfil the Hermitian property, the commutation relations $[\Sigma_\alpha, \Sigma_b] = 2i\Sigma_c$ (cyclically), and $[\Sigma_0, \text{everything}] = 0$, it follows that the set $\{\Sigma_0, \Sigma_1, \Sigma_2, \Sigma_3\}$ is a set 'analogous' to the set of the well known 2×2 Pauli matrices, and $A_f \approx u(2)$.

Representation theory. Let $H_2 \equiv \mathcal{V}_x = \text{span}\{|x\rangle, \left|x^{\perp}\right\rangle\}$ and $H_N = \text{span}\{|i\rangle\}_{i=1}^{N}$. There are two basic matrix representations: the two-dimensional $\pi_2 : A_f \to \text{Lin}(H_2)$, and the N-dimensional reducible one $\pi_N : A_f \to \text{Lin}(H_N)$. For the oracle function $f(i) = 1$, $1 \leqslant i \leqslant k < N$, and zero otherwise, these representations read for $\pi_2(A) \equiv \pi_2(\alpha\Sigma_0 + \beta\Sigma_1 + \gamma\Sigma_2 + \delta\Sigma_3)$

$$\pi_2(A) = \begin{pmatrix} (\alpha + \delta) & (\beta - i\gamma) \\ (\beta + i\gamma) & (\alpha - \delta) \end{pmatrix},$$

and $\pi_N(A) \equiv \pi_N(\alpha\Sigma_0 + \beta\Sigma_1 + \gamma\Sigma_2 + \delta\Sigma_3)$

$$\pi_N(A) = \begin{pmatrix} (\alpha + \delta)\dfrac{1}{k}\widehat{\mathbf{1}}_{k\times k} & (\beta - i\gamma)\dfrac{1}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{k\times(N-k)} \\ (\beta + i\gamma)\dfrac{1}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{(N-k)\times k} & (\alpha - \delta)\dfrac{1}{N-k}\widehat{\mathbf{1}}_{(N-k)\times(N-k)} \end{pmatrix},$$

where $(\widehat{\mathbf{1}}_{st})_{ij} = 1$, $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant t$.

As a numerical example, for $N = 4$, $k = 1$, with $f(1) = 1$ and zero elsewhere, we obtain

$$\pi_4(\Sigma_1)=\frac{1}{\sqrt{3}}\begin{pmatrix}0&1&1&1\\1&0&0&0\\1&0&0&0\\1&0&0&0\end{pmatrix},\quad \pi_4(\Sigma_-)=\frac{1}{\sqrt{3}}\begin{pmatrix}0&1&1&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix},$$

$$\pi_4(\Sigma_2)=\frac{\mathrm{i}}{\sqrt{3}}\begin{pmatrix}0&1&1&1\\-1&0&0&0\\-1&0&0&0\\-1&0&0&0\end{pmatrix},\quad \pi_4(\Sigma_+)=\frac{1}{\sqrt{3}}\begin{pmatrix}0&0&0&0\\1&0&0&0\\1&0&0&0\\1&0&0&0\end{pmatrix},$$

$$\pi_4(\Sigma_3)=\begin{pmatrix}1&0&0&0\\0&-1/3&-1/3&-1/3\\0&-1/3&-1/3&-1/3\\0&-1/3&-1/3&-1/3\end{pmatrix},\quad \pi_4(\Sigma_0)=\begin{pmatrix}1&0&0&0\\0&1/3&1/3&1/3\\0&1/3&1/3&1/3\\0&1/3&1/3&1/3\end{pmatrix}.$$

Let us reconsider the concept of the quantum database: initially we have promoted the n binary strings $(a_1, a_2, \ldots, a_n)$ which constitute the elements of the classical database with size $N = 2^n$, to a set of basis elements $\{|a_1, a_2, \ldots, a_n\rangle\}$ of an N-dimensional Hilbert space $H = (H_2)^{\otimes n}$, where $H_2 = \mathrm{span}\{|0\rangle, |1\rangle\}$. In decimal enumeration of state vectors we write $|a_1, a_2, \ldots, a_n\rangle \equiv |i\rangle$, $i = 1, 2, \ldots, N$, which is the D database used at the beginning. From the elements in D we next construct the projection operators in H, i.e. $P_{(a_1,a_2,\ldots,a_n)} = |a_1, a_2, \ldots, a_n\rangle \langle a_1, a_2, \ldots, a_n|$, by the map $\mathrm{e}^{\mathrm{i}\phi} |a_1, a_2, \ldots, a_n\rangle \to P_{(a_1,a_2,\ldots,a_n)}$, where $0 \leqslant \phi < 2\pi$. This leads to the database $\Pi = \{|i\rangle \langle i|\}_{i=1}^N = \{\rho_i\}_{i=1}^N \approx D/U(1)$ consisting of a collection of N pure density matrices obtained by the database state vector up to an exponential phase factor viz. an element of the $U(1)$ group. Let us introduce the following operation: given the unitary matrices A, B, let the adjoint map $Ad(A) : \Pi \to \Pi : \rho \to Ad(A)(\rho) = A\rho A^\dagger$, where the property $Ad(AB)(\rho) = Ad(A)Ad(B)(\rho)$ is valid. Then the following adjoint action,

$$Ad(U_G)(\rho_s) = U_G \rho_s U_G^\dagger = Ad(U)Ad(J_s)\, Ad(U^\dagger)Ad(J_x)(\rho_s)$$

is the natural extension of Grover's search map from the database of states D, into the database Π of the projection operators.

Next, let us consider the oracle function f, introduced as the characteristic function of subset $I \subset \Delta$ of marked items. For simplicity, we will use the shorthand ρ and $\Sigma_{0,1,2,3}$ for the n-dimensional representation of the density matrix of the algorithm and for the generators of the oracle algebra, as well as for all other involved operators. The initial vector and its corresponding density matrix, in terms of $|x\rangle$, $|x^\perp\rangle$ and the Σ are $|s\rangle = \sqrt{\frac{k}{N}}\,|x\rangle + \sqrt{\frac{N-k}{N}}\,|x^\perp\rangle \in \mathcal{V}_x$, and in the N-dimensional representation read

$$\rho_x \equiv |x\rangle \langle x| = s_3^{(x)}\Sigma_3 + s_0^{(x)}\Sigma_0,$$

with Bloch vector components $(s_0^{(x)} = \frac{1}{2}, s_1^{(x)} = 0, s_2^{(x)} = 0, s_3^{(x)} = \frac{1}{2})$, and

$$\rho_s = |s\rangle \langle s| = \tfrac{1}{2}\Sigma_0 + s_1^{(0)}\Sigma_1 + s_1^{(0)}\Sigma_3,$$

with components $s^{(0)} = (s_1^{(0)}, s_2^{(0)}, s_3^{(0)})$, where

$$s_1^{(0)} = \frac{\sqrt{k(N-k)}}{N},\quad s_2^{(0)} = 0, s_3^{(0)} = -\frac{N-2k}{2N}.$$

The reflection operators with respect to vector $|s\rangle$ and $|x\rangle$ are, respectively,

$$J_s = \frac{N-2k}{N}\Sigma_3 - \frac{2\sqrt{k(N-k)}}{N}\Sigma_1,$$

and

$$J_x = \mathbf{1}_{\mathcal{V}_x} - 2\,|x\rangle\,\langle x| = -\Sigma_3.$$

The unitary search matrix equals $U_G = -UJ_sU^\dagger J_x$, where $U \in U(N)$ due to the $U(N)$ invariance of the Grover algorithm. For $U = \mathbf{1}_x$ (hereafter used as the abbreviation $\mathbf{1}_{\mathcal{V}_x} \equiv \mathbf{1}_x$),

$$\begin{aligned} U_G &= \frac{N-2k}{N}\Sigma_0 + \mathrm{i}\frac{2\sqrt{k(N-k)}}{N}\Sigma_2 \\ &= \exp(\mathrm{i}\theta\Sigma_2), \end{aligned}$$

with $\theta = \arcsin(2\sqrt{k(N-k)}/N)$. For any $n \in \mathbb{N}$, it holds that $U_G^n = \exp(in\theta\Sigma_2)$ and then

$$\rho^{(n)} := U_G^n \rho_s U_G^{n\dagger} = \tfrac{1}{2}\Sigma_0 + s_1^{(n)}\Sigma_1 + s_3^{(n)}\Sigma_3,$$

where Bloch vector components $s^{(n)} = (s_1^{(n)}, s_2^{(n)}, s_3^{(n)})$ read

$$s_1^{(n)} = -\tfrac{1}{2}\sin(2n\theta - 2\alpha), \quad s_2^{(n)} = 0, s_3^{(n)} = \tfrac{1}{2}\cos(2n\theta - 2\alpha),$$

and $\alpha = \arccos(\sqrt{k/N})$. Since for any $A \in \mathrm{End}(\mathcal{V}_x)$, the trace is evaluated as $\mathrm{Tr}(A) = \langle x|A|x\rangle + \langle x^\perp | A | x^\perp \rangle$, it follows that the algorithm's success probability is

$$p_n = \mathrm{Tr}(\rho^{(n)}\,|x\rangle\,\langle x|\,) = \cos^2(n\theta - \alpha),$$

and $p_n = 1$ iff $\cos^2(n\theta - \alpha) = 1$, for $N \gg 1$, $k < N$, i.e. the complexity of the algorithm is $O(\sqrt{N/k})$.

Remark. For $n \in \mathbb{N}$, the density matrix $\rho^{(n)}$ lies in the $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$ plane, where $\widetilde{\Sigma}_a$ will denote the axis corresponding to the operator Σ_a.

3. The parametric quantum search

CPTP maps. An outline of the required mathematical setting is given next.

Let a finite-dimensional Hilbert space be H and let the set of endomorphisms be $\mathrm{End}(H)$. A *positive* map $\mathcal{E} : End(H) \to \mathrm{End}(H)$ gives $\mathcal{E}(X) \geqslant 0$ for any positive element $X \in \mathrm{End}(H)$. Given a (normalized) element $|\Psi\rangle \in H$, its rank-1 projection operator is $\rho_\Psi = |\Psi\rangle\langle\Psi|$. Let P be the set of all such ρ_Ψ elements. Let further $D_P = \text{convex hull}(P)$ be the set of density matrices $\rho \in D_P$, where any ρ is positive, Hermitian and of unit trace. Those elements describe the *state* of a quantum system in H.

A CPTP map $\mathcal{E} : D_P \to D_P$, transforms density matrices into themselves, namely $\mathcal{E}(\rho)$ is positive and the Hermitian matrix with $\mathrm{Tr}(\mathcal{E}(\rho) = 1$. Additionally it is *completely positive*, namely for any $n \in \mathbb{N}$, the extension map $\mathbf{1}\otimes\mathcal{E}$ acting on $M_n \otimes D_P$, whereM_n is the algebra of the square matrices of dimension n, and is again positive [13, 14].

There are two possible ways to represent a CPTP map $\mathcal{E}$. One is the *operator sum representation (OPS):* there is a set of operators $\{S_i\}_{i=1}^n$, (the so-called Kraus generators), with the normalization $\sum_{i=1}^n S_i^\dagger S_i = \mathbf{1}$, such that $\mathcal{E}(\rho) = \sum_{i=1}^n S_i \rho S_i^\dagger$. The OPS has a unitary freedom (the unitary equivalence of Kraus generators)[13], namely, for two sets of Kraus generators $\{S_i\}_{i=1}^n$ and$\{S_i'\}_{i=1}^n$, the equality $\mathcal{E}(\rho) = \sum_{i=1}^n S_i \rho S_i^\dagger = \sum_{i=1}^n S_i' \rho S_i'^\dagger$ holds iff there is a unitary matrix$U = [u_{kl}]$ such that, $S_i' = \sum_{l=1}^n u_{il} S_l$.

The second representation is the *unitary dilation representation:* let H_A be an auxiliary Hilbert space of some finite dimension, let H_A be a quantum system with state space, and let ρ_A be its density matrix. Then there is a unitary operator V acting on $H_A \otimes H$ such that $\mathcal{E}(\rho) = \mathrm{Tr}_A V(\rho_A \otimes \rho)V^\dagger$, where Tr_A is the partial trace with respect to the auxiliary space H_A[13, 15].

Fast search in the database of density matrices. Next, we utilize the $U(N)$ symmetry of Grover's algorithm [5]. Explicitly we have $U_G = -UJ_sU^\dagger J_x$, where by their definition reflections J_x, J_s admit $\mathcal{V}_x$ space as invariant subspace i.e. $J_s\,(\mathcal{V}_x) \in \mathcal{V}_x$ and $J_x\,(\mathcal{V}_x) \in \mathcal{V}_x$. Since $UJ_sU^\dagger = J_{Us}$, we also have $J_{Us}(\mathcal{V}_x) \in \mathcal{V}_x$, so finally $U_G(\mathcal{V}_x) \in \mathcal{V}_x$. A particular choice for U is to be a one-parameter subgroup generated by an element of oracle algebra $A_f \subset \mathbf{su}(N)$ of the form

$$U = U_\varphi = \mathrm{e}^{-\mathrm{i}H_\varphi} = \exp\left(-\mathrm{i}\varphi\Sigma_2\right),$$

$\varphi \in [0, 2\pi)$, where $\Sigma_2 = -\mathrm{i}|x\rangle\langle x^\perp| + \mathrm{i}|x^\perp\rangle\langle x|$, or explicitly

$$U_\varphi = \mathrm{e}^{\mathrm{i}\varphi\Sigma_2} = \Sigma_0\cos\varphi + \mathrm{i}\Sigma_2\sin\varphi.$$

In terms of the N-dimensional representation π_N of A_f, we obtain that $\pi_N(\mathrm{e}^{\mathrm{i}\varphi\Sigma_2}) = \mathrm{e}^{\mathrm{i}\varphi\pi_N(\Sigma_2)}$, where

$$\mathrm{e}^{\mathrm{i}\varphi\pi_N(\Sigma_2)} = \begin{pmatrix} \dfrac{\cos\varphi\widehat{\mathbf{1}}_{k\times k}}{k} & \dfrac{\sin\varphi\widehat{\mathbf{1}}_{k\times(N-k)}}{\sqrt{k(N-k)}} \\ \dfrac{-\sin\varphi\widehat{\mathbf{1}}_{(N-k)\times k}}{\sqrt{k(N-k)}} & \dfrac{\cos\varphi\widehat{\mathbf{1}}_{(N-k)\times(N-k)}}{N-k} \end{pmatrix}.$$

The origin of the parametric quantum search model is the unitary invariance U_φ, considered as the rotation in the database vector space. This rotation operator is allowed to be modified in a dynamical way, namely due to the unintended interaction of the search system with an external quantum system. This will be shown to result in a transformation of the rotation U_φ into a mixture of rotations, namely to a CPTP map with unitary generators. The above modification is physically well motivated as an external interaction of the search quantum system. Cases of modified rotation operators due to external interaction parametrized by some parameter χ have been investigated (see [16] for similar parametric rotations).

The effect of parametric dependence will amount to replace the φ-rotation $U = U_\varphi$, or its $Ad(U_\varphi)$, as it appears in $Ad(U_G)$, by a CPTP map with Kraus operators e.g. $\{T_0, T_1\}$, depending on the parameter χ. This in turn will cause the embedding of $Ad(U_G)$ into the generic CPTP map $\mathcal{E}_T$, defined as follows: $\mathcal{E}_T : \Pi \to$ convex hull(Π), where

$$\mathcal{E}_T = p_1 Ad(T_0 J_s T_0^\dagger\, J_x) + p_2 Ad(T_1 J_s T_1^\dagger\, J_x),$$

with $p_1, p_2 \in [0, 1]$, $p_1 + p_2 = 1$. This means that $\mathcal{E}_T$, depending on the value of the parameter χ, maps in general pure density matrices of the database Π to mixtures of states that belong to the convex hull of elements of the database Π.

For particular choices of values of parameter χ we will construct various special examples of the generic map $\mathcal{E}_T$ with its Kraus generators $\{T_0, T_1\}$. These special examples with their respective generators will be denoted as $\mathcal{E}_S = \{R_0, R_1\}$, $\mathcal{E}_V = \{V_0, V_1\}$ and $\mathcal{E}_W = \{W_0, W_1\}$ (see below).

Relaxing unitarity via parametric rotations. The search maps $\mathcal{E}_S, \mathcal{E}_W$: the standard framework for describing the quantum search is the sub-plane spanned by vectors of Hilbert space $\mathcal{V}_x$. If $\mathcal{V}_x$ is taken to be the state space of a quantum system—let us call it the 'search system'—then we consider an auxiliary quantum system with state space isomorphic to $\mathcal{V}_x$. This system is taken to interact with the 'search system' via the Hamiltonian operator that generates the φ-rotation i.e. $H_\varphi = \varphi\Sigma_2$, by the following interaction term:

$$H_R = H_\varphi + H_{\mathrm{aux}} = \varphi\Sigma_2 \otimes \mathbf{1} + \frac{\chi}{2}\,(\mathbf{1} - \Sigma_3) \otimes \Sigma_2.$$

(See [16] for similar interaction terms, [17, 18], and see [19] for an alternative method that also utilizes the Hamiltonian operator in the quantum search.) From this Hamiltonian we obtain the evolution operator $U_R = \exp(-\mathrm{i}H_R)$, (for $\hbar = 1$) where parameter χ is the strength of

interaction between the search and auxiliary systems. Operator U_R, after projecting onto the search system via partial tracing at the auxiliary 1, becomes a CPTP map $\mathcal{E}_R$ that replaces the unitary φ-rotation, for non-zero values of the χ parameter. This map reads explicitly

$$\rho \to \ \mathcal{E}_R(\rho) = \mathrm{Tr}_{\mathrm{aux}}\left(U_R\rho \otimes |x\rangle\ \langle x|\ U_R^\dagger\right) = \sum_{i=0}^{1} R_i \rho R_i^\dagger,$$

where $R_i = \mathrm{Tr}_{\mathrm{aux}}\left(U_R|x\rangle\langle x^\perp|\right) = \langle i|U_R|x\rangle$, with $i = 0, 1$, corresponding to the labels $x, x^\perp$, are the Kraus generators of map $\mathcal{E}_R$ satisfying the completeness relation $R_0^\dagger R_0 + R_1^\dagger R_1 = 1$. (see [15])

Lemma 1. *The parametric φ-rotation map $\rho \to \mathcal{E}_R(\rho) = \sum_{i=0}^{1} R_i \rho R_i^\dagger$, is described by the operators $R_0 = (\cos\mu(\chi)1 + \frac{\mathrm{i}\chi}{2}\delta(\chi)\Sigma_2)\,\mathrm{e}^{-\frac{\mathrm{i}\chi}{2}\Sigma_2}$, $R_1 = \varphi\delta(\chi)\,\mathrm{e}^{-\frac{\mathrm{i}\chi}{2}\Sigma_2}$, with $\delta(\chi) = \frac{\sin\mu(\chi)}{\mu(\chi)}$ and $\mu(\chi) = \sqrt{\frac{\chi^2}{4} + \varphi^2}$, $\chi \geqslant 0, 0 < \varphi < 2\pi$.*

Proof. For the Hamiltonian of the total system we write

$$H_R = H_\varphi + H_{\mathrm{aux}} = \varphi\Sigma_2 \otimes \mathbf{1} + \frac{\chi}{2}\,(\mathbf{1} - \Sigma_3) \otimes \Sigma_2.$$

Then, for the time evolution operator we have that

$$\mathrm{e}^{-\mathrm{i}H_R} = \mathrm{e}^{\mathbf{1}\otimes\left(-\frac{\mathrm{i}\chi}{2}\Sigma_2\right)}\,\mathrm{e}^{\Sigma_2\otimes(-\mathrm{i}\varphi\mathbf{1})+\Sigma_3\otimes\left(\frac{\mathrm{i}\chi}{2}\Sigma_2\right)}.$$

Employing the well known BCH formula

$$\mathrm{e}^{\Sigma_1\otimes\alpha_1+\Sigma_2\otimes\alpha_2+\Sigma_3\otimes\alpha_3} = (\cosh\alpha)\otimes 1 + \left(\frac{\sinh\alpha}{\alpha}\right)(\Sigma_1\otimes\alpha_1 + \Sigma_2\otimes\alpha_2 + \Sigma_3\otimes\alpha_3)$$

where

$$\alpha_1 = \mathbf{0}, \quad \alpha_2 = -\mathrm{i}\varphi\mathbf{1}, \quad \alpha_3 = \frac{\mathrm{i}\chi}{2}\Sigma_2$$

and $\alpha = \left(\alpha_1^2 + \alpha_2^2 + \alpha_3^2\right)^{1/2} = \mathrm{i}\mu\,(\chi)\,\mathbf{1}$, $\cosh\alpha = \cos\mu\,(\chi)\,\mathbf{1}$, $\sinh\alpha = \mathrm{i}\sin\mu\,(\chi)\,\mathbf{1}$, we obtain that

$$\mathrm{e}^{\Sigma_2\otimes(-\mathrm{i}\varphi\mathbf{1})+\Sigma_3\otimes\left(\frac{\mathrm{i}\chi}{2}\Sigma_2\right)} = \begin{pmatrix} \cosh\alpha + \dfrac{\mathrm{i}\chi}{2}\delta\,(\chi)\,\Sigma_2 & -\varphi\delta\,(\chi)\,\mathbf{1} \\ \varphi\delta\,(\chi)\,\mathbf{1} & \cosh\alpha - \dfrac{\mathrm{i}\chi}{2}\delta\,(x)\,\Sigma_2 \end{pmatrix}.$$

Moreover

$$\mathrm{e}^{\mathbf{1}\otimes\left(-\frac{\mathrm{i}\chi}{2}\Sigma_2\right)} = \begin{pmatrix} \mathrm{e}^{-\frac{\mathrm{i}\chi}{2}\Sigma_2} & 0 \\ 0 & \mathrm{e}^{-\frac{\mathrm{i}\chi}{2}\Sigma_2} \end{pmatrix}$$

and therefore

$$\mathrm{e}^{-\mathrm{i}H_R} = \begin{bmatrix} \left(\cosh\alpha + \dfrac{\mathrm{i}\chi}{2}\delta\,(\chi)\,\Sigma_2\right)\mathrm{e}^{-\frac{\mathrm{i}\chi}{2}\Sigma_2} & -\varphi\delta\,(\chi)\,\mathrm{e}^{-\frac{\mathrm{i}\chi}{2}\Sigma_2} \\ \varphi\delta\,(\chi)\,\mathrm{e}^{-\frac{\mathrm{i}\chi}{2}\Sigma_2} & \left(\cosh\alpha - \dfrac{\mathrm{i}\chi}{2}\delta\,(\chi)\,\Sigma_2\right)\mathrm{e}^{-\frac{\mathrm{i}\chi}{2}\Sigma_2} \end{bmatrix}.$$

So the generators $R_a = \langle a|\ U_R\,|x\rangle$, $a = 0, 1$, of the CPTP map, are obtained as

$$R_0 = \left(\cos\mu\,(\chi)\,\mathbf{1} + \frac{\mathrm{i}\chi}{2}\delta\,(\chi)\,\Sigma_2\right)\mathrm{e}^{-\frac{\mathrm{i}\chi}{2}\Sigma_2}, \quad R_1 = \varphi\delta\,(\chi)\,\mathrm{e}^{-\frac{\mathrm{i}\chi}{2}\Sigma_2}.$$

□

As a result of the substitution $AdU_\varphi \to \mathcal{E}_R$ introduced above, a new modified search map is now introduced by the substitution $AdU_G \to \mathcal{E}_S$, where $\mathcal{E}_S$ involves the Kraus generators R_0, R_1 of the map $\mathcal{E}_R$ as follows,

$$\mathcal{E}_S = \tfrac{1}{2}Ad(R_0 J_s R_0^\dagger J_x) + \tfrac{1}{2}Ad(R_1 J_s R_1^\dagger J_x).$$

Next, we will proceed to define the new search map $\mathcal{E}_V$ (see below), based on the unitary preconditioning of the generator introduced above. Before doing so, sets $G_{1,2}$ must be defined.

We introduce two particular sets of values G_1 and G_2 for the parameter χ : first, the set of *good values* of the quantum noise parameter χ,

$$G_1 = \{\chi_n = \pi\sqrt{4n^2 - 4\varphi^2/\pi^2}, n \in \mathbb{Z}_+ - \{1\}\},$$

for which generator R_0 becomes unitary and R_1 vanishes, and the search map $\mathcal{E}_S$ reduces to the unitary map with complexity $\mathcal{O}(\sqrt{N/k})$; second, the set G_2 defined as follows: the form of generators R_j, $j = 0, 1$ implies that in order for either both to be simultaneously normal operators or for one of them to vanish, it must be the case that $\cos\mu(\chi) = 0$ or $\sin\mu(\chi) = 0$, respectively. If $\sin\mu(\chi) = 0$, then $\chi \in G_1$, and as mentioned above, the search operator reduces to a unitary matrix and the algorithm returns to its classical form. If $\cos\mu(\chi) = 0$, then $\chi \in G_2$, where

$$G_2 = \{\chi_n = \pi\sqrt{4n^2 + 4n + (1 - 4\varphi^2/\pi^2)}, n \in \mathbb{Z}_+\},$$

and by means of the functions $\mu(\chi_n) = n\pi + \frac{\pi}{2}$, $\delta(\chi_n) = \frac{\sin\mu(\chi_n)}{\mu(\chi_n)} = \pm\left(n\pi + \frac{\pi}{2}\right)^{-1}$, we introduce $W_0 \equiv R_0(\chi_n)$ and $W_1 \equiv R_1(\chi_n)$, or explicitly

$$W_0 = \frac{\mathrm{i}\chi_n}{2}\delta(\chi_n)\,\Sigma_2\,\mathrm{e}^{-\frac{\mathrm{i}\chi_n}{2}\Sigma_2}, \quad \text{and} \quad W_1 = \varphi\delta(\chi_n)\,\mathrm{e}^{-\frac{\mathrm{i}\chi_n}{2}\Sigma_2}, \chi_n \in G_2.$$

Consequently this defines a new search map

$$\mathcal{E}_W = \tfrac{1}{2}Ad(W_0 J_s R W_0^\dagger J_x) + \tfrac{1}{2}Ad(W_1 J_s W_1^\dagger J_x),$$

where W_0, W_1 are the generators $W_j = R_j(\chi)$, $j = 0, 1$, $\chi \in G_2$.

Remark. The values of the parameter $\chi \in G_1$ will be referred to as *good* χ of the *first kind,* and the values $\chi \in G_2$ as *good* χ of the *second kind.*

The search map $\mathcal{E}_V$. Next we state the following lemma concerning the nearest unitary matrix of a given matrix [17, 18, 20].

Lemma 2. *Let A be a non-singular complex square matrix, then the nearest unitary matrix to it, in the sense of Frobenius norm, is the unitary matrix which becomes involved in its polar decomposition.*

Proof. If $A \in M_n(\mathbb{C})$ is unitary, the proof is trivial since $A = (AA^\dagger)^{1/2}U = U$. Suppose A is non-unitary and look for a proper unitary $Q \in M_n(\mathbf{C})$ which minimizes the quantity $\|A - Q\|_F^2 \geqslant 0$, where $\|X\|_F = \sqrt{\mathrm{Tr}(XX^\dagger)}$ is the Frobenius norm. It is valid that

$$\begin{aligned}\|A - Q\|_F^2 &= \mathrm{Tr}\{(A - Q)(A^\dagger - Q^\dagger)\}\\ &= \mathrm{Tr}(AA^\dagger) - \mathrm{Tr}(QA^\dagger) - \mathrm{Tr}(AQ^\dagger) + \mathrm{Tr}\mathbf{1}\\ &= \mathrm{Tr}(AA^\dagger) - 2\mathrm{Re}[\mathrm{Tr}(Q^\dagger A)] + n.\end{aligned}$$

Due to the singular value decomposition of $A = V\Sigma W^\dagger$ (where V, W are unitary, with the columns the eigenvectors of $AA^\dagger$ and $A^\dagger A$ respectively, and Σ is diagonal) we have that

$$\begin{aligned}\mathrm{Re}[\mathrm{Tr}(Q^\dagger A)] &= \mathrm{Re}[\mathrm{Tr}(Q^\dagger V\Sigma W^\dagger)]\\ &= \mathrm{Re}[\mathrm{Tr}(W^\dagger Q^\dagger V\Sigma)]\\ &= \mathrm{Re}[\mathrm{Tr}(\Psi\Sigma)].\end{aligned}$$

The matrix $\Psi = W^\dagger Q^\dagger V$ is unitary since W, Q, V are also unitary, so $\mathrm{Tr}(\Psi\Psi^\dagger) = n$ or $\sum_{i=1}^n |\psi_{ii}|^2 = 1$. Recall that for n arbitrary complex numbers $z_k = x_k + y_k \mathrm{i}$, $k = 1, 2, \ldots, n$, and n arbitrary non-negative reals $\vartheta_1, \vartheta_2, \ldots, \vartheta_n \geqslant 0$, it holds that

$$\Re\left(\sum_{k=1}^n \vartheta_k z_k\right) = \sum_{k=1}^n \vartheta_k x_k \leqslant \sum_{k=1}^n \vartheta_k |z_k|$$

and the equality is true iff $z_k = x_k \geqslant 0$. These all imply that

$$\begin{aligned}\mathrm{Re}[\mathrm{Tr}(Q^\dagger A)] &= \mathrm{Re}[\mathrm{Tr}(\Psi\Sigma)] \\ &= \mathrm{Re}\left(\sum_{k=1}^n \psi_{ii}\sigma_{ii}\right) \\ &\leqslant \sum_{k=1}^n |\psi_{ii}|\,\sigma_{ii}\end{aligned}$$

and the equality is valid iff $\psi_{ii} \geqslant 0$. Matrix Ψ is unitary, so $|\psi_{ii}|^2 = 1$, for all $i = 1, \ldots, n$, therefore $\psi_{ii} = 1$ for $i = 1, \ldots, n$, namely $\Psi = \mathbf{1}$. This implies that the minimum of $\|A - Q\|_F^2$ is equal to $\|A - Q\|_{F\,\min}^2 = \mathrm{Tr}(AA^\dagger) - 2\sum_{i=1}^n \sigma_{ii} + n$, where all σ_{ii} are the singular eigenvalues of A, and this equality is true iff $\Psi = \mathbf{1}$ or $W^\dagger Q^\dagger V = \mathbf{1}$, namely $Q = VW^\dagger$. In such a case, the singular value decomposition of A gives

$$A = V\Sigma W^\dagger = (V\Sigma V^\dagger)(VW^\dagger) = (V\Sigma V^\dagger)Q,$$

which, due to the fact that $(AA^\dagger)^{1/2} = V\Sigma V^\dagger$, the latter equation is identified with the polar decomposition of A, and since A is non-singular, this polar decomposition is unique [20]. □

We investigate now a new form of the PQSA by introducing an optimal unitary *preconditioning* of the search map $\mathcal{E}_S$ above, to be called $\mathcal{E}_V$. Since $\mathcal{E}_S$ is determined by the generators of map $\mathcal{E}_R \equiv \{R_0, R_1\}$, we replace these generators by $\mathcal{E}_{RV} \equiv \left\{\frac{1}{\sqrt{2}}V_0, \frac{1}{\sqrt{2}}V_1\right\}$ respectively, which are their optimally closed unitaries (see below). This choice eventually leads to the following *random unitary operation* [21],

$$\mathcal{E}_V = \tfrac{1}{2}Ad(V_0 J_s V_0^\dagger\, J_x) + \tfrac{1}{2}Ad(V_1 J_s V_1^\dagger\, J_x). \tag{1}$$

Remark. Unitary preconditioning and *symmetry breaking*. For any non-singular $n \times n$ complex matrix R, let $V = (RR^\dagger)^{-1/2}R$ be the unique unitary matrix which occurs in the polar decomposition of R, and which is also the nearest unitary matrix to R in the sense of the Frobenius norm. Define next the two maps, u and g_G, where $G = SU(2)$, $G = U(1) \oplus U(1)$, and let us study their compatibility (see the diagram below). Explicitly, the definitions are $u : End(\mathbf{C}^n) \longrightarrow End(\mathbf{C}^n)$, which is the map of the Kraus generator treated as an N-dimensional matrix to its nearest unitary matrix, and $g_G : \mathcal{E} \longrightarrow \mathcal{E}'$, which transforms a CPTP map e.g. $\mathcal{E}(\rho) = \sum_{i=0}^1 S_i \rho S_i^\dagger$ to $\mathcal{E}'(\rho) = \sum_{i=0}^1 S_i' \rho S_i'^\dagger$, by transforming its Kraus generators with $G = SU(2)$ or $G = U(1) \oplus U(1)$ i.e.

$$\begin{pmatrix} S_0' \\ S_1' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix} \begin{pmatrix} S_0 \\ S_1 \end{pmatrix}$$

$$\begin{pmatrix} S_0' \\ S_1' \end{pmatrix} = \begin{pmatrix} \mu & 0 \\ 0 & \nu \end{pmatrix} \begin{pmatrix} S_0 \\ S_1 \end{pmatrix},$$

with $\alpha, \beta, \mu, \nu \in \mathbf{C}$, and $|\alpha|^2 + |\beta|^2 = 1$ for the $SU(2)$ and $|\mu| = |\nu| = 1$ for the $U(1) \oplus U(1)$ cases, respectively.

Referring to the diagram below, consider now the CPTP maps $\mathcal{E}_R$, $\mathcal{E}_{RV}$, $\mathcal{E}'_R$, $\mathcal{E}'_{RV}$, with their respective pairs of Kraus generators $\{R_i\}_{i=0}^1$, $\{R'_i\}_{i=0}^1$, $\{V_i\}_{i=0}^1$, $\{V'_i\}_{i=0}^1$. Let the maps g_G, and the map u defined by $u : \mathcal{E} = \sum_{i=0,1} \lambda_i Ad(R_i) \longrightarrow u(\mathcal{E}) = \sum_{i=0,1} \lambda_i Ad(V_i)$, where $R_{0,1}$ are non-singular $n \times n$ complex matrices, and $V_{0,1}$ are their nearest unitary matrices as above. These maps can be composed alternatively and then be applied as indicated in the diagram

$$\begin{array}{ccccc} & & g_G & & \\ & \mathcal{E}_R & \longrightarrow & \mathcal{E}'_R & \\ u & \downarrow & \searrow\searrow & \downarrow & u. \\ & \mathcal{E}_{RV} & \longrightarrow & \mathcal{E}'_{RV} & \\ & & g_G & & \end{array}$$

We find that the diagram is commutative (i.e. $u \circ g_G = g_G \circ u$) for $G = U(1) \oplus U(1)$, and not commutative (i.e. $u \circ g_G \neq g_G \circ u$) for $G = SU(2)$.

This result implies that generators of $\mathcal{E}_R$ enjoy a $G = SU(2)$ symmetry while those of $\mathcal{E}_{RV}$ enjoy the smaller symmetry of $G = U(1) \oplus U(1)$. Therefore the introduced optimal preconditioning of the generators has as its consequence a *symmetry breaking* effect for the search map. All subsequent results obtained by utilizing $\mathcal{E}_{RV}$ (see the new search map $\mathcal{E}_V$ introduced previously), are valid up to a $U(1)$ transformation of its Kraus generator.

Next, the following lemma determines sets of parameters in which the unitarily preconditioned search map is valid.

Lemma 3. *The contractive CPTP map of equation (1) is generated by means of the two unitary Kraus operators indicated in that equation, which involve the unitary operators* $\left\{\frac{1}{\sqrt{2}}V_0, \frac{1}{\sqrt{2}}V_1\right\}$. *These are defined as* $V_0 = (R_0R_0^\dagger)^{-1/2}R_0 = \mathrm{e}^{\mathrm{i}(\psi(\chi)-\frac{\chi}{2})\Sigma_2}$, $V_1 = (R_1R_1^\dagger)^{-1/2}R_1 = \mathrm{e}^{-\frac{\mathrm{i}\chi}{2}\Sigma_2}$, $0 < \varphi < 2\pi$, $\varphi \neq \pi/2, 3\pi/2$, *where* V_0, V_1 *are the nearest unitary matrices to* R_0, R_1; *in the sense of the Frobenius norm, the function* $\psi(\chi)$ *is determined by the equation*

$$\left(\cos^2\mu(\chi) + \frac{\chi^2}{4}\delta^2(\chi)\right)\cos^2\psi(\chi) = \cos^2\mu(\chi),$$

and $\chi \notin G_1$.

Proof. According to lemma 1 we take that

$$\left(R_0R_0^\dagger\right)^{1/2} = \left(\cos^2\mu(\chi) + \frac{\chi^2}{4}\delta^2(\chi)\right)^{1/2}\mathbf{1}$$

and it is obvious that $\det\left(\left(R_0R_0^\dagger\right)^{1/2}\right) = \left(\cos^2\mu(\chi) + \frac{\chi^2}{4}\delta^2(\chi)\right)^{1/2} \neq 0$ for every $\chi \geqslant 0$.

So $\left(R_0R_0^\dagger\right)^{-1/2} = \left(\cos^2\mu(\chi) + \frac{\chi^2}{4}\delta^2(\chi)\right)^{-1/2}\mathbf{1}$, and $V_0 = \left(R_0R_0^\dagger\right)^{-1/2}R_0$, or

$$V_0 = \left[\frac{\cos\mu(\chi)}{\left(\cos^2\mu(\chi) + \frac{\chi^2}{4}\delta^2(\chi)\right)^{1/2}}\mathbf{1} + \mathrm{i}\frac{\frac{\chi}{2}\delta(\chi)}{\left(\cos^2\mu(\chi) + \frac{\chi^2}{4}\delta^2(\chi)\right)^{1/2}}\Sigma_2\right]\mathrm{e}^{-\frac{\mathrm{i}\chi}{2}\Sigma_2}.$$

Due to the relation

$$\left(\frac{\cos\mu(\chi)}{\left(\cos^2\mu(\chi) + \frac{\chi^2}{4}\delta^2(\chi)\right)^{1/2}}\right)^2 + \left(\frac{\frac{\chi}{2}\delta(\chi)}{\left(\cos^2\mu(\chi) + \frac{\chi^2}{4}\delta^2(\chi)\right)^{1/2}}\right)^2 = 1$$

there exists an angle $\psi(\chi)$ such that

$$\cos\psi(\chi) = \frac{\cos\mu(\chi)}{\left(\cos^2\mu(\chi) + \frac{\chi^2}{4}\delta^2(\chi)\right)^{1/2}},$$

namely, $\left[\cos^2\mu(\chi) + \frac{\chi^2}{4}\delta^2(\chi)\right]\cos^2\psi(\chi) = \cos^2\mu(\chi)$.

Table 1. In the table the existence of the various CPTP search maps in terms of their generators is denoted with yes/no, versus the two disjoint sets G_1, G_2 of parameter χ. In the case where $\chi \in G_2$, where Kraus generators have been replaced by their nearest unitary (upper right), this gives rise to a search map that preserves the projectivity of an initial density matrix.

G_2 / G_1	$\chi \notin G_2$	$\chi \in G_2$
$\chi \notin G_1$	Yes $R_{0,1}$ Yes $V_{0,1}$ No $W_{0,1}$	Yes $R_{0,1}$ Yes $v_{0,1}$ *Projectivity* Yes $W_{0,1}$
$\chi \in G_1$	Yes $R_{0,1}$ $(R_0 = Rot(\frac{n\pi}{2}))$ No $V_{0,1}$ $r_1 = 0$ No $W_{0,1}$	

Therefore we obtain the first generator

$$V_0 = [\cos\psi(\chi)\,\mathbf{1} + \mathrm{i}\sin\psi(\chi)\,\Sigma_2]\,\mathrm{e}^{-\frac{\mathrm{i}\chi}{2}\Sigma_2} = \mathrm{e}^{\mathrm{i}(\psi(\chi)-\frac{\chi}{2})\Sigma_2}.$$

As for the other generator R_1, we take that

$$\left(R_1 R_1^{\dagger}\right)^{1/2} = \varphi\delta(\chi)\,\mathbf{1}$$

and determine the values of parameter χ for which this operator can be inverted, namely

$$\varphi\delta(\chi) \neq 0, \forall\chi \notin G_1.$$

So, for values of χ such that $\chi \notin G_1$, the second unitary generator reads

$$V_1 = \left(R_1 R_1^{\dagger}\right)^{-1/2} R_1 = \mathrm{e}^{-\frac{\mathrm{i}\chi}{2}\Sigma_2}.$$

For the case that $\chi \in G_1$, we have that $R_1 = 0$ and $R_0 = \mathrm{e}^{-\frac{\mathrm{i}\chi}{2}\Sigma_2}$, due to the fact that $\sin\mu(\chi) = 0$. We then conclude that for these values of the quantum noise parameter χ, the search operator reduces to a unitary matrix $U_G = R_0(\chi)$, $\chi \in G_1$, and the algorithm returns to its classical form. □

In order to complete the investigation of search maps obtained by the various possible values of parameter χ, we examine next the case $\chi \in G_2$, since G_1, G_2 are disjoint sets. The following proposition can be proved.

Proposition 4. *Let the operator be $\mathcal{E}_V^m(\rho_s)$, where $\mathcal{E}_V^m$ is the m-times composition of the map $\mathcal{E}_V$, and let χ be the asymptotic of the sequence of $\chi_n \in G_2$. For $m = \mathcal{O}(\sqrt{N/K})$, matrix $Q = \mathcal{E}_V^m(\rho_s)$ is projective (see also table 1).*

Proof. Let us first calculate $\mathcal{E}_V^m(\rho_s)$. According to the previous lemma, we have that

$$\mathcal{E}_V(\rho_s) = \tfrac{1}{2}(V_0 J_s V_0^{\dagger} J_x)\rho_s(V_0 J_s V_0^{\dagger} J_x)^{\dagger} + \tfrac{1}{2}(V_1 J_s V_1^{\dagger} J_x)\rho_s(V_1 J_s V_1^{\dagger} J_x)^{\dagger}$$

or

$$\mathcal{E}_V(\rho_s) = \tfrac{1}{2}\,\mathrm{e}^{\mathrm{i}(\pi-\theta-2\varphi(\chi))\Sigma_2}\rho_s\,\mathrm{e}^{-\mathrm{i}(\pi-\theta-2\varphi(\chi))\Sigma_2} + \tfrac{1}{2}\,\mathrm{e}^{\mathrm{i}(\pi+\chi-\theta)\Sigma_2}\rho_s\,\mathrm{e}^{-\mathrm{i}(\pi+\chi-\theta)\Sigma_2}$$

where $\varphi(\chi) = \psi(\chi) - \frac{\chi}{2}$, $\theta = \sin^{-1}\left(2\sqrt{k(N-k)}/N\right)$, $\alpha = \cos^{-1}(\sqrt{k/N})$. Introducing the variables $\gamma_1 \equiv \gamma_1(\chi, N) = \pi - \theta - 2\varphi(\chi)$, $\gamma_2(\chi, N) = \pi + \chi - \theta$ we take that

$$\mathcal{E}_V(\rho_s) = \tfrac{1}{2}\,\mathrm{e}^{\mathrm{i}\gamma_1\Sigma_2}\rho_s\,\mathrm{e}^{-\mathrm{i}\gamma_1\Sigma_2} + \tfrac{1}{2}\,\mathrm{e}^{\mathrm{i}\gamma_2\Sigma_2}\rho_s\,\mathrm{e}^{-\mathrm{i}\gamma_2\Sigma_2}$$

or

$$\mathcal{E}_V(\rho_s) = \tfrac{1}{2}\left(Ad(\mathrm{e}^{\mathrm{i}\gamma_1\Sigma_2}\rho_s) + Ad(\mathrm{e}^{\mathrm{i}\gamma_2\Sigma_2}\rho_s)\right).$$

After m queries, it holds that

$$\mathcal{E}_V^m(\rho_s) = \left[\tfrac{1}{2}\left(Ad(\mathrm{e}^{\mathrm{i}\gamma_1\Sigma_2}) + Ad(\mathrm{e}^{\mathrm{i}\gamma_2\Sigma_2})\right)\right]^m(\rho_s)$$

or that

$$\mathcal{E}_V^m(\rho_s) = \frac{1}{2^m}\sum_{\nu=0}^{m}\binom{m}{\nu}\mathrm{e}^{\mathrm{i}[(m-\nu)\gamma_2+\nu\gamma_1]\Sigma_2}\rho_s\,\mathrm{e}^{-\mathrm{i}[(m-\nu)\gamma_2+\nu\gamma_1]\Sigma_2}.$$

The diagonalization of ρ_s gives $\rho_s = \mathrm{e}^{\mathrm{i}\alpha\Sigma_2}\rho_x\,\mathrm{e}^{-\mathrm{i}\alpha\Sigma_2}$; after trivial calculations we obtain that the matrix form of $\mathcal{E}_V^m(\rho_s)$ is

$$\mathcal{E}_V^m(\rho_s) = \frac{1}{2^{m+1}}\begin{pmatrix} 2^m + \sum_{\nu=0}^{m}\binom{m}{\nu}\cos 2A(\nu) & \sum_{\nu=0}^{m}\binom{m}{\nu}\sin 2A(\nu) \\ \sum_{\nu=0}^{m}\binom{m}{\nu}\sin 2A(\nu) & 2^m - \sum_{\nu=0}^{m}\binom{m}{\nu}\cos 2A(\nu)\end{pmatrix}$$

where $A(\nu) = -[(m-\nu)\gamma_2 + \nu\gamma_1 + \alpha]$. Employing well known trigonometric formulae we obtain that

$$\begin{aligned}\sum_{\nu=0}^{m}\binom{m}{\nu}\begin{Bmatrix}\cos 2A(\nu)\\ \sin 2A(\nu)\end{Bmatrix} &= \sum_{\nu=0}^{m}\binom{m}{\nu}\begin{Bmatrix}\cos(4\psi(\chi)\nu - 2m\gamma_2 - 2\alpha)\\ \sin(4\psi(\chi)\nu - 2m\gamma_2 - 2\alpha)\end{Bmatrix}\\ &= 2^m\cos^m(2\psi(x))\begin{Bmatrix}\cos(4m\psi(\chi)\nu - 2m\gamma_2 - 2\alpha)\\ \sin(4m\psi(\chi)\nu - 2m\gamma_2 - 2\alpha)\end{Bmatrix}\\ &= 2^m\cos^m(2\psi(\chi))\begin{Bmatrix}\cos T\\ \sin T\end{Bmatrix}\end{aligned}$$

with the obvious identification $T = 2m\psi(\chi) - 2m\gamma_2 - 2\alpha$. This finally leads to the following expression for the density matrix after m queries:

$$\mathcal{E}_V^m(\rho_s) = \frac{1}{2}\begin{pmatrix}1+\cos^m(2\psi(\chi))\cos T & \cos^m(2\psi(\chi))\sin T\\ \cos^m(2\psi(\chi))\sin T & 1-\cos^m(2\psi(\chi))\cos T\end{pmatrix} \equiv Q. \quad (2)$$

Q is a projective operator since it is a 2×2 matrix with eigenvalues 0,1. Next we will find a vector $|\tilde{\psi}\rangle = \binom{\mu}{\nu}$ such that $Q = |\tilde{\psi}\rangle\langle\tilde{\psi}|$. It holds that

$$\frac{1}{2}\begin{pmatrix}1+(-1)^m\cos T & (-1)^m\sin T\\ (-1)^m\sin T & 1-(-1)^m\cos T\end{pmatrix} = |\tilde{\psi}\rangle\langle\tilde{\psi}| \text{or}$$

$$\begin{pmatrix}\cos^2\left(\frac{m\pi+T}{2}\right) & \sin\left(\frac{m\pi+T}{2}\right)\cos\left(\frac{m\pi+T}{2}\right)\\ \sin\left(\frac{m\pi+T}{2}\right)\cos\left(\frac{m\pi+T}{2}\right) & \sin^2\left(\frac{m\pi+T}{2}\right)\end{pmatrix} = \begin{pmatrix}\mu^2 & \mu\nu\\ \mu\nu & \nu^2\end{pmatrix}$$

and therefore

$$\begin{Bmatrix}\mu = \cos\left(\frac{m\pi+T}{2}\right)\\ \nu = \sin\left(\frac{m\pi+T}{2}\right)\end{Bmatrix} \text{or} \begin{Bmatrix}\mu = -\cos\left(\frac{m\pi+T}{2}\right)\\ \nu = -\sin\left(\frac{m\pi+T}{2}\right)\end{Bmatrix}$$

i.e.

$$|\tilde{\psi}\rangle = \binom{\mu}{\nu} = \pm\binom{\cos\left(\frac{m\pi+T}{2}\right)}{\sin\left(\frac{m\pi+T}{2}\right)}.$$

The probability of the success of the algorithm equals:

$$P = |\langle x||\tilde{\psi}\rangle|^2 = \cos^2\left(\frac{m\pi+T}{2}\right) = \cos^2(m\gamma_2+\alpha)$$

since $T = 2m\psi(\chi) - 2m\gamma_2 - 2\alpha$ and $\cos\psi(\chi) = 0$ for $\chi \in G_2$ (i.e. $\psi(\chi) = \pi/2$). The algorithm will be effective iff $\left|\tilde{\psi}\right\rangle = \pm|x\rangle$, namely $\cos(m\gamma_2 + a) = \pm 1$ or

$$\cos(m(\pi\sqrt{4n^2 + 4n + (1 - 4\varphi^2/\pi^2)} - \theta) + \alpha) = \pm 1.$$

or

$$\cos(m\chi_n - m\theta + \alpha) = 1,$$

where $\chi_n \in G_2$. Due to χ being the asymptotic of $\chi_n \in G_2$, i.e. we have that $\chi \approx \chi_n$, the equation above will become

$$\cos(-m\theta + \alpha) = \pm 1.$$

This occurs for $m = \mathcal{O}(\sqrt{N/k})$. □

Euclidean and angular distance. The algorithm investigated so far aims to search the database Π for the wanted item $\rho_x = |x\rangle\langle x|$, starting from the density matrix $\rho_s = |s\rangle\langle s|$, by means of the CPTP search map $\mathcal{E}_T^m(\rho_s) = \mathcal{E}_T^m(|s\rangle\langle s|)$, where $\mathcal{E}_T \in \{\mathcal{E}_S, \mathcal{E}_V, \mathcal{E}_W\}$, that will act m times on the initial density matrix. To evaluate the efficiency of the algorithm with respect to the χ values we next introduce two figures of merit: the *Euclidean distance* $d_T^{(m)}$ *and the angular distance* $\vartheta_T^{(m)}$, furnishing the value of the overlap between the Bloch vectors of the target and the searching density operators i.e.

$$d_T^{(m)} = \left\|\mathcal{E}_T^m(\rho_s) - \rho_x\right\|_F$$

and

$$\vartheta_T^{(m)} = \left|\cos^{-1}\left(\frac{\langle\mathcal{E}_T^m(\rho_s), \rho_x\rangle}{\left\|\mathcal{E}_T^m(\rho_s)\right\| \|\rho_x\|}\right)\right|$$

where $\langle\mathcal{E}_T^m(\rho_s), \rho_x\rangle = \frac{1}{2}\mathrm{Tr}\,\mathcal{E}_T^m((\rho_s)\,\rho_x)$ and $\|X\|_F = \sqrt{\mathrm{Tr}(XX^\dagger)}$ is the Frobenius norm.

Proposition 5. *The Frobenius norm, the Euclidean and the angular distance for the search map* $\mathcal{E}_V$ *, after m queries equal respectively:*

$$\left\|\mathcal{E}_V^m(\rho_s)\right\|_F = \frac{1}{\sqrt{2}}\sqrt{1 + \cos^{2m}(2\psi(\chi))},$$

$$d_V^{(m)} = \frac{1}{\sqrt{2}}\sqrt{1 + \cos^m(2\psi(\chi)) \cdot (\cos^m 2\psi(\chi) - \cos T)},$$

$$\vartheta_V^{(m)} = \left|\cos^{-1}\left(\frac{1 + \cos^{2m}(2\psi(\chi))\cos T}{\sqrt{2}\sqrt{1 + \cos^{2m}(2\psi(\chi))}}\right).\right|$$

Proof. Straight forward calculations (cf equation (2)). □

Remark. Simple calculation shows that for $m = \mathcal{O}(\sqrt{N/k}) \gg 1$, the following are valid: $\left\|\mathcal{E}_W^m(\rho_s)\right\|_F \to 0$, $\vartheta_W^{(m)} = 0$ for $\chi_n \approx 2\pi n$ when $n \gg 1$. Then, although $\left\|\mathcal{E}_W^m(\rho_s)\right\|_F \to 0$, namely the algorithm fails to radially detect its target, we claim that due to $\vartheta_W^{(m)} = 0$, after $m = \mathcal{O}(\sqrt{N/k})$ queries, the algorithm remains efficient, because in order to find $|x\rangle\langle x|$, it suffices only to determine the direction of its Bloch vector.

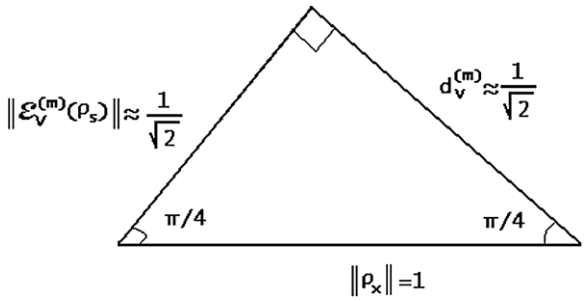


Figure 1. The asymptotic situation depicted in the form of an isosceles orthogonal triangle formed by the norms of the target vector, the search vector and their difference vector after $m = \mathcal{O}(\sqrt{N/k})$ queries.

4. Novel search strategy with the parametric quantum search

What is important is that our analysis so far has shown that the parametric quantum search for all values of parameter χ retain the original algorithms' complexity for finding the marked item(s) i.e. $\mathcal{O}(\sqrt{N/k})$. Indeed, at first, regardless of the choice of the CPTP map, it holds that the algorithm's density matrix always lies in a great circle of the Bloch sphere in the $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$ plane, as occurs in the case of Grover's original algorithm. Next, we observe that, if we choose the map $\mathcal{E}_V$ to be the search operator, with $\chi \notin G_1 \cup G_2$, then, for $m = \mathcal{O}(\sqrt{N/k})$, the quantities $\left\|\mathcal{E}_V^m(\rho_s)\right\|_F$, $d_V^{(m)}$ and $\vartheta_V^{(m)}$ are very close to $\frac{1}{\sqrt{2}}$, $\frac{1}{\sqrt{2}}$ and $\frac{\pi}{4}$ respectively.

In figure 1 the asymptotic situation, namely when $m = \mathcal{O}(\sqrt{N/k})$ and $N \gg 1$, is depicted in the form of an orthogonal and isosceles triangle with the length of the hypotenuse the norm of the wanted density matrix $\|\rho_x\| = 1$, and the vertical sides the norm of the asymptotic density matrix $\left\|\mathcal{E}_V^m(\rho_s)\right\|_F \approx \frac{1}{\sqrt{2}}$, and the norm of their difference

$$\left\|\mathcal{E}_V^m(\rho_s) - \rho_x\right\|_F \equiv d_V^{(m)} \approx \tfrac{1}{\sqrt{2}}.$$

These facts lead us to deduce that, (a) for all $m \in \mathbb{N}$, the current density matrix $\mathcal{E}_V^m(\rho_s)$ does not vanish, so the direction of the current vector $|s^{(m)}\rangle$ remains detectable, and (b) two factors characterize the performance of the parametric algorithm as it is formulated here, namely the *accuracy* of approaching the target and the *number of steps* taken by the algorithm.

The preceding analysis shows that the accuracy is improving sequentially toward the angular bound of $\frac{\pi}{4}$. Therefore if we terminate the search after $m = \mathcal{O}(\sqrt{N/k})$ steps and subsequently the received vector, which is lying in the plane $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$, is plane-rotated clockwise or counter-clockwise by $\frac{\pi}{4}$, the obtained vector will be accepted or rejected as the correct one at the cost of one more additional rectifying question to the oracle. This additional question will not alter the rank of the algorithm complexity chosen i.e. $\mathcal{O}(\sqrt{N/k})$.

Another choice for improving this accuracy while retaining the complexity is to enlarge the size N of the database, as is evident from figure 1.

On the other hand, in figure 2 the plot of the ratio of change of the cosine of angular distance $\cos\vartheta_V^{(m)}$ to the size of database N is presented.

When complexity is kept fixed i.e. of order $\mathcal{O}(\sqrt{N/k})$, the angular accuracy of determining the wanted vector depends on the size N in a manner that according to the plot presents a threshold behavior. This database size threshold shows that above a certain value of N the ratio approaches zero and therefore the angular accuracy reaches its best possible value i.e. $\frac{\pi}{4}$. This implies that the parametric dependence leaves practically unaffected the performance

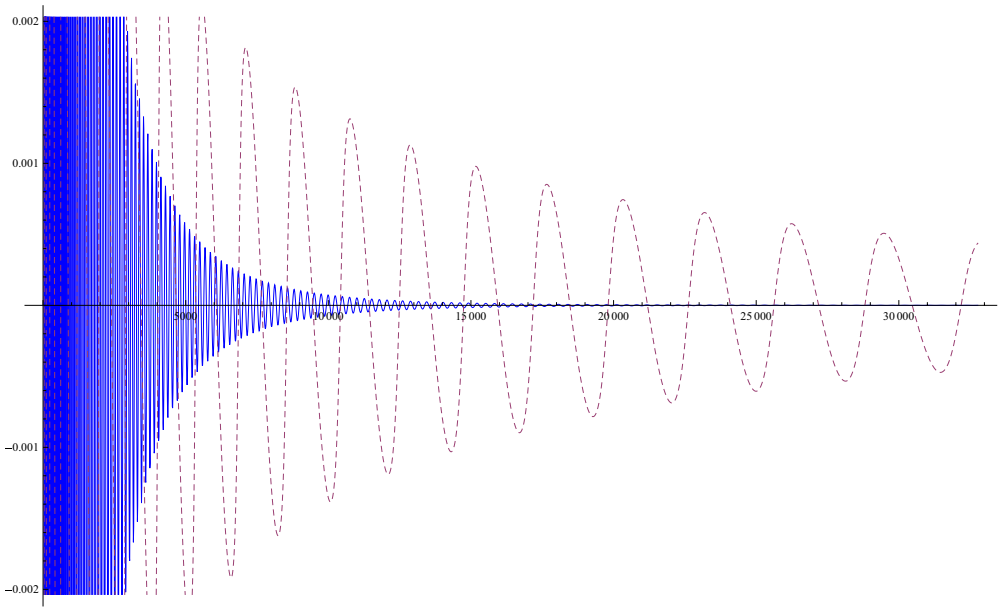


Figure 2. A plot of the ratio of change of cosine of angular distance for: (database size, x-axis), $m = \pi/4\sqrt{N}$ (thick line) and $m = \sqrt{N}$ queries (dashed line), $k = 1$ (one marked item) and $\chi = 0.3$ (parameter).

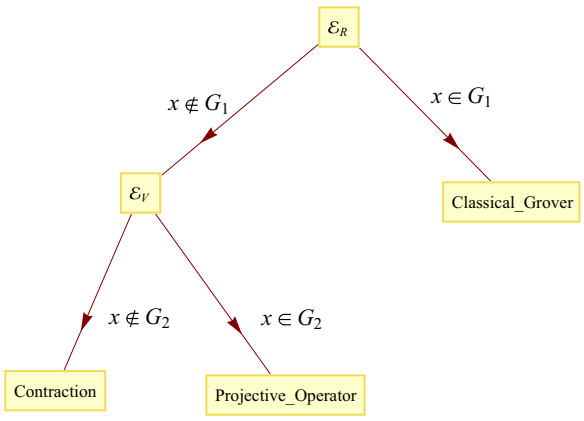


Figure 3. Decision tree for constructing CPTP search maps.

of the algorithms with database sizes beyond the threshold value. To be more precise in the estimation of this threshold value, we can select a tolerance parameter $\Theta \ll 1$, to bound the ratio i.e. $\left|\frac{\partial \cos \vartheta_V^{(m)}}{\partial N}\right| < \Theta$. From the satisfaction of this condition a threshold value of database size Nth is deduced, and then the noisy algorithms that operate with database sizes $N > N$th, with complexity $\mathcal{O}(\sqrt{N/k})$, will determine the target vector up a $\pm\frac{\pi}{4}$ rotation in the plane of the final vector.

In figure 3 a decision tree is presented which summarizes the various possibilities of constructing search maps, depending on the possible positive values taken by the parameter.

The fact illustrated is that for all values of parameter χ there is always a successful search map that, within optimal accuracy restrictions, will be able to provide an answer of equal complexity to that of the original algorithm.

Below we present our search strategy, which is valid for all positive χ, by referring also to the decision tree of search maps.

(a) Construct Kraus generators R_0, R_1.
(b) If the strength of coupling is of the first kind, i.e. $\chi \in G_1$, then the search map $\mathcal{E}_S$ reduces to a unitary matrix and the algorithm returns to its original form.
(c) If otherwise, then construct the map $\mathcal{E}_V$ from $\mathcal{E}_S$ and perform the following steps.
    (1) If the parameter is of the second kind i.e. $\chi \in G_2$, then, according to proposition 1, the density matrix $\mathcal{E}_V^m(\rho_s)$ is projective, i.e. a pure state, and the algorithm is successful after $m = \mathcal{O}(\sqrt{N/k})$ queries.
    (2) If otherwise, namely if $\chi \notin G_1 \cup G_2$, then we cope with the two rival characteristics of the algorithm, namely accuracy and complexity, as follows: select a tolerance value Θ, calculate analytically for $m = \mathcal{O}(\sqrt{N/k})$ the state $\mathcal{E}_V^m(\rho_s)$ and estimate the threshold Nth for which $\left|\frac{\partial \cos \vartheta_V^{(m)}}{\partial N}\right| < \Theta$ is valid. For algorithms with database sizes $N > N$th compute the state's $\mathcal{E}_V^m(\rho_s)$ Bloch vector, in the $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$ plane and rotate it randomly clockwise or counter-clockwise by $\frac{\pi}{4}$ on the same plane, and ask the oracle one more additional question about the correctness of the resulting vector.

In all the above cases the order of magnitude $\mathcal{O}(\sqrt{N/k})$ of the complexity is preserved and within the range of the selected tolerance Θ; the noisy algorithm preserves the quadratic speed of the original one.

The sub-case $c2$, inside the search strategy outlined, suggests the following recipe for finding the threshold of database size Nth: for an algorithm running in databases with size $N > N$th the impact of the parameter is practically negligible. The validity of the recipe concerns the case $\chi \notin G_1 \cup G_2$, and works as follows: after choosing the complexity to be $\mathcal{O}(\sqrt{N/k})$, and since the angular fidelity quantifying the algorithm's performance depends on size N, we choose to work in an asymptotic regime in which this dependence has died out. Practically, this requires that the fidelity's derivative with respect to N becomes smaller than a tolerance parameter Θ. This requirement determines the value of threshold Nth, and when $N > N$th the algorithm locates the target vector up to a plane rotation by $\pm\frac{\pi}{4}$ performed on the Bloch reached at step $m = \mathcal{O}(\sqrt{N/k})$. This recipe can be illustrated by referring to figures 4 and 5.

Indeed, the shaded areas in figures 4 and 5 are defined by points with coordinates (χ, N), which determine algorithms for which the transient dependence of angular fidelity treated as a function of the database size N has been washed out. This can be taken to mean that the derivative of the fidelity with respect to N is practically zero, or more specifically lies below a chosen tolerance parameter Θ, usually taken to be about 10^{-6}. Figures 4 and 5 correspond to the cases of $k = 1$ and $k = 7$ respectively for $\chi \notin G_1 \cup G_2$. In particular, and for the purposes of demonstrating the basic idea, in these figures an interval $\frac{\pi}{2}\sqrt{40} \leqslant \chi \leqslant \frac{\pi}{2}\sqrt{60}$ has been used which does not contain points $\chi \in G_1 \cup G_2$, also $4 \leqslant N \leqslant 2^{10}$. The mentioned operational recipe can be described by means of the figures as follows: for a chosen χ on the horizontal axis an Nth is determined in the lower boundary of the shaded region. This lower boundary consists of threshold sizes Nth, each one being the infimum of the database size, over which the complexity remains practically unaffected by the parameter. Algorithms with such databases can search successfully despite the presence of the non-zero parameter χ.

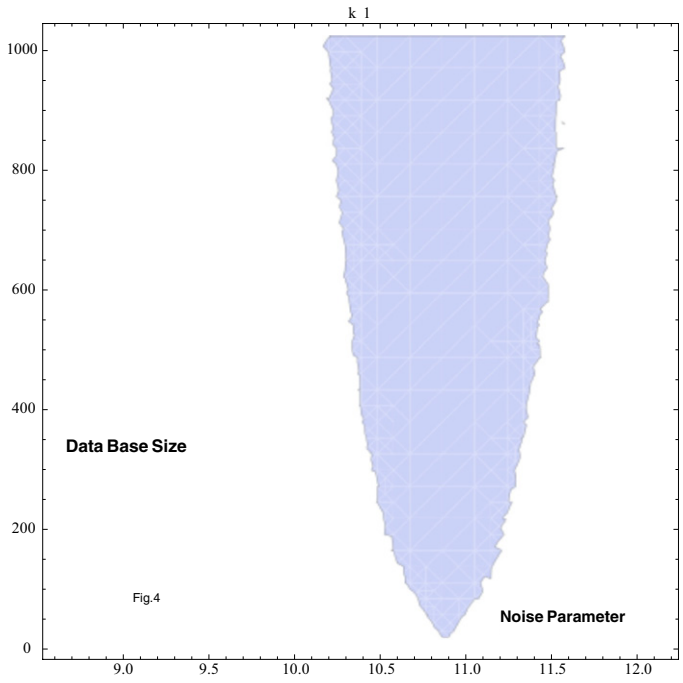


Figure 4. Shaded areas demarcated by χ parameter interval $[\pi/2\sqrt{40}, \pi/2\sqrt{60}]$, and database size in the interval $[4, 2^{10}]$, where their points correspond to algorithms for which the angular fidelity is independent of N with precision bounded by tolerance Θ for the case of $k = 1$

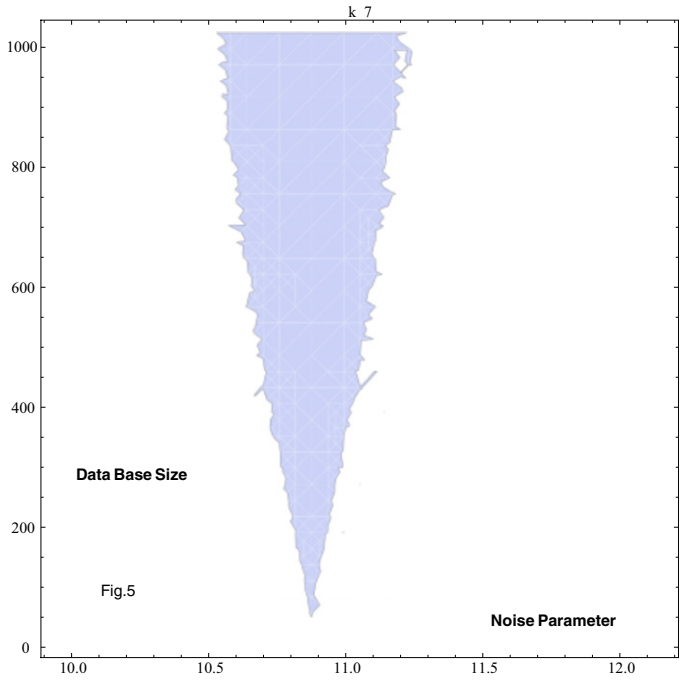


Figure 5. The same as above but for $k = 7$.

Remark. If we choose the value of $\chi \in [0, +\infty)$ at random, the sets G_1, G_2 are of measure zero since they are countably infinite, so $P[\chi \in G_1 \cup G_2] = 0$ and $P[\chi \notin G_1 \cup G_2] = 1$. Therefore, the branch $c2$ of the decision tree is valid almost with certainty.

5. Spherical geodesic and azimuthal symmetry

In this section we are going to show a complementary and important geometrical aspect of quantum search algorithm that relates the reduced complexity with the spherical geodesic motion of the density's matrix 3-vector on the Bloch sphere. To this end, recall that the oracle algebra is endowed with the trace inner product $\langle \cdot, \cdot \rangle = A_f \times A_f \to \mathbb{R}$, defined for any two elements $x, y \in A_f$, as $\langle x, y \rangle := \mathrm{Tr}(xy^\dagger)$. By virtue of this product the success probability reads $p_n = |\langle x|s_n\rangle|^2 = \langle \rho^{(n)}, \rho_x \rangle$ and is written in terms of 3-vectors $\overrightarrow{s}^{(n)}$ and $\overrightarrow{s}^{(x)}$ as

$$\begin{aligned} p_n &= \mathrm{Tr}(\rho^{(n)}\rho_x) = \tfrac{1}{2} + 2\overrightarrow{s}^{(n)} \cdot \overrightarrow{s}^{(x)} \\ &= \tfrac{1}{2} + 2\cos d_{S^2}(\overrightarrow{s}^{(n)} \cdot \overrightarrow{s}^{(x)}). \end{aligned}$$

Function d_{S^2} stands for the spherical geodesic distance between two points determined by radii $\overrightarrow{\alpha}$ and $\overrightarrow{\beta}$ on a sphere S^2, and is the distance of the shortest path along the sphere's surface from $\overrightarrow{\alpha}$ to $\overrightarrow{\beta}$, lying along a great circle, and equals $d_{S^2} = \cos^{-1}(\overrightarrow{\alpha} \cdot \overrightarrow{\beta})$, (for previous works regarding the relation of the quantum search to geodesics see [24, 25]; also for geometric aspects of quantum theory and quantum states, see respectively [26, 27]). The distance d_{S^2}, $(0 \leqslant d_{S^2} \leqslant \pi)$ is determined by the success probability at step n [29],

$$d_{S^2}(\overrightarrow{s}^{(n)} \cdot \overrightarrow{s}^{(x)}) = \cos^{-1}(p_n - 1/2) \tag{3}$$

$$= \cos^{-1}(\tfrac{1}{4}(1 - D_{\mathrm{FS}}(|x\rangle, |s_n\rangle))), \tag{4}$$

where in the last equation the Fubini–Study distance D_{FS} appears. Recall that the Fubini–Study distance $D_{\mathrm{FS}}(|\widetilde{\psi_1}\rangle, |\widetilde{\psi_2}\rangle)$ between two $U(1)$ rays

$$|\widetilde{\psi_i}\rangle = \{\mathrm{e}^{\mathrm{i}\delta_i}|\psi_i\rangle \,|0 \leqslant \delta_i < 2\pi, |\psi_i\rangle \in H\}$$

of the complex projective plane $CP \approx SU(2)/U(1)$, corresponding to vectors $|\psi_i\rangle \in H$, $i = 1, 2$, in Hilbert space H, is defined as

$$D_{\mathrm{FS}}(|\widetilde{\psi_1}\rangle, |\widetilde{\psi_2}\rangle) = \inf_{\delta} || \, |\psi_1\rangle - \mathrm{e}^{\mathrm{i}\delta}|\psi_2\rangle \, ||^2$$

and is equal to

$$D_{\mathrm{FS}}(|\widetilde{\psi_1}\rangle, |\widetilde{\psi_2}\rangle) = 2(1 - |\langle\psi_1|\psi_2\rangle|^2)$$

(see e.g. [28]). Identifying $|\psi_2\rangle \equiv U_G^n|s\rangle \equiv |s_n\rangle$, and $|\psi_1\rangle \equiv |x\rangle$, and denoting the 'transition probability' between these vectors by $p_n = |\langle s_n|x\rangle|^2$, equation (4) is obtained.

Referring to the three related sequences by p_n, $d_{S^2;n}$, $D_{\mathrm{FS};n}$, $n = 0, 1, 2, \ldots$ pertinent to the algorithms that are associated with the success probabilities and with the two geodesic distances in the Bloch sphere S^2 and the projective plane CP respectively, we remark, echoing [26], that the introduction of spherical and projective geometry in our context illustrates how the notions of probability and distance become interlinked, once the quantum search algorithm is formulated in a geometric manner. The geodesic distances with respect to the d_{S^2} and D_{FS} metrics determine the transition probability between the two states and vice versa.

Referring to the Bloch sphere picture of the search algorithm, we note that searching is displayed as a sequence of steps made of small arcs taken on the great circle that joins the initial point with the north pole, which is the end point of the Bloch vector associated with the wanted item. The order of magnitude of the number of such steps is identified with the

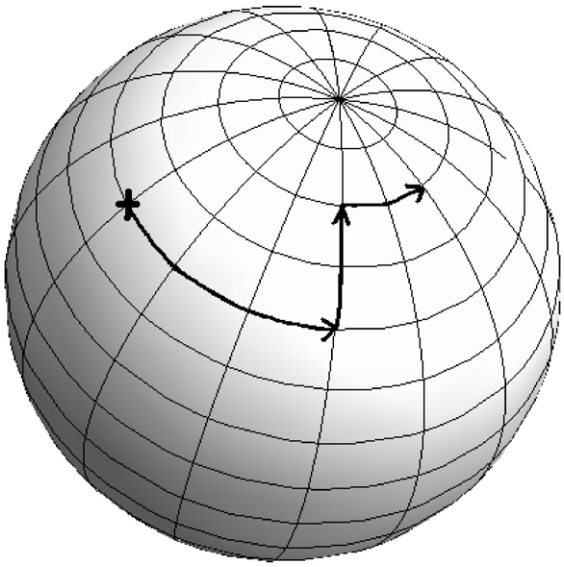


Figure 6. Display of Bloch sphere and the circle of points with equal spherical distance from N, and also the azimuthal and a polar arc.

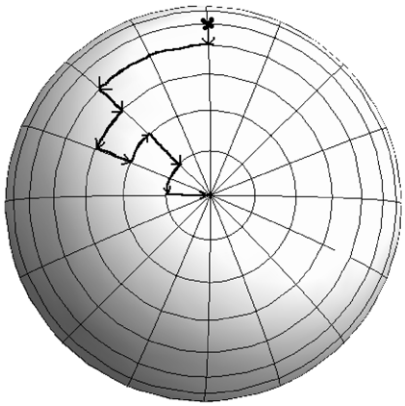


Figure 7. Display of a zigzag search trajectory as seen from a point of view lying over the north pole; the total of nine steps before reaching the pole contains four azimuthal and five polar arcs.

complexity. This geometrical picture actually motivates the finding of a hidden symmetry of the search algorithm as follows: referring to figure 6 we consider the circle C_I which is the locus of points having constant spherical distance from the north pole.

Circle C_I contains the end point I of the Bloch vector associated with initial ρ_{ss}, and it is parallel to the equator. If we allow for interruptions in the trajectory of searching from point I to the north pole $\mathcal{N}$, in the form of arcs on circles parallel and interior to the circle C_I, then a piece-wise continuous trajectory will be formed. This trajectory is constituted by arcs with constant polar distance (*polar arcs*), or with constant azimuthal distance (*azimuthal arcs*), from the north pole. Since the polar arcs do not change the polar distance from $\mathcal{N}$, they are of zero computational cost. In fact, according to our previously stated definition, the complexity refers only to the number of azimuthal arcs needed to reach the pole. In figure 7 an example

of such a zigzag search trajectory is displayed, which is made of nine steps in total, of which only five are azimuthal and count in the complexity.

This symmetry of the algorithm will be called *azimuthal symmetry* hereafter and will be formalized as follows. Recall that any density matrix in the course of searching has the Bloch vector along axes $\widetilde{\Sigma}_1$, $\widetilde{\Sigma}_3$ i.e. $\rho = a\Sigma_1 + b\Sigma_3$, and also that the search unitarity is $U_G = \exp(\mathrm{i}\phi\Sigma_2)$; therefore any rotation of ρ that generates a non-zero component along the $\widetilde{\Sigma}_2$ axis i.e.

$$\begin{aligned}\rho \to \rho' &\equiv \mathrm{e}^{\mathrm{i}\gamma\Sigma_3}\rho\,\mathrm{e}^{-\mathrm{i}\gamma\Sigma_3} \equiv V_3(\gamma)\rho V_3(\gamma)^\dagger \\ &= (\cos\gamma)a\Sigma_1 + b\Sigma_3 + (\sin\gamma)\Sigma_2,\end{aligned}$$

yields a density which has its Σ_3 component preserved, and the projection along the wanted projector $|x\rangle\langle x|$ is also preserved i.e. $\mathrm{Tr}(|x\rangle\langle x|\rho) = \mathrm{Tr}(|x\rangle\langle x|\rho')$, due to the fact that $\mathrm{Tr}(|x\rangle\langle x|\Sigma_2) = 0$. This implies that the complexity of a search performing only azimuthal arcs via U_G for α times, equals the complexity of the search that contains an equal number of azimuthal arcs, which however may be interrupted by any number of polar arcs, where polar arcs are implemented by the action of $V_3(\gamma)$. This equality of complexities is expressed in terms of the minimization of the projection of the time-evolved density matrix on the density matrix of a marked item i.e.

$$\begin{aligned}1 &= \min_\alpha \langle x|U_G^\alpha \rho_{ss} U_G^{\alpha\dagger}|x\rangle \\ &= \min_\alpha \langle x|U_G^{\alpha_1} V_3(\gamma)U_G^{\alpha_2}\ldots V_3(\gamma)U_G^{\alpha_r}\rho_{ss}(U_G^{\alpha_1}V_3(\gamma)U_G^{\alpha_2}\ldots V_3(\gamma)U_G^{\alpha_r})^\dagger|x\rangle,\end{aligned}$$

where $\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_r$.

6. Invariances in the parametric quantum search

In this final chapter we are going to study some underlying invariances of the PQSA. These invariances are due to the symmetry algebra A_f, that has been shown to generate the evolution of the density matrix. Firstly, we construct the general invariant CP map that admits the algorithm's density matrix as a fixed point. In addition, we study the affine transformation induced from the invariant CP map upon the density matrix Bloch vector, and determine its free parameters and the geometry of their set. Also working within the space $\mathcal{V}_x$, we determine the position of the search map $\mathcal{E}_V$ in a tetrahedron displaying unital qubit maps. Secondly, we show that there is a certain time invariant *positional structure* in the density matrix, both in the unitary and in the CP map case.

First we need to recall the following two characterizations of CP maps acting on qubits.

(i) In the Pauli matrix basis a density matrix is written as $\rho = \frac{1}{2}(\mathbf{1}_2 + \vec{w}\cdot\vec{\sigma})$ where $\vec{w} \in \mathbb{R}^3$ and $|\vec{w}| \leqslant 1$. Recall also that any CPTP map $\mathcal{E}_{\Lambda,t} : \mathcal{M}(\mathbb{C}^2) \to \mathcal{M}(\mathbb{C}^2)$, can be represented in the $\{\mathbf{1}, \vec{\sigma}\}$ basis by a unique 4×4 matrix $E_{\Lambda,t} = \left(\begin{smallmatrix}1 & 0\\ t & \Lambda\end{smallmatrix}\right)$, where $\Lambda \in \mathbb{R}^{3\times 3}$, $t \in \mathbb{R}^{3\times 1}$, which induces an affine transformation in the Bloch vector viz. $\mathcal{E}_{\Lambda,t}(w_0\mathbf{1} + \vec{w}\cdot\vec{\sigma}) = w_0\mathbf{1} + (\Lambda\vec{w} + t)\cdot\vec{\sigma}$.

The matrix elements of $E_{\Lambda,t}$ are determined via a trace inner product $\langle\cdot,\cdot\rangle = A_f \times A_f \to \mathbb{R}$, defined as $\langle x, y\rangle := \frac{1}{2}\mathrm{Tr}(xy^\dagger)$ on elements $x, y \in A_f$. Explicitly, $E_{\alpha\beta} := \langle\sigma_\alpha, \mathcal{E}(\sigma_\beta)\rangle = \frac{1}{2}\mathrm{Tr}(\sigma_\alpha\mathcal{E}(\sigma_\beta))$, for some map$\mathcal{E}$, and E is its associated matrix. Matrix E has an SVD decomposition $E = UDW^\dagger$, with D an (almost) diagonal matrix. In cases like ours with map $\mathcal{E}_V$ with unitary Kraus generators, Λ is orthogonal and is taken to be diagonal with eigenvalues $\lambda \equiv \{\lambda_1, \lambda_2, \lambda_3\}$,i.e. $\mathcal{E}_{\Lambda,t} \to \mathcal{E}_{(\lambda,t)}$, where $\Lambda = diag(\lambda)$. As

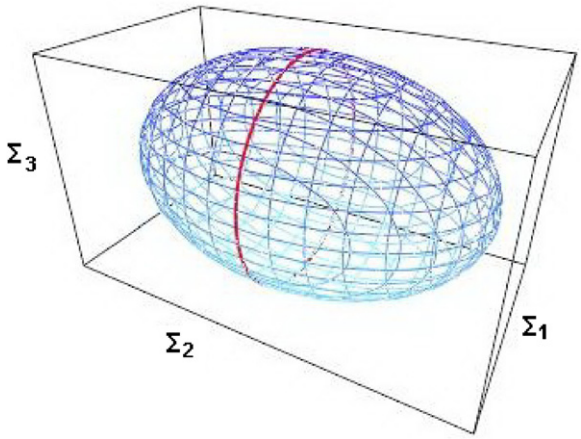


Figure 8. The ellipsoid as the image of the pure state density matrix under the action of a CP map with $\chi = 5.4$, and $k = 1$ wanted items .

a result map $\rho \to \mathcal{E}_{(\lambda,t)}(\rho)$ induces on the column formed by the Bloch vector components $(\frac{1}{2}, \frac{1}{2}s_1, \frac{1}{2}s_3, \frac{1}{2}s_3)$ of matrix ρ, an affine transformation via matrix

$$E_{(\lambda,t)} = \begin{pmatrix} 1 & & & \\ t_1 & \lambda_1 & & \\ t_2 & & \lambda_2 & \\ t_3 & & & \lambda_3 \end{pmatrix}.$$

Geometrically, the image of pure density matrices ρ, i.e. the image of the Bloch sphere $s_1^2 + s_2^2 + s_3^2 = 1$, under the action of $\mathcal{E}_{(\lambda,t)}$, is a displaced ellipsoid with equation

$$\frac{(s_1 - t_1)^2}{\lambda_1^2} + \frac{(s_2 - t_2)^2}{\lambda_2^2} + \frac{(s_3 - t_3)^2}{\lambda_3^2} = 1;$$

see also figure 8.

(ii) A geometric picture for unital CPTP maps on qubits arising from the necessary condition for complete positivity, which reads $|\lambda_1 \pm \lambda_2| \leqslant |1 \pm \lambda_3|$, where $\lambda_1, \lambda_2, \lambda_3$ are the eigenvalues of matrix Λ in map $\mathcal{E}$, see [31] (for proofs and generalizations to non-unital maps, see [30–32]). Positive maps are identified with points in $\mathbb{R}^3$, with the coordinates $\{\lambda_1, \lambda_2, \lambda_3\}$. Then the geometrical meaning of the four inequalities above determines a regular tetrahedron [30, 33–35]. Each one of the four equalities $|\lambda_1 + \lambda_2| = |1 + \lambda_3|$, $|\lambda_1 - \lambda_2| = |1 - \lambda_3|$ is a plane on which the triangular faces of the regular tetrahedron are lying, and also the vertices have the coordinates

$$(1, 1, 1), (1, -1, -1), (-1, 1, -1), (-1, -1, 1).$$

Since for positive maps $|\lambda_i| \leqslant 1$, $i = 1, 2, 3$, then these maps are contained in a unit cube, and the CP unital maps are lying inside the tetrahedron or on its faces or edges.

Along the lines of the previously outlined geometric theory for maps, we now turn to the geometric characterization of the search map $\mathcal{E}_V$, as well as of the symmetric CP map of the density matrix valid for both the quantum unitary search and the parametric search. The symmetric CP map refers to a map that leaves invariant the density matrix of the algorithm. Recall that the algorithm's density matrix has a Bloch vector lying in the $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$ plane, both in the unitary case, when evolution is driven by AdU_G, and in the non-unitary case, when evolution is driven by $\mathcal{E}_V$.

Definition. *Let ρ be the density matrix of the search algorithm and let $\pi_n(\rho)$ be its n-dimensional representation. Map $\mathcal{E}$ is an invariant CPTP map iff $\mathcal{E}(\pi_n(\rho)) = \pi_n(\rho)$ i.e. $\pi_n(\rho)$ is admitted as a fixed point from any invariant map.*

For $\mathcal{E}_V$ it is true that

$$\mathcal{E}_V^m(\pi_n(\rho_s)) = \left(\frac{1}{2^m}\sum_{r=0}^{m}\binom{m}{r} Ad\left(W_{r,m}\right)\right)\pi_n(\rho_s),$$

with $W_{r,m} = \exp\{\mathrm{i}[(-2r\psi(\chi) + m(\pi + \chi - \theta)]\pi_n(\Sigma_2)\}$, and that it retains the initial density matrix in the $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$ plane, i.e. for $m \in \mathbb{N}$

$$\mathcal{E}_V^m(\pi_n(\rho_s)) = \tfrac{1}{2}\pi_n(\Sigma_0) + s_1^{(m)}\pi_n(\Sigma_1) + s_3^{(m)}\pi_n(\Sigma_3),$$

where

$$s_1^{(m)} = \tfrac{-1}{2}\cos^m(2\psi(\chi))\sin(2\psi(\chi)m - 2m\chi - 2a + 2m\theta)$$
$$s_3^{(m)} = \tfrac{1}{2}\cos^m(2\psi(\chi))\cos(2\psi(\chi)m - 2m\chi - 2a + 2m\theta)$$

and $a = \cos^{-1}(\sqrt{\frac{k}{N}})$. An immediate consequence of the definition and these properties is as follows.

Proposition 6. *An invariant search CP map $\mathcal{E}$ for $\pi_n(\rho)$, is associated with a matrix $E_{(\lambda,t)}$ with parameters $t_1 = t_3 = 0$, $\lambda_1 = \lambda_3$, and $1 = \frac{1}{\lambda_1^2} + \frac{t_2^2}{\lambda_2^2}$. The set of all such invariant maps is $E \equiv \{E_{(\lambda,t)}, \lambda_1, \lambda_2, \lambda_3, t_1, t_2, t_3 \in \mathbb{R}^6 \mid t_1 = t_3 = 0, \lambda_1 = \lambda_3$ and $\frac{1}{\lambda_1^2} + \frac{t_2^2}{\lambda_2^2} = 1\}$.*

Proof. First, recall that in the n-dimensional representation, the pure density matrix in Grover's original algorithm read

$$\pi_n(\rho_s) = |s\rangle\langle s| = \tfrac{1}{2}\pi_n(\Sigma_0) + s_1^{(0)}\pi_n(\Sigma_1) + s_1^{(0)}\pi_n(\Sigma_3)$$

(for the sake of simplicity we will use the notation ρ and $\Sigma_{1,2,3}$) with the Bloch vector components $(s_1^{(0)}, s_2^{(0)}, s_3^{(0)})$, where

$$s_1^{(0)} = \frac{\sqrt{k(N-k)}}{N}, \quad s_2^{(0)} = 0, \quad s_3^{(0)} = -\frac{N-2k}{2N}.$$

Since $\mathcal{E}(\rho) = \rho = \frac{1}{2}\Sigma_0 + s_1^{(0)}\Sigma_1 + s_3^{(0)}\Sigma_3$ and ρ's Bloch vector endpoint is lying on a circle (C) in the $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$ plane, then $\mathcal{E}(\rho)$'s Bloch vector endpoint is lying on a circle (C'), equal to (C), in a plane parallel to the $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$ plane. Therefore, for the displaced ellipsoid mentioned above, we have that its first and third semi-axes (on the $\widetilde{\Sigma}_1$ and $\widetilde{\Sigma}_3$ axes respectively) are of equal length, i.e. $\lambda_1 = \lambda_3$, and moreover, for the same reason, there is no displacement along the $\widetilde{\Sigma}_1$ and $\widetilde{\Sigma}_3$ axes. So, the ellipsoid is centered at some point $(0, t_2, 0)$, namely $t_1 = t_3 = 0$.

Finally, due to all the above, the image of the pure density matrix, under the action of the invariant CP map $\mathcal{E}$, will become

$$\frac{\left(s_1^{(0)} - 0\right)^2}{\lambda_1^2} + \frac{\left(s_2^{(0)} - t_2\right)^2}{\lambda_2^2} + \frac{\left(s_3^{(0)} - 0\right)^2}{\lambda_3^2} = 1, \quad \text{i.e.} \frac{1}{\lambda_1^2} + \frac{t_2^2}{\lambda_2^2} = 1.$$

All these also identify the set E and complete the proof. □

Geometrically, for any given t_2, the invariance set E is determined by parameters lying in the intersection of the cross curve cylinder $\frac{1}{\lambda_1^2} + \frac{t_2^2}{\lambda_2^2} = 1$, with the plane $\lambda_1 = \lambda_3$. (Recall that the Cartesian equation of a plane cross curve is $\frac{a^2}{x^2} + \frac{b^2}{y^2} = 1$.) The set E as a family of these

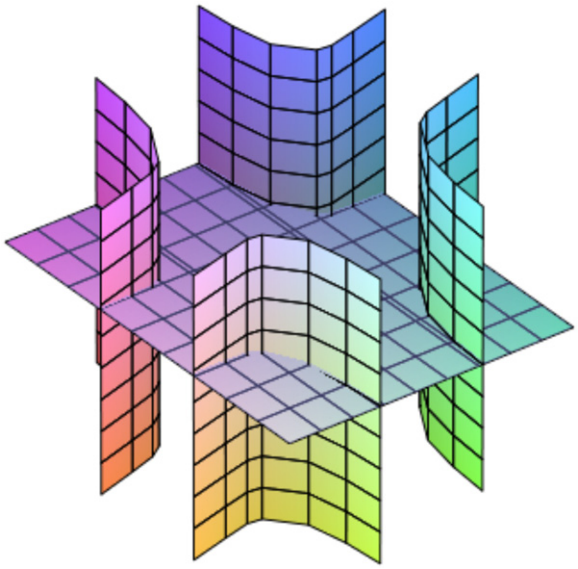


Figure 9. The cross curve which occurs as the intersection of the cross cylinder with the plane (see text).

intersections parametrized by t_2 is presented in figure 9. Note that the intersection marked with $t_2 = 0$ concerns the unital maps $\mathcal{E}(\mathbf{1}) = \mathbf{1}$, for which $\overrightarrow{t} = 0$, i.e. the transformation of the Bloch vector is not an affine one.

Our map $\mathcal{E}_V$ is unital but is of course not invariant, therefore, as with respect to the tetrahedron picture of the qubit CP maps, we find that by varying its free parameter χ, its representing point covers a line segment on one of the edges of the tetrahedron; see figure 10 where the corresponding line segment (for the $k = 1$ item and $\phi = \frac{\pi}{4}$) is extended from A to M. This can be easily proved, since for any $0 \leqslant p \leqslant 1$ the eigenvalues of $\mathcal{E}_V = pAd(V_0 J_s V_0^\dagger J_x) + (1-p)Ad(V_1 J_s V_1^\dagger J_x)$ are $\lambda_1 = \lambda_2 = 1 + 2p(p-1)(1-\cos(\psi(\chi)))$, $\lambda_3 = 1$.

We now turn to the second kind of invariance exhibited by the algorithm. To account for the manifested *positional invariance* shared by the density matrix during the course of searching we introduce the following three symbols: ★, ■, and ▼ (for explicit values see below).

Referring to the displays for the density matrix below, we see a 'cross' filled in with equal matrix elements of three types of symbols. Explicitly the ■ element fills the horizontal and vertical lines of the 'cross', and the intersection of them is filled by symbol ★, and all remaining places are filled by the symbol ▼, (see the display in equation (6)). Note also that the symbol ★ occupies a position identified with the non-zero components of the marked vectors.

This structure persistently re-appears in any version of the algorithm: closed and open, of one and of many marked items (see display 5 for one item and display 6 for the two-item case). The thickness of the 'cross' is determined by k, the number of marked items. This pattern is a manifestation of the algebraic invariance of the algorithm which, in terms of the oracle algebra, implies that only the Σ_1, Σ_3 components of the Bloch vector are non-zero, and which is tantamount to saying that only matrices $\pi_n(\Sigma_1)$, $\pi_n(\Sigma_3)$ are used in the expression of the density matrix.

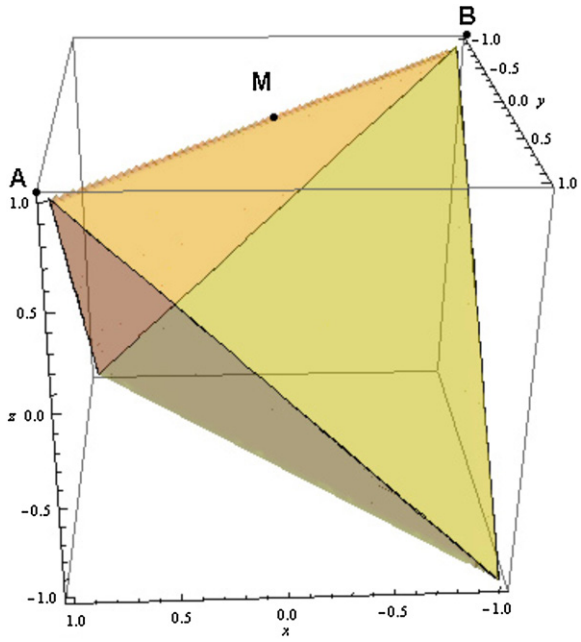


Figure 10. The eigenvalues are along the line segment AM , where A(1,1,1), B(−1,−1,1), are vertices of the regular tetrahedron, and M is the midpoint of the edge AB.

Below we provide displays of the density matrix $\mathcal{E}_V^m(\pi_n(\rho_s))$ for $n = N$, $k = 1$ and $k = 2$, with the following values (see equations (5),(6))

$$k=1 \quad \bigstar = \frac{3}{2} \quad \blacksquare = \frac{1}{\sqrt{N-1}} s_1^{(m)} \quad \blacktriangledown = \frac{1}{N-1}\left(\frac{1}{2} - s_3^{(m)}\right)$$
$$k=2 \quad \bigstar = 1 \quad \blacksquare = \frac{1}{\sqrt{N-2}} s_1^{(m)} \quad \blacktriangledown = \frac{1}{N-2}\left(\frac{1}{2} - s_3^{(m)}\right).$$

The $k = 1$ marked item:

$$\mathcal{E}_V^m(\pi_N(\rho_s)) = \begin{pmatrix} \bigstar & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \cdots \\ \blacksquare & \blacktriangledown & \blacktriangledown & \blacktriangledown & \blacktriangledown & \blacktriangledown & \cdots \\ \blacksquare & \blacktriangledown & \blacktriangledown & \blacktriangledown & \blacktriangledown & \blacktriangledown & \cdots \\ \blacksquare & \blacktriangledown & \blacktriangledown & \blacktriangledown & \blacktriangledown & \blacktriangledown & \cdots \\ \blacksquare & \blacktriangledown & \blacktriangledown & \blacktriangledown & \blacktriangledown & \blacktriangledown & \cdots \\ \blacksquare & \blacktriangledown & \blacktriangledown & \blacktriangledown & \blacktriangledown & \blacktriangledown & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}. \tag{5}$$

The $k = 2$ marked items:

$$\mathcal{E}_V^m(\pi_N(\rho_s)) = \frac{1}{2}\begin{pmatrix} \blacktriangledown & \blacktriangledown & \blacksquare & \blacksquare & \blacktriangledown & \blacktriangledown & \blacktriangledown \\ \blacktriangledown & \blacktriangledown & \blacksquare & \blacksquare & \blacktriangledown & \blacktriangledown & \blacktriangledown \\ \blacksquare & \blacksquare & \bigstar & \bigstar & \blacksquare & \blacksquare & \blacksquare \\ \blacksquare & \blacksquare & \bigstar & \bigstar & \blacksquare & \blacksquare & \blacksquare \\ \blacktriangledown & \blacktriangledown & \blacksquare & \blacksquare & \blacktriangledown & \blacktriangledown & \blacktriangledown \\ \blacktriangledown & \blacktriangledown & \blacksquare & \blacksquare & \blacktriangledown & \blacktriangledown & \blacktriangledown \\ \blacktriangledown & \blacktriangledown & \blacksquare & \blacksquare & \blacktriangledown & \blacktriangledown & \blacktriangledown \end{pmatrix}. \tag{6}$$

Compare these with the similar displays for the case of the zero $\chi = 0$ quantum search in [36, 37].

7. Conclusions

The aim of this work is to introduce a novel version of the search algorithm in which the unitarity of the original algorithm is relaxed and replaced by a map operating in the density matrix space. Within this new framework, the work addresses some novel algebraic and geometric properties (symmetries) of the search algorithm, with or without the influence of external quantum noise. The choice of model for quantum noise, though not dictated by some realistic physical situations is instead able to highlight a mathematical methodology that is considered useful for studying the quantum search as well as other quantum algorithms where quantum noise must be taken into account in both qualitative and quantitative terms. These specific choices explain the name 'toy model' chosen for the PQSA.

Important points of the PQSA investigated here are:

(a) the introduction and study of the properties of the *oracle algebra*, manifesting the underlying $SU(2)$ symmetry of the algorithm;
(b) the unitary preconditioning of the Kraus generator of the underlying CPTP search map in the presence of quantum parametric noise, having as a consequence the *symmetry breaking* effect, from $SU(2)$ to $U(1) \oplus U(1)$;
(c) the manifested algorithm's *robustness*, proved for a sequence of values of the noise parameter, and the possibility of further basing on this robustness the formulation of a *novel search strategy*; this strategy, though not valid universally for databases of any size, actually determines the infima of the database sizes over which the PQSA performs accurately with the complexity $\mathcal{O}(\sqrt{N})$;
(d) the proof of the algorithm's *azimuthal symmetry*, manifested in the Bloch sphere picture of the model, enabled by the oracle algebra;
(e) the *positional invariance* of the density matrix for the search quantum system, a property also attributed to the oracle algebra and its higher-dimensional representation.

Closing, we should remark that the PQSA as formulated here may provide fruitful links to other open quantum system algorithms and models that similarly outperform their classical rivals in several tasks, as for example is the case of quantum walks; along these lines a first step has been undertaken in [39].

Acknowledgments

One of us (ChK) acknowledges a PhD Scholarship from the Technical University of Crete.

Appendix. Oracle algebra $N = 8$ $k = 2$

In this appendix we give explicitly the matrix representation of the oracle algebra generators and of the partial units in marked/unmarked subspaces, for dimension $N = 8$. To empasize the structure of the matrices and their similarity to Pauli matrices zero elements are omitted. The marked items/vectors are taken to be $k = 2$, and to occupy the first two positions in the database set Δ, i.e. the first two vectors $|1\rangle$, $|2\rangle$, in the canonical basis of the database vector space D.

$$\pi_8(\mathbf{1}) = \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{pmatrix},$$

$$\pi_8(\mathbf{1}_{k=2}) = \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \end{pmatrix}, \quad \pi_8(\mathbf{1}_{N-k=6}) = \begin{pmatrix} & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{pmatrix},$$

$$\pi_8(\Sigma_0) = \begin{pmatrix} 11 & & \\ 11 & & \\ & 111111 & \\ & 111111 & \\ & 111111 & \\ & 111111 & \\ & 111111 & \\ & 111111 & \end{pmatrix}, \quad \pi_8(\Sigma_1) = \begin{pmatrix} & 111111 & \\ & 111111 & \\ 11 & & \\ 11 & & \\ 11 & & \\ 11 & & \\ 11 & & \\ 11 & & \end{pmatrix},$$

$$\pi_8(\Sigma_3) = \begin{pmatrix} 11 & & \\ 11 & & \\ & 111111 & \\ & 111111 & \\ & -111111 & \\ & 111111 & \\ & 111111 & \\ & 111111 & \end{pmatrix}, \quad \pi_8(\Sigma_2) = \begin{pmatrix} & -i111111 & \\ & 111111 & \\ 11 & & \\ 11 & & \\ i11 & & \\ 11 & & \\ 11 & & \\ 11 & & \end{pmatrix}.$$

References

[1] Grover L 1997 *Phys. Rev. Lett.* **79** 325
[2] Grover L 1996 *Proc. 28th Annu. ACM Symp. on the Theory of Computing* (New York: ACM) pp 212–8
[3] Zalka C 1999 *Phys. Rev.* A **60** 2746
[4] Boyer M, Brassard G, Hoyer P and Tapp A 1996 *Proc. 4th Workshop on Physics and Computation* pp 36–43
[5] Grover L 1998 *Phys. Rev. Lett.* **80** 4329
[6] Mosca M 2009 *Quantum Algorithms (Springer Encyclopaedia and Systems Science)* (New York: Springer)
[7] Hoyer P, Mosca M and de Wolf R 2003 *ICALP'03: International Colloquium on Automata, Languages and Programming* (*Lecture Notes in Computer Science* vol 2719) (New York: Springer) pp 291–9
[8] Magniez F, Nayak A and Roland J 2007 *STOC'07: Proc. Symp. on the Theory of Computing* pp 575–83
[9] Shenvi N, Brown K R and Whaley K B 2003 *Phys. Rev.* A **68** 052313
[10] Fang Y, Kaszlikowski D, Chin C, Tay K, Kwek L C and Oh C H 2005 *Phys. Lett.* A **345** 265
[11] Davies E B 1976 *The Quantum Theory of Open Systems* (London: Academic)
[12] Breuer H P and Petruccione F 2002 *The Theory of Open Quantum Systems* (Oxford: Oxford University Press)
[13] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)

[14] Choi M D 1975 *Linear Algebra Appl.* **10** 285
[15] Kraus K 1983 *States, Effects and Operations* (Berlin: Springer)
[16] Chuang I L and Yamamoto Y 1997 *Phys. Rev.* A **55** 114
[17] Ellinas D and Konstandakis Ch 2004 *AIP Conf. Proc.* **734** 179
[18] Konstandakis Ch 2007 Quantum search algorithms in un-shorted databases *MSc Thesis* Technical University of Crete (in Greek)
[19] Farhi E and Gutmann S 1998 *Phys. Rev.* A **57** 2403
[20] Horn R A and Johnson C R 1990 *Matrix Analysis* (Cambridge: Cambridge University Press)
[21] Alicki R and Lendi K 1987 *Quantum Dynamical Semigroups and Their Applications* (Berlin: Springer)
[22] Jozsa R 1999 arXiv:quant-ph/9901021v1
[23] Ellinas D and Konstandakis Ch 2011 *AIP Conf. Proc.* **1363** 73
[24] Alvarez J J and Gomez C 2000 arXiv:quant-ph/9910115
[25] Miyake A and Wadati M 2001 *Phys. Rev.* A **64** 042317
[26] Brody D C and Hughston L P 2001 *J. Geom. Phys.* **38** 19
[27] Zyczkowski K and Słomczynski W 2001 *J. Phys. A: Math. Gen.* **34** 6689
[28] Ellinas D 1994 On coherent states and q-deformed algebras *Proc. Int. Symp. on Coherent States: Past, Present and Future (Oak Ridge, USA, 1993)* ed D H Feng, J R Klauder and M R Strayer (Singapore: World Scientific) pp 139–51
[29] Pressley A 2010 *Elementary Differential Geometry* 2nd edn (London: Springer) chapter 6.5
[30] Li Oi D K 2001 arXiv:quant-ph/0106035v1
[31] King C and Ruskai M B 2001 *IEEE Trans. Inform. Theory* **47** 192
[32] Fujiwara A and Algoet P 1999 *Phys. Rev.* A **59** 3290
[33] Pasieka A, Kribs D W, Laflamme R and Pereira R 2009 *Acta Applicandae Math.* **108** 697
[34] Ruskai M B, Szarek S and Werner E 2002 *Linear Algebra Appl.* **347** 159
[35] Horn A 1954 *Am. J. Math.* **76** 620
[36] Fang Y, Kaszlikowski D, Chin C, Tay K, Kwek L C and Oh C H 2005 *Phys. Lett.* A **345** 265
[37] Cui J and Fan H 2010 *J. Phys. A: Math. Theor.* **43** 045305
[38] Ambainis A 2004 *ACM SIGACT* **35** 22
[39] Ellinas D and Konstandakis Ch 2013 Parametric quantum search algorithm as quantum walk: a quantum simulation, in preparation

Entropy **2015**, *17*, 4838-4862; doi:10.3390/e17074838

OPEN ACCESS
entropy
ISSN 1099-4300
www.mdpi.com/journal/entropy

Article

Faster Together: Collective Quantum Search

Demosthenes Ellinas * and Christos Konstandakis

Department of Electronic & Computer Engineering, QLab, Technical University of Crete, GR 731 00 Chania Crete, Greece; E-Mail: konstandakis@science.tuc.gr

* Author to whom correspondence should be addressed; E-Mail: ellinas@ece.tuc.gr.

Academic Editor: Kevin H. Knuth

Received: 8 May 2015 / Accepted: 30 June 2015 / Published: 10 July 2015

Abstract: Joining independent quantum searches provides novel collective modes of quantum search (merging) by utilizing the algorithm's underlying algebraic structure. If n quantum searches, each targeting a single item, join the domains of their classical oracle functions and sum their Hilbert spaces (merging), instead of acting independently (concatenation), then they achieve a reduction of the search complexity by factor $\mathcal{O}(\sqrt{n})$.

Keywords: quantum search algorithm; search complexity; Young diagram; completely positive trace preserving maps; quantum channels.

PACS classifications: 03.67.Lx

1. Introduction

The quantum search algorithm, from its initial conception [1–3], to the subsequent manifold of ongoing developments, see e.g., the various open research projects addressing the association of quantum search with e.g., quantum entanglement [4], quantum programming [5], error faultiness [6], fixed-point quantum search [7], and quantum walks [8], constitutes one of the pillars of the research area of quantum computing. Despite its simplicity and the manifested versatility in applications the algorithm remains a challenge to meet, especially when it is considered as a computational primitive that could be synthesized in non trivial ways with itself.

This point of view is put forward in this work, where utilizing the underlying algebraic structure of the search algorithm and its matrix representation theory [9], the algorithm is treated as a computational unit

composed in two different ways, to be called *merging* and *concatenation*. Merging of two algorithms creates a computational advantage that reduces search complexity in contradistinction to non joint searches of simple concatenation. More accurately, it is shown that the merging of n single searches with database dimensions $N_k = 2^k$, $k = 1, ..., n$, causes a complexity reduction proportional of square root of n. This main result of collective search is scrutinized in all intermediated joining schemes, where among n searches k are merged and the rest are left concatenated, via partitioning databases into distinct groups of merged algorithms and then concatenating the resulting groups. The logistics of joining schemes is carried out via Young diagrams and tableaux of partitions, as well as majorization theory [10]. (Proofs and examples are placed in the second part of the paper).

1.1. Single Quantum Search

Find $1 \leq k < N$ marked elements from the set $\Delta = \{1, 2, ...N\}$, by improving the classical complexity $\mathcal{O}(N)$ of the search.

The ν binary strings $(a_1, a_2, ..., a_\nu)$ form the elements of classical database with size $N = 2^\nu$, which are assigned via $(a_1, a_2, ..., a_\nu) \rightarrow |a_1, a_2, ..., a_\nu\rangle \equiv |i\rangle$, $i = 1, ..., N$, to N basis vectors of Hilbert space $H = (span\{|0\rangle, |1\rangle\})^{\otimes\nu}$. Via the assignment $|i\rangle \rightarrow |i\rangle\langle i|$, this leads to the database $\Pi = \{|i\rangle\langle i|\}_{i=1}^N = \{\rho_i\}_{i=1}^N \approx l_2(\Delta)/U(1)$ consisting of a collection of N pure density matrices. Let the oracle function f, introduced as the characteristic function of subset $I \subset \Delta$ of marked items, namely $f(i) = 1$ for $i \in I$ and $f(i) = 0$ for $i \notin I$. The density matrices ρ_x, ρ_s, for the marked and initial vectors are expressed in terms of vectors $|x\rangle$, $|x^\perp\rangle$, and $|s\rangle = \frac{1}{\sqrt{N}}\sum_{i=1}^N |i\rangle$, where $|x\rangle$ and $|s\rangle$, are the the solution state and the equiprobable superposition of all database states, respectively. Define the reflection operators $J_x = \mathbf{1} - 2|x\rangle\langle x|$, $J_s = \mathbf{1} - 2|s\rangle\langle s|$, and the unitary search operator $U_G = -J_s J_x$, that implements a search via the action $\rho \rightarrow U_G \rho U_G^\dagger$. Next, introduce the $\Sigma_0, \Sigma_1, \Sigma_2$ and Σ_3 as the Hermitian generators of oracle algebra A_f [9],

$$\begin{aligned} \Sigma_1 &= |x\rangle\langle x^\perp| + |x^\perp\rangle\langle x|, \quad \Sigma_2 = -i|x\rangle\langle x^\perp| + i|x^\perp\rangle\langle x|, \\ \Sigma_3 &= |x\rangle\langle x| - |x^\perp\rangle\langle x^\perp|, \quad \Sigma_0 = |x\rangle\langle x| + |x^\perp\rangle\langle x^\perp|, \end{aligned}$$

with commutation relations $[\Sigma_\alpha, \Sigma_b] = 2i\Sigma_c$ (cyclically), $a, b, c \in \{0, 1, 2, 3\}$, and Σ_0 central, *i.e.*, $A_f \approx u(2)$ (see Appendix for the representation theory).

In terms of oracle algebra generators the search operator reads $U_G = \exp(i\theta\Sigma_2)$, with $\theta = \arcsin(-2\sqrt{k(N-k)}/N)$. It holds that $U_G^m = \exp(im\theta\Sigma_2)$, $m \in \mathbf{N}$, and then $\rho^{(m)} := U_G^m \rho_s U_G^{m\dagger}$, and $p_m = Tr(\rho^{(m)}|x\rangle\langle x|) = \cos^2(m\theta - \alpha)$, and $p_m = 1$ iff $\cos^2(m\theta - \alpha) = 1$, for $N \gg 1$, $k < N$, *i.e.*, the complexity of the algorithm is $\mathcal{O}(\sqrt{N/k})$.

2. Collective Quantum Search: Merging and Concatenation

Considering joining of two searches in Hilbert spaces $H_r = span\{|i\rangle\}_{i=1}^{N_r}$, $r = 1, 2$, with dimensions N_1, N_2 in the form of concatenation, we first need to embed their database vectors into a larger space $H_1 \oplus H_2$ of dimension $N_1 + N_2$, by padding in zeros into their components, on their top or on their tail, until their number becomes $N_1 + N_2$. By convention, concatenating searches of dim N_1 with one of dim N_2, would mean to form new basis vectors $\{|\emptyset\rangle_{N_1} \oplus |i\rangle_{N_2}; i = 1, ..., N_2\}$, and $\{|i\rangle_{N_1} \oplus |\emptyset\rangle_{N_2},$

$i = 1, ..., N_1\}$, where we denote by $|\emptyset\rangle_{N_1}$, $|\emptyset\rangle_{N_2}$, the respective null vector with all their components being zero. These two new sets of basis vectors constitute the database of the jointed algorithms of dim $N_1 + N_2$. The marked vector to be called $|x_{conc}\rangle$ will read

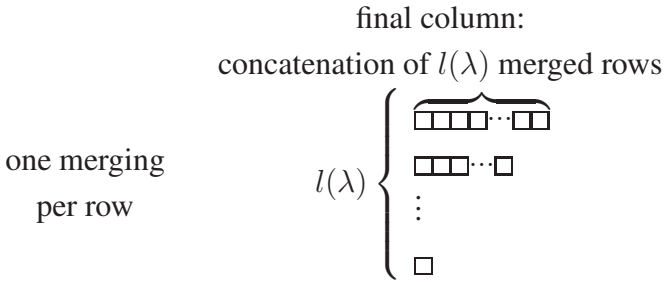
$$|x_{conc}\rangle = |x_1\rangle_{N_1} \oplus |\emptyset\rangle_{N_2} + |\emptyset\rangle_{N_1} \oplus |x_2\rangle_{N_2} = \begin{pmatrix} |x_1\rangle \\ |x_2\rangle \end{pmatrix}.$$

Definition 1. *l-merging and l-concatenation. Let l quantum search algorithms [1]* $U_r(f_r) : H_r \to H_r$, $r = 1, 2, ..., l$ *with* $H_r = span\{|i\rangle\}_{i=1}^{N_r}$ *their database Hilbert spaces,* $U_r(f_r) = -J_{s_r} J_{x_r}$, *where the reflection operators* $J_{s_r} = \mathbf{1} - 2\,|s_r\rangle\,\langle s_r|$, *and* $J_{x_r} = \mathbf{1} - 2\,|x_r\rangle\,\langle x_r|$, *are defined wrt some vectors* $|x_r\rangle$ *and* $|s_r\rangle$, *with* $|s_r\rangle = \frac{1}{\sqrt{N_r}} \sum_{i=1}^{N_r} |i\rangle$, *and* $|x_r\rangle = \sum_{i=1}^{N_r} f_r(i)\,|i\rangle \in H_r$ *the target vectors; here* $f_r : Z_{N_r} \to Z_2$ *their respective oracle functions. We further denote the merged space by* $H_{merg} = \oplus_{r=1}^{l} H_r$ *with* $N_{merg} = N_1 + N_2 + \cdots + N_l$, *let also a quantum search algorithm* $U_{merg}(f_{merg}) : H_{merg} \to H_{merg}$, *with* $H_{merg} = span\{|i\rangle\}_{i=1}^{N_{merg}}$ *its space,* $U_{merg}(f_{merg}) = -J_{|s_{merg}\rangle} J_{|x_{merg}\rangle}$, *its search unitary, and* $f_{merg} : Z_{N_{merg}} \to Z_2$ *its l-target oracle function, and also denoted by* $|x_{merg}\rangle = \sum_{i=1}^{N_{merg}} f_{merg}(i)\,|i\rangle$, *the l-target vector.*

Lemma 1. *Let a 2-concatenation with search operator* $U_{conc} = -J_{|s_{conc}\rangle} J_{|x_{conc}\rangle}$. *Then the following decomposition is valid* $U_{conc} = U_1 \oplus U_2$, *where* U_1, U_2 *are the search operators in Hilbert spaces with dimensions* N_1, N_2, *respectively.*

2.1. Collective Quantum Search: Joining Schemes and Young Diagrams

By convention we take the horizontal direction in a Young diagram (for notation *c.f.* [11]) to denote merging (the number of row boxes equals the number of merged searches), and in the vertical direction the number of rows denotes concatenated sets, *i.e.*,



Recall the partial order of majorization between partitions [10]. Let partitions $\pi = (\pi_1, ..., \pi_s)$ and $\rho = (\rho_1, ..., \rho_t)$; if $s \geq t$ then π weakly majorizes ρ, written as $\pi \overset{w}{\succ} \rho$, if the following inequalities are satisfied,

$$\sum_{i=1}^{k} \pi_i \geq \sum_{i=1}^{k} \rho_i, 1 \leq k \leq t, \sum_{i=1}^{s} \pi_i \geq \sum_{i=1}^{t} \rho_i.$$

If the last relation above is only an equality, then π majorizes ρ , written as $\pi \succ \rho$. Associating partitions to Young diagrams, *i.e.*, $\pi \to Y(\pi)$, an equivalent definition of majorization of partitions is induced via

Lemma 2. *(Muirhead's Lemma) If* $\pi, \rho \vdash m$, *then* $\pi \succ \rho$ *iff* $Y(\pi)$ *can be obtained from* $Y(\rho)$ *by moving boxes up to lower numbered rows.*

In this way all, Young diagrams of given m are partially ordered in the poset $\{\pi \vdash m, \succ\}$, via their associated Young diagrams as shown schematically below,

$$\begin{array}{ccc} Y(\pi) & \overset{\textit{move boxes up}}{\longleftarrow} & Y(\rho) \\ \downarrow & & \uparrow \\ \pi & \succ & \rho \end{array}$$

In the context of collective search, we say equivalently that if diagram $Y(\pi)$ of a partition π describing a joining scheme for a set of searches, has been obtained from some other $Y(\rho)$ by merging some searches among them, *i.e.*,

$$Y(\pi) \overset{\textit{move boxes up, merging a search}}{\longleftarrow} Y(\rho),$$

then $\pi \succ \rho$.

2.2. Collective Quantum Search: Complexity

For the corresponding search complexities T_π, T_ρ we have the following lemma.

Lemma 3. *The search complexity function $T_\pi(N_1, ..., N_n)$, for a given joining scheme of n searches with dimensions $N_1, ..., N_n$, described by partition π, is a Schur concave function, for which it is valid that for any two weakly majorized partitions $\pi^w \succ \rho$ of n, the corresponding complexities are anti-isotonic, i.e., $T_\pi \leq T_\rho$.*

For simplicity's sake, hereafter and unless otherwise stated we consider that a single search algorithm has only one marked element, *i.e.*, $k = 1$. Symbolism: $\langle N_k; N_l \rangle \equiv \frac{N_k + \cdots + N_l}{l-k+1}$. We state the following lemma.

Lemma 4. *Let l searches with database Hilbert space dimensions $\{N_1, ..., N_l\}$, arranged in a Young tableau either as an l -box row, in case of merging, or as an l-box column, in case of concatenation. Denoting the corresponding complexities as $T_{merg}^{(N_1,...,N_l)} = \left\lfloor \frac{\pi}{4}\sqrt{\langle N_1; N_l \rangle} \right\rfloor$ and $T_{conc}^{(N_1,...,N_l)} = \left\lfloor \frac{\pi}{4}\sqrt{N_1} \right\rfloor + \cdots + \left\lfloor \frac{\pi}{4}\sqrt{N_l} \right\rfloor$ respectively, it is valid that $T_{merg}^{(N_1,...,N_l)} \leq T_{conc}^{(N_1,...,N_l)}$.*

Having introduced the main concepts and mathematical tools of collective quantum search we proceed to state and show the main result.

Consider the ratio of the extreme values of complexities T_{conc}/T_{merg}, *i.e.*, "all concatenated" over "all merged". The sequence $\{N_i\}_{i=1}^n$ of dimensions, can be of two distinct kinds : (i) $\{N_i\}_{i=1}^n$ an unbounded sequence, e.g., N_i's are consecutive terms of sequence 2^i (a natural choice for database sizes), in this case we show that $T_{conc}/T_{merg} = \mathcal{O}(\sqrt{n})$; (ii) if the sequence $\{N_i\}_{i=1}^n$ is bounded (e.g., $N_i = 2^{b_i}$,where $\{b_i\}_{i=1}^n$ is bounded), then the ratio $\frac{T_{conc}}{T_{merg}} \in \Theta(n)$, *i.e.*, it is asymptotically linear in n, the number of databases (for "Big Theta" notation *c.f.* [12]). Next lemma and proposition provides an estimation for the search complexity for arbitrary database dimensions.

Lemma 5. *If* $T^{(c)}_{conc} = \sum_{i=1}^{n} \frac{\pi}{4}\sqrt{N_i}$ *and* $T^{(c)}_{merg} = \frac{\pi}{4}\sqrt{\frac{1}{n}\sum_{i=1}^{n} N_i}$, *are the continuous analogues (continuous functions) for complexities* T_{conc}, T_{merg}, *then, i)* $T_{merg} = \left\lfloor T^{(c)}_{merg} \right\rfloor$ *ii)* $\frac{T^{(c)}_{conc}}{T^{(c)}_{merg}} - \frac{n}{T^{(c)}_{merg}} < \frac{T_{conc}}{T_{merg}} < \frac{T^{(c)}_{conc}}{T^{(c)}_{merg}-1}$.

Proposition 1. *For arbitrary positive integers (database sizes)* N_i, $i = 1, 2, ..., n$ *it holds that*

$$\sqrt{n}T^{(c)}_{merg} < T^{(c)}_{conc} \leq nT^{(c)}_{merg}$$

Moreover, if N_i *are:*

(a) consecutive terms of the unbounded sequence $\{N_i\}_{i=1}^{n}$ *with* $N_i = 2^i$, *then* $T_{conc} = \mathcal{O}(\sqrt{n})T_{merg}$.

(b) terms of a bounded sequence of positive integers with $p = \sup\{N_i\}_{i=1}^{n}$, $q = \inf\{N_i\}_{i=1}^{n}$, *then :* $\frac{T_{conc}}{T_{merg}} \in \Theta(n)$, *i.e.,* $n\lambda^{-1}T_{merg} \leq T_{conc} \leq n\lambda T_{merg}$, *with* $\lambda = \left\lfloor \frac{\pi}{4}\sqrt{p} \right\rfloor \left\lfloor \frac{\pi}{4}\sqrt{q} \right\rfloor^{-1}$.

Remark 1. *(i) If* $N_i = 2^{b_i}$ *, for all* $i = 1, ..., n$, *and* $\{b_i\}_{i=1}^{n}$ *is an increasing and bounded above sequence of positive integers, the statement of lemma remains valid.*

(ii) Since $\lim_{n\to\infty} N_n = 2^6$, *database sizes* N_n *are asymptotically equal to a constant number, and this is true since* $(\boldsymbol{R}, |\cdot|)$ *is a complete metric space. Observe that the curve in Figure 1 is close to line* $y = x$ *(i.e., the ratio* T_{conc}/T_{merg} *is close to* n*). In the special case of constant sequence* $\{N_j\}$, *for the continuous versions* $T^{(c)}_{conc}, T^{(c)}_{merg}$ *of the complexities, we have that* $T^{(c)}_{conc}/T^{(c)}_{merg} = n$, *for all* n.

(iii) Since every sequence in R *has a monotone subsequence, it follows that, given a bounded above sequence* $\{N_j\}$, *we can always extract a monotone subsequence* $\{N_{c_j}\}$ *necessarily bounded, and therefore convergent. (c.f. Bolzano-Weirstrass theorem, stating that each bounded sequence in* R^m *has a convergent subsequence). Hence, even if* $\{N_j\}$ *is bounded above but not convergent, if using only* $\{N_{c_j}\}$ *as database sizes, the ratio* T_{conc}/T_{merg} *will be close to database number.*

(iv) A geometric interpretation of inequalities of the proposition, providing bounds for the complexity, is that asymptotically, the ratio $\frac{T_{conc}}{T_{merg}}$ *lies in the interior of an angle* $\delta = \arctan(\lambda) - \arctan(\lambda^{-1})$ *with vertex at point* $(0, 0)$ *and sides along directions* $n\lambda^{-1}$ *and* $n\lambda$, *symmetric wrt bisector* $y = x$*; it lies on the bisector if* $N_i = N$, *i.e., all distances are equal, (in this case the search operator is* $U_{G;conc}(nN) = \oplus_{i=1}^{n} U_G(N) = \mathbf{1}_n \otimes U_G(N)$*).*

A special case of minimum complexity is stated in the following lemma.

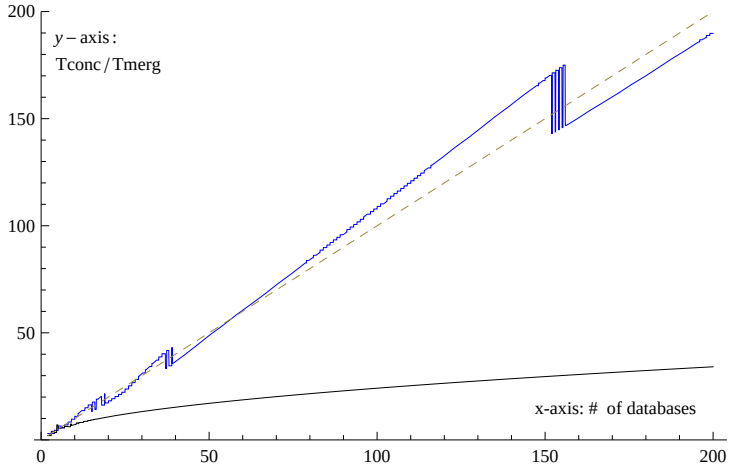


Figure 1. Plots for T_{conc}/T_{merg} , for non decreasing and bounded above sequence of database sizes (blue curve), and an unbounded one (black curve). Here the bounded sequence $N_j = 2^{b_j}, b_j = \left\lfloor \frac{6j^2+j-1}{j^2+4} \right\rfloor, N_1 = 2, \lambda = \frac{\left\lfloor \frac{\pi}{4}\sqrt{p} \right\rfloor}{\left\lfloor \frac{\pi}{4}\sqrt{q} \right\rfloor}, p = 2^6, q = N_1 = 2$, and the unbounded one $N_j = 2^j$, $N_1 = 2$ are used. Dashed line: $y = x$.

Lemma 6. *The complexity of an l merging is minimum and independent of l if and only if all involved database dimensions are equal.*

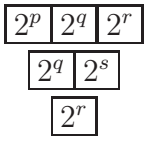
2.3. Collective Quantum Search: Threshold Cases

Summarizing the study so far by referring to sequences $(1^n) \prec \pi_2 \prec \ldots \prec \pi_{k-1} \prec (n)$ and $T_{(1^n)} \geq T_{\pi_2} \geq \cdots \geq T_{\pi_{k-1}} \geq T_{(n)}$, we note that: the first sequence concerns the weak ordering of partitions ranging from total concatenation to total merging of n searches. The second one concerns the associated numerical ordering of these schemes via comparison between their corresponding complexities. We seek to clarify which are the generic threshold cases in the sequences according to some criteria, *i.e.*, the cases in which merging gives no computational advantage in search, due to some circumstantial reasons to be determined. Two such criteria are, the *conjugate partition criterion (CPC)*, and the *threshold partition criterion (TPC)*. In case of CPC the $*$ conjugation for partitions is used to single out as threshold cases the self-conjugate partitions $\pi = \pi^*$ for which $T_\pi = T_{\pi^*}$, [13], under some specified database dimensions. In case of TPC the threshold cases are the so called threshold partition π, which hold a balanced number of boxes (searches) in the upper and lower parts of its Young diagram.

2.3.1. Conjugate Partition Criterion

The complexity of any joining scheme is determined both by the partition shaping its Young diagram and by filling of partition's boxes by the respective Hilbert space dimensions N_i of quantum databases. A simplification is the standard tableau and particularly the physically motivated choice $N_i = 2^i$. Consider n jointed searches interpolating between full concatenation with partition (1^n) and full merging with partition (n) . Consider the conjugation of partition $\pi \to \pi^*$, which produces partition π^* by turning rows into column and vice versa and then assign dimensions N_{ij} to each box (search), *i.e.*, $(\pi_i, j) \to N_{ij}$, and seeks values for N_{ij}, so that the ensuing complexities are equal, *i.e.*, $T_\pi = T_{\pi^*}$. This equality is

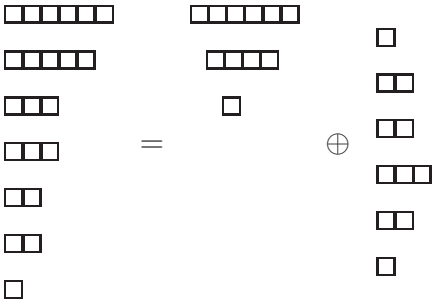
achieved by any intermediate joining scheme $(1^n) \prec \pi \prec (n)$, which is self conjugate, *i.e.*, $\pi = \pi^*$. E.g. in $\pi \vdash 6$, partition $\pi = (3,2,1)$ is self-conjugate and the next choice of dimensions gives equal complexity



The indicated filling with dimensions p, q, r, s fulfils condition, *i.e.*, $T_{(3,2,1)} = T_{(3,2,1)^*}$.

2.3.2. Threshold Partition Criterion

Proceeding from full concatenation to full merging of n searches by moving up one box at a time (merging one more search), creates diagrams that majorize all preceding ones, as explained. Explicitly, let of division of a $Y(\pi)$ into two disjoint pieces, $Y_u(\pi)$ with boxes lying on and to the right of the diagonal, and $Y_d(\pi)$ be the rest piece, *i.e.*, $Y(\pi) = Y_u(\pi) \cup Y_d(\pi)$. E.g. for partition $\pi = (6,5,3,3,2,2,1)$ the diagrams $Y(\pi)$, $Y_u(\pi)$ and $Y_d(\pi)$ are



Let next $y_u(\pi)$ be a partition whose parts are the lengths of the rows of the shifted shape $Y_u(\pi)$, and $y_d(\pi)$ be the partition whose parts are the lengths of the columns of $Y_d(\pi)$. If n is even and $\pi \vdash n$, then partition π is called *graphic partition* iff $y_u(\pi)^w \prec y_d(\pi)$ and it is called *threshold partition* π_{th} iff $y_u(\pi_{th}) = y_d(\pi_{th})$ [13]. In the case of threshold partition it follows that $T_{y_u(\pi)} = T_{y_d(\pi)}$ and that half of the number of merging responsible for crossing the diagonal have already happened (*i.e.*, $|y_u| = |y_d| = \frac{N}{2}$). This threshold relation landmarks the midway situation before the onset of total merging. For the example above the pairs $y_u(\pi) = (6,4,1)$, $y_d(\pi) = (6,4,1)$, and $y_u(\pi) = (7,3,1)$, $y_d(\pi) = (6,3,2)$ satisfy the TPC.

2.4. Oracle Algebra for Collective Quantum Search

Let database Hilbert spaces $H_{N_1}, H_{N_2}, H_{N_3}$, where $H_{N_i} = l_2(\Delta_{N_i})$ with $N_1 = N_2 = N_3 = 4$, and let the marked items be the first, the third, and the second elements in $H_{N_1}, H_{N_2}, H_{N_3}$, respectively. To the partitions $(111), (21), (3)$, of 3, correspond the joining (i) a $3-$merging in database $H_{N_1+N_2+N_3} = \oplus_{i=1}^{3} H_{N_i}$, (ii) a 2-merging in $H_{N_1+N_2} = \oplus_{i=1}^{2} H_{N_i}$, a single in H_{N_3}, and concatenation between them, and finally (iii) concatenation of searches in $H_{N_1}, H_{N_2}, H_{N_3}$. Using notation $|x_N^\pi\rangle$ and $\pi_N(\Sigma_a^\pi)$, $a = 1,2,3,0$ we have:

(i) 3-merging in $H_{N_1+N_2+N_3}$;
The marked items are $|1\rangle, |7\rangle, |10\rangle$, so $\left|x_{12}^{(3)}\right\rangle = \frac{1}{\sqrt{3}}(|1\rangle + |7\rangle + |10\rangle)$, $\left|x_{12}^{(3)\perp}\right\rangle = \frac{1}{\sqrt{9}}(|2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |8\rangle + |9\rangle + |11\rangle + |12\rangle)$, and the 12-dim representation of oracle algebra generators are

$$\pi_{12}(\Sigma_1^{(3)}) = \pi_{12}\left(\left|x_{12}^{(3)}\right\rangle\left\langle x_{12}^{(3)\perp}\right|\right) + H.c.,\ \pi_{12}(\Sigma_2^{(3)}) = \pi_{12}\left(-i\left|x_{12}^{(3)}\right\rangle\left\langle x_{12}^{(3)\perp}\right|\right) + H.c.,$$

$$\pi_{12}(\Sigma_3^{(3)}) = \pi_{12}\left(\left|x_{12}^{(3)}\right\rangle\left\langle x_{12}^{(3)}\right|\right) - H.c.,\ \pi_{12}(\Sigma_0^{(3)}) = \pi_{12}\left(\left|x_{12}^{(3)}\right\rangle\left\langle x_{12}^{(3)}\right|\right) + H.c.$$

(ii) 2-merging in $H_{N_1+N_2}$, single search in H_{N_3}, and concatenation between them;
The marked items are $|1\rangle, |7\rangle$ in $H_{N_1+N_2}$, and $|2\rangle$ in H_{N_3}, so $\left|x_8^{(2,1)}\right\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |7\rangle)$, $\left|x_8^{(2,1)\perp}\right\rangle = \frac{1}{\sqrt{6}}(|2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |8\rangle)$, $\left|x_4^{(2,1)}\right\rangle = |2\rangle$, $\left|x_4^{(2,1)\perp}\right\rangle = \frac{1}{\sqrt{3}}(|1\rangle + |3\rangle + |4\rangle)$. Since e.g., $\left|x_{12}^{(2,1)}\right\rangle = \left|x_8^{(2,1)}\right\rangle \oplus \left|x_4^{(2,1)}\right\rangle$, the generators decompose

$$\pi_{12}(\Sigma_a^{(2,1)}) = \pi_8(\Sigma_a^{(2,1)}) \oplus \pi_4(\Sigma_a^{(2,1)}).$$

(iii) Single searches in H_{N_1}, H_{N_2} and H_{N_3} and concatenation between them;
The marked items are $|1\rangle \in H_{N_1}$, $|3\rangle \in H_{N_2}$, and $|2\rangle \in H_{N_3}$. E.g. for H_{N_1}, $\left|x_4^{(1,1,1)}\right\rangle = |1\rangle$, $\left|x_4^{(1,1,1)\perp}\right\rangle = \frac{1}{\sqrt{3}}(|2\rangle + |3\rangle + |4\rangle)$, etc, so for $a = 1, 2, 3, 0$, the following decomposition is obtained,

$$\pi_{12}(\Sigma_a^{(1,1,1)}) = \bigoplus_{H_{1,2,3}} \pi_4(\Sigma_a^{(1,1,1)}).$$

Having the oracle algebra matrix generators we compute the unitary search operators for the three corresponding partitions,

$$U_G^{(3)} = \exp\left(i\theta_{12}\pi_{12}(\Sigma_2^{(3)})\right),$$
$$U_G^{(2,1)} = \exp\left(i\theta_8\pi_8(\Sigma_2^{(2,1)})\right) \oplus \exp\left(i\theta_4\pi_4(\Sigma_2^{(2,1)})\right),$$
$$U_G^{(1,1,1)} = \bigoplus_{H_{1,2,3}} \exp\left(i\theta_4\pi_4(\Sigma_2^{(1,1,1)})\right),$$

where $\theta_N = \arcsin(-2\sqrt{k(N-k)}/N)$ with $k = 1$. By means of a similar search unitary, the collective quantum search complexity measures can be computed.

2.4.1. Generalized Azimuthal Symmetry

Let the partition $\tau = (N_1, N_2, \cdots, N_l)$ of N of length $l = l(\tau)$, and let the one parameter subgroup $U_a(1) = e^{i\phi_a\pi_a(\Sigma_3)}$, generated by $\pi_a(\Sigma_3) \in End(H_a)$. Let the group $G = U(N)$ and the subgroup $K = \bigoplus_{a=N_1}^{N_l} U_a(1)$. Consider a concatenation of l searches for a given partition $\tau \vdash N$, with search operator $U_G^{(\tau)} := \bigoplus_{a=N_1}^{N_l} U_G^{(a)}$ and search step implemented by the transformation $\rho \to U_G^{(\tau)}\rho U_G^{(\tau)\dagger}$. Let further the unitary operator $V_3(\phi) = \bigoplus_{a=N_1}^{N_l} e^{i\phi_a\pi_a(\Sigma_3)} \in K$, $\phi = (\phi_a)_{a=N_1}^{N_l} \in [0, 2\pi)^l$, then the transformation

$$\rho \to \rho' = V_3(\phi)U_G^{(\tau)}\rho U_G^{(\tau)\dagger}V_3(\phi)^\dagger,$$

preserves the projection of density matrix ρ along the collective marked vector $|x\rangle\langle x| := \bigoplus_{a=N_1}^{N_l} |x_a\rangle\langle x_a|$, or equivalently preserves the $\bigoplus_{a=N_1}^{N_l} \pi_a(\Sigma_3)$ component of the collective density matrix [9]. This implies the search complexity remains invariant under the action of V_3.

This equality of complexities is expressed in terms of the minimization of the projection of time-evolved collective density matrix on the collective marked item, *i.e.*,

$$\begin{aligned} 1 &= \min_{\alpha} \langle x| U_G^{(\tau)\alpha} \rho_{ss} U_G^{(\tau)\dagger\alpha} |x\rangle \\ &= \min_{\alpha} \langle x| \left(U_G^{(\tau)\alpha_1} V_3(\phi) U_G^{(\tau)\alpha_2} ... V_3(\phi) U_G^{(\tau)\alpha_r} \right) \rho_{ss} \\ &\quad \times \left(U_G^{(\tau)\alpha_1} V_3(\phi) U_G^{(\tau)\alpha_2} ... V_3(\phi) U_G^{(\tau)\alpha_r} \right)^{\dagger} |x\rangle , \end{aligned}$$

where $\alpha = \alpha_1 + \cdots + \alpha_r$, which is a generalization of an analogues formula for $l = 1$, describing the azimuthal symmetry of single search algorithm [9]. To any partition $\tau \vdash N$ there corresponds a symmetry group $M_\tau = G/K$ for the collective quantum search.

3. Proofs, Examples, and Discussion

In this second part of the paper we have put together a number of items :

1. "Collective quantum search: Merging and Concatenation", with proofs of lemmas and numerical examples; in the following section.
2. "Collective quantum search: Joining Schemes and Young diagrams" we have placed the proof of the main proposition and of the auxiliary lemmas, together with numerical examples that demonstrate the workings of collective quantum search; in the final section.
3. "Oracle algebra and representations" we introduce the mathematical details of the oracle algebra and some examples from its matrix representations.

3.1. Collective Quantum Search

3.1.1. Merging and Concatenation

Proof. (Lemma 1) The target vector decomposes in $|x_{conc}\rangle = |x_1\rangle \oplus |\emptyset\rangle_{N_2} + |\emptyset\rangle_{N_1} \oplus |x_2\rangle \in H_1 \oplus H_2$. Let the initial vectors $|x_{conc}\rangle, |s_{conc}\rangle$ and the corresponding projection operators $|x_{conc}\rangle\langle x_{conc}|$, $|s_{conc}\rangle\langle s_{conc}|$. Then

$$|s_{conc}\rangle = |s_1\rangle \oplus |\emptyset\rangle_{N_2} + |\emptyset\rangle_{N_1} \oplus |s_2\rangle = \begin{pmatrix} |s_1\rangle \\ |s_2\rangle \end{pmatrix}$$

$$|s_{conc}\rangle\langle s_{conc}| = \begin{pmatrix} |s_1\rangle\langle s_1| & \\ & |s_2\rangle\langle s_2| \end{pmatrix} = |s_1\rangle\langle s_1| \oplus |s_2\rangle\langle s_2|$$

$$J_{s_{conc}} = \mathbf{1}_{N_1+N_2} - 2|s_{conc}\rangle\langle s_{conc}| = \begin{pmatrix} J_{s_1} & \\ & J_{s_2} \end{pmatrix} = J_{s_1} \oplus J_{s_2}.$$

Similarly

$$|x_{conc}\rangle \langle x_{conc}| = |x_1\rangle \langle x_1| \oplus |x_2\rangle \langle x_2|$$

and

$$J_{x_{conc}} = \mathbf{1}_{N_1+N_2} - 2\,|x_{conc}\rangle \langle x_{conc}| = \begin{pmatrix} J_{x_1} & \\ & J_{x_2} \end{pmatrix} = J_{x_1} \oplus J_{x_2}.$$

So the search operator by means of the previous decomposition splits into a direct sum, *i.e.*

$$U_{conc}(f_{conc}) = -\left(J_{s_1} \oplus J_{s_2}\right)\left(J_{x_1} \oplus J_{x_2}\right) = U_1 \oplus U_2.$$

Similarly, for an l-concatenation it is valid that $U_{conc} = \bigoplus_{j=1}^{l} U_j$. □

Symmetries of U_{conc} and U_{merg}. For concatenation, the search operator is determined up to a $V_1 \oplus V_2$ unitary, *i.e.*

$$U_{conc} = -(V(N_1) \oplus V(N_2))(J_{s_1} \oplus J_{s_2})(V(N_1) \oplus V(N_2))^{\dagger}(J_{x_1} \oplus J_{x_2}).$$

Note that $V(N_1) \oplus V(N_2)$ is the diagonal subgroup of group $V(N_1 + N_2)$. By induction on l, a l-concatenation algorithm, has $\bigoplus_{i=1}^{l} V(N_l)$-symmetry, which is the diagonal subgroup of $U(N_{merg})$.

Grover [2] showed that for a single search algorithm with one target vector, the unitary search operator $U_G = -J_s J_x$ can be replaced by a more general operator which is also unitary and it can be in one of the two following equivalent forms

$$\begin{aligned} U_G &= -J_s V^{\dagger} J_x V \\ U_G &= -V^{\dagger} J_s V J_x, \end{aligned}$$

with $V \in U(N)$. These symmetries survive in the case of joined searches as follows. For merged algorithms the unitary symmetry is $U(N_{merg})$, *i.e.*,

$$U_{merg} = -J_{s_{merg}} V(N_{merg})^{\dagger} J_{x_{merg}} V(N_{merg}).$$

3.1.2. Joining Schemes and Young diagrams

Partitions are specified by lower case Greek letters. If λ is a partition of a non negative integer k, we write $\lambda \vdash k$ and call k the weight of the partition, and $\lambda = (\lambda_1, ..., \lambda_k)$ is a sequence of non negative integers λ_i for $i = 1, 2, ..., k$, such that $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_k \geq 0$ with $\sum_{i=1}^{k} \lambda_i = k$. The non zero λ_i are called the parts of λ and their number $l(\lambda)$ is the length of λ. In specifying λ, the trailing zeros, that is those $\lambda_i = 0$, are often omitted. By way of illustration, if $k = 10$, we regard $(4, 2, 2, 1, 1, 0, 0, 0, 0, 0)$ and $(4, 2, 2, 1, 1)$ as the same partition λ, for which it holds that $|\lambda| = 10$ and $l(\lambda) = 5$. Each partition λ of weight $|\lambda| = k$, and length $l(\lambda)$ defines a (Ferrers) Young diagram $Y(\lambda)$ consisting of $|\lambda|$ boxes arranged in $l(\lambda)$ left-adjusted rows of lengths from top to bottom $\lambda_1, ..., \lambda_{l(\lambda)}$, while zeros in λ do not appear in $Y(\lambda)$ (in the English convention). The notation follows in large part that of [11].

The notion of number partition is associated to the joining of quantum searches as follows: given a number of search algorithms m with database dimensions $N_1, N_2, ..., N_m$, we can join them either by

merging or by concatenating in various ways therefore number m is partitioned as $\lambda \vdash m$, where every part λ_i of λ denotes the number of algorithms joined in a similar way, *i.e.*, either by merging or by concatenation. Thus every possible joining scheme corresponds to a Ferrers diagram and vice versa, *i.e.*, $\pi \to T_\pi$, $\rho \to T_\rho$, we find by way of example that $T_\pi \leq T_\rho$.

The latter implies that the sequence of majorized partitions is mapped to the multi-set of complexities, *i.e.*, the example of partitions of 6 worked out below yields

$$\pi \vdash 6: \quad 6 \succ 51 \succ 42 \succ \tfrac{3^2}{41^2} \succ 321 \succ \tfrac{2^3}{31^3} \succ 2^2 1^2 \succ 21^4 \succ 1^6$$

$$T_\pi: \qquad 3 < 4 < 6 \leq \tfrac{6}{7} < 9 \leq \tfrac{9}{10} < 12 < 14 < 17$$

The multi-set of complexities $\{3, 4, 6, 6, 7, 9, 9, 10, 12, 14, 17\}$ form a piecewise ordered set where the numerical ordering is anti-isotonic wrt the majorization order *i.e.*, in general $\pi \succ \rho$ corresponds to $T_\pi \leq T_\rho$. See Figure 2 below.

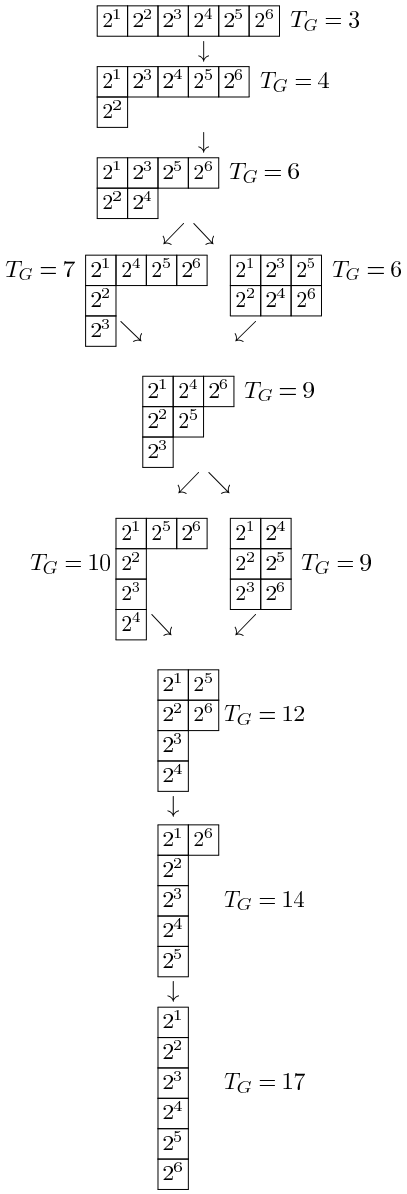


Figure 2. Young tableaux for $m = 6$ and the corresponding complexities T_G .

3.1.3. Complexity

Proof. (Lemma 3) Let an integer partition $\pi = (\pi_1, ..., \pi_j, ..., \pi_{l(\pi)}) \vdash n$, and the multi-variable functions $\phi_\mu(x) : \mathbf{R}_+^n \to \mathbf{R},\ \mu = 1, 2, ..., l(\pi),$ where

$$\phi_\mu(x) = \left\lfloor \frac{\pi}{4} \frac{1}{\sqrt{\pi_\mu}} \sqrt{\sum_{j=1}^{\pi_\mu} x_j} \right\rfloor ,$$

with $x = (x_1, ..., x_n)$, and π_i the part i of partition π, which enumerates the number of databases involved in a merging scheme. Each of these functions ϕ_μ is a multi-variable Schur-concave function: indeed since $(x, y) \to \sqrt{x + y}$ is Schur-concave function and also $x \to \lfloor \phi(x) \rfloor$ is a Schur-concave function if $\phi(x)$ is one (Chapter 3 in [10]), we conclude that ϕ_μ as well as their linear combination is a Schur-concave function.

The linear combination of ϕ_μ's functions is also a Schur-concave function, and this in particular is valid for the search complexity T_π associated with a partition π, *i.e.*, $\pi \to T_\pi$, or explicitly

$$T_\pi(x) = \sum_{\mu=1}^{l(\pi)} \phi_\mu(x).$$

is Schur-concave.

So, if $\pi, \rho \vdash t$ s.t. $\pi \succ \rho$, then $T_\pi(N) \leq T_\rho(N)$, where $N = (N_1, ..., N_t)$ □

Diagrammatically

$$\begin{array}{ccc} \pi & \succ & \rho \\ \downarrow & & \downarrow \\ T_\pi & \leq & T_\rho \end{array}$$

Example 1. *For* $n = 16$ *and the partition* $\pi = (6, 4, 4, 2)$, *there are four functions of variables* $x = (x_1, ..., x_{16})$,

$$\begin{aligned} \phi_1(x_1, ..., x_{16}) &= \left\lfloor \frac{\pi}{4\sqrt{6}} \sqrt{x_1 + x_2 + x_3 + x_4 + x_5 + x_6} \right\rfloor , \\ \phi_2(x_1, ..., x_{16}) &= \left\lfloor \frac{\pi}{4\sqrt{4}} \sqrt{x_7 + x_8 + x_9 + x_{10}} \right\rfloor , \\ \phi_3(x_1, ..., x_{16}) &= \left\lfloor \frac{\pi}{4\sqrt{4}} \sqrt{x_{11} + x_{12} + x_{13} + x_{14}} \right\rfloor , \\ \phi_4(x_1, ..., x_{16}) &= \left\lfloor \frac{\pi}{4\sqrt{2}} \sqrt{x_{15} + x_{16}} \right\rfloor . \end{aligned}$$

each one of them and their linear combination is a Schur-concave function.

Proof. (Lemma 4) Applying Jensen inequality [14] for the convex function $x \to \sqrt{x}$ yields

$$\frac{\pi}{4} \sqrt{\frac{N_1 + \cdots + N_l}{l}} \leq \frac{1}{l} \left(\frac{\pi}{4} \sqrt{N_1} + \cdots + \frac{\pi}{4} \sqrt{N_l} \right)$$

which implies

$$\left\lfloor \frac{\pi}{4}\sqrt{\frac{N_1+\cdots+N_l}{l}} \right\rfloor \leq \left\lfloor \frac{\pi}{4}\sqrt{N_1} \right\rfloor + \cdots + \left\lfloor \frac{\pi}{4}\sqrt{N_l} \right\rfloor .$$

In the relation above the equality is reached iff $0 \leq \sum_{i=1}^{l} \left\{ \frac{\pi}{4}\sqrt{N_i} \right\} < \frac{1}{2}$, where $\{x\}$ denotes the fractional part of the real number x. Notice that the special case where all the numbers appearing in the integral part are all integers, never occurs due to the involvement of π . □

Proof. (Lemma 6) Let $N_1, ..., N_l$ be the sizes of databases, then the complexity equals

$$T_{merg}^{(N_1,...,N_l)} = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N_1+\cdots+N_l}{l}} \right\rfloor .$$

Due to AM-GM inequality, we take that

$$T_{merg}^{(N_1,...,N_l)} \geq \left\lfloor \frac{\pi}{4}\sqrt{\sqrt[l]{N_1...N_l}} \right\rfloor = \left\lfloor \frac{\pi}{4}\sqrt[2l]{N_1...N_l} \right\rfloor$$

The equality holds iff $N_1 = ... = N_l \equiv N$, and therefore the minimum is

$$T_{merg,\min}^{(N,...,N)} = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor .$$

□

Remark 2.

(i) For comparison reasons we find that the complexity of l-concatenation algorithm is

$$T_{conc}^{(N_1,...,N_l)} = \sum_{j=1}^{l} \left\lfloor \frac{\pi}{4}\sqrt{N_j} \right\rfloor$$

since $U_{conc} = \bigoplus_{j=1}^{l} U_j(f_j)$. Moreover, if $N_1 = ... = N_l \equiv N$, then

$$T_{conc}^{(N,...,N)} = l \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor = lT_{merg,\min}^{(N,...,N)},$$

(ii) The total tableau complexity for a joining scheme described by its corresponding Young diagram λ is computed as follows: let a Young diagram $\lambda = (i_1, i_2, ..., i_r)$ then the total search algorithm consists of r groups of concatenated sub-algorithms where each group contains $i_1, i_2, ..., i_r$ merged algorithms. Via previous lemma and remark, the tableau complexity equals $T_{\lambda}^{(N_1,...,N_k)} = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N_1+\cdots+N_{i_1}}{i_1}} \right\rfloor + \left\lfloor \frac{\pi}{4}\sqrt{\frac{N_{i_1+1}+\cdots+N_{i_1+i_2}}{i_2}} \right\rfloor + \cdots$
$+ \left\lfloor \frac{\pi}{4}\sqrt{\frac{N_{i_1+...+i_{r-1}+1}+\cdots+N_k}{i_r}} \right\rfloor$, *where $i_0 = 0$ and $i_1 + \cdots + i_r = k$. If all databases are of equal size N, then for any diagram λ the tableau complexity equals* $T_{\lambda}^{(N,...,N)} = r \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$.

3.1.4. Main Proposition

Next, we consider the ratio of the extreme values of complexities T_{conc}/T_{merg} ("all concatenated" over "all merged"), and regarding the sequence of the dimensions $\{N_i\}_{i=1}^n$, two cases are arising for its asymptotic behaviour. Moreover, for arbitrary positive integers (database sizes) N_i, $i = 1, 2, ..., n$ we prove that for the continuous analogues (continuous functions) for the complexities T_{conc}, T_{merg}, it holds that $\sqrt{n} < \frac{T_{conc}^{(c)}}{T_{merg}^{(c)}} \leq n$.

In more details, if $\{N_i\}_{i=1}^n$ is an unbounded sequence, specifically N_i's are consecutive terms of the geometric sequence 2^i (which is the most natural and reasonable choice for database sizes), we conclude that $T_{conc}/T_{merg} = \mathcal{O}(\sqrt{n})$. Otherwise, namely if the sequence $\{N_i\}_{i=1}^n$ is bounded (e.g., $N_i = 2^{b_i}$,where $\{b_i\}_{i=1}^n$ is bounded), it results that the ratio T_{conc}/T_{merg} is asymptotically linear with respect to the number n of the databases. This fact leads to an interesting observation: although the qualitative difference between a bounded and an unbounded sequence of database sizes is essential (notice that $N_i = 2^i$ increases exponentially fast), however, the quantitative change that entails to the ratio of complexities, is only quadratic (quadratic reduction) with respect to the database population.

Proof. (Lemma 5) Straightforward calculations. □

Proposition 2. *For arbitrary positive integers (database sizes)* N_i, $i = 1, 2, ..., n$ *it holds that*

$$\sqrt{n}T_{merg}^{(c)} < T_{conc}^{(c)} \leq nT_{merg}^{(c)}$$

Moreover, if N_i *are:*

(a) consecutive terms of the unbounded sequence $\{N_i\}_{i=1}^n$ *with* $N_i = 2^i$, *then* $T_{conc} = \mathcal{O}(\sqrt{n})T_{merg}$

(b) terms of a bounded sequence of positive integers with $p = \sup\{N_i\}_{i=1}^n$, $q = \inf\{N_i\}_{i=1}^n$, *then :* $\frac{T_{conc}}{T_{merg}} \in \Theta(n)$, *i.e.,* $n\lambda^{-1}T_{merg} \leq T_{conc} \leq n\lambda T_{merg}$, *with* $\lambda = \left\lfloor \frac{\pi}{4}\sqrt{p} \right\rfloor \left\lfloor \frac{\pi}{4}\sqrt{q} \right\rfloor^{-1}$.

Proof. Applying the Cauchy-Schwarz inequality we obtain that: $T_{conc}^{(c)2} \leq n^2 T_{merg}^{(c)2}$. Moreover $T_{conc}^{(c)} = \sum_{i=1}^n \frac{\pi}{4}\sqrt{N_i} > \frac{\pi}{4}\sqrt{\sum_{i=1}^n N_i} = T_{merg}^{(c)}\sqrt{n}$, so $\sqrt{n} < \frac{T_{conc}^{(c)}}{T_{merg}^{(c)}}$.

(a) Carrying out trivial calculations, we take :

$$\frac{1}{n}\left(\frac{T_{conc}^{(c)}}{T_{merg}^{(c)}}\right)^2 = 1 + \frac{2\sum_{i\neq j}\sqrt{N_i N_j}}{T_{merg}^{(c)2}}\frac{\pi^2}{16n}.$$

In this first case, we have that $N_i = 2^i$, so

$$2\sum_{i\neq j}\sqrt{N_i N_j} = 2(\sqrt{2^n} - 1)^2(\sqrt{2} + 1)^2 - 2(2^n - 1)$$

and $T_{merg}^{(c)2} = \frac{\pi^2}{16n}2(2^n - 1)$. Therefore:

$$\frac{1}{n}\left(\frac{T_{conc}^{(c)}}{T_{merg}^{(c)}}\right)^2 = \frac{(1 - \frac{1}{\sqrt{2^n}})^2(\sqrt{2} + 1)^2}{1 - \frac{1}{2^n}}.$$

The RHS of the above asymptotically equals to $(\sqrt{2}+1)^2$, so $\frac{T^{(c)}_{conc}}{T^{(c)}_{merg}} \approx (\sqrt{2}+1)\sqrt{n}$, *i.e.* $\frac{T^{(c)}_{conc}}{T^{(c)}_{merg}} = \mathcal{O}(\sqrt{n})$ and $\frac{T_{conc}}{T_{merg}} = \mathcal{O}(\sqrt{n})$ because due to previous Lemma and

$$\lim_{n\to\infty} \frac{n}{T^{(c)}_{merg}} = 0,\ T^{(c)}_{merg} \gg 1$$

asymptotically, it holds that

$$\frac{T_{conc}}{T_{merg}} \approx \frac{T^{(c)}_{conc}}{T^{(c)}_{merg}}.$$

(b) Since $p = \sup\{N_i\}_{i=1}^n$, $q = \inf\{N_i\}_{i=1}^n$, then for all $i = 1, 2, ..., n$, is valid that $2 \leq q \leq N_i \leq p$, so

$$n\left\lfloor \frac{\pi}{4}\sqrt{q} \right\rfloor \leq T_{conc} = \sum_{i=1}^{n} \left\lfloor \frac{\pi}{4}\sqrt{N_i} \right\rfloor \leq n\left\lfloor \frac{\pi}{4}\sqrt{p} \right\rfloor.$$

Moreover $\left\lfloor \frac{\pi}{4}\sqrt{q} \right\rfloor \leq T_{merg} \leq \left\lfloor \frac{\pi}{4}\sqrt{p} \right\rfloor$. Therefore $n\lambda^{-1} \leq \frac{T_{conc}}{T_{merg}} \leq n\lambda$ and $\frac{T_{conc}}{T_{merg}} \in \Theta(n)$.

□

3.1.5. Geometry of Complexity Reduction

All concave functions fulfil a very intuitive geometric condition with their graph, namely that the center of mass of a set of points lying on the graph is lying not above the graph itself. Quantifying this geometric property leads to the Jensen inequality [14], which in fact is the reason for achieving complexity reduction in various forms of joining schemes. This is demonstrated below by means of a numerical example.

Example 2. *Numerical example (see Figure 3). Let the Young diagram of shape* $(5, 4, 1)$ *and let the following Young tableau (strictly increasing row and column-wise, no repetitions)*

1	2	4	7	8
3	5	6	9	
10				

where N_i*'s are database sizes :* $N_1 = 2^3$, $N_2 = 2^4$, $N_3 = 2^5$, $N_4 = 2^6$, $N_5 = 2^7$, $N_6 = 2^8, N_7 = 2^9, N_8 = 2^{10}, N_9 = 2^{11}, N_{10} = 2^{12}$

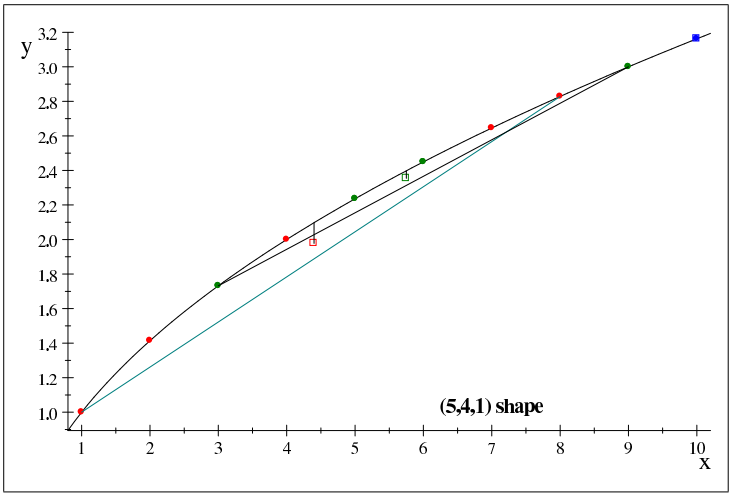


Figure 3. Jensen's inequality for the numerical example. Round dots represent points lying on the graph, and square dots represent center of mass points.

Row 1

Referring to the graph of the complexity function $y = f(x) = \sqrt{x}$ *we mark the* 5 *points* $v^1 = \left\{\left(2^3, \sqrt{2^3}\right), \left(2^4, \sqrt{2^4}\right), \left(2^6, \sqrt{2^6}\right), \left(2^9, \sqrt{2^9}\right), \left(2^{10}, \sqrt{2^{10}}\right)\right\}$ *and the center of mass vector* c^1*, with coordinates* $\left(\frac{2^3+2^4+2^6+2^9+2^{10}}{5}, \frac{\sqrt{2^3}+\sqrt{2^4}+\sqrt{2^6}+\sqrt{2^9}+\sqrt{2^{10}}}{5}\right) = (324.8, 13.891)$*, and its crossing point with the graph of* f *:* $q^1 = (324.8, \sqrt{324.8}) = (324.8, 18.0222)$

Row 2

In the graph of complexity function $f(x) = \sqrt{x}$ *mark the* 4 *points* $v^2 = \left\{\left(2^5, \sqrt{2^5}\right), \left(2^7, \sqrt{2^7}\right), \left(2^8, \sqrt{2^8}\right), \left(2^{11}, \sqrt{2^{11}}\right)\right\}$ *the center of mass vector* $c^2 = (616.0, 19.556)$ *and its crossing point with the graph* $q^2 = (616.0, \sqrt{616.0}) = (616.0, 24.8193)$

Row 3

In the graph of complexity function $f(x) = \sqrt{x}$ *mark the* 1 *point* $v^3 = c^3 = q^3 = (2^{12}, 2^6)$.

Equal Complexity Tableaux and Shapes. Motivated by the geometric explanation of the complexity measure for various schemes of joining quantum search algorithms as has been studied in previous section, we proceed to address the problem of determining shapes and tableaux describing ways of joining searches. We study joining of database spaces of equal dimension N. The complexity is differentiated from one scheme to the other due to the difference of the associated Young diagram shapes, so we call it shape complexity.

					7
					61
				6	52
				51	43
			5	42	**511**
		4	41	**411**	**421**
	3	31	32	33	**331**
2	21	22	**311**	**321**	4111
11	**111**	**211**	**221**	3111	**322**
		1111	2111	**222**	3211
			11111	2211	2221
				21111	31111
				111111	22111
					211111
					1111111

Joined quantum searches, all of which have equal Hilbert space dimension N and share the same shape complexity, are displayed as a pattern of bold typed integer partitions from 3 to 7 within the Young lattice. The pattern of equal complexities is independent from N.

$$c_y^1 + c_y^2 + c_y^3 \leq q_y^1 + q_y^2 + q_y^3$$

Figure 4 displays the contour of equal complexity families of joined quantum algorithms having unequal database sizes. A constant complexity difference (vertical segments) is chosen between tableau complexity (lower broken line) describing concatenation of groups of merged quantum searches and its upper bound (upper full line) describing the same group jointed by concatenation only.

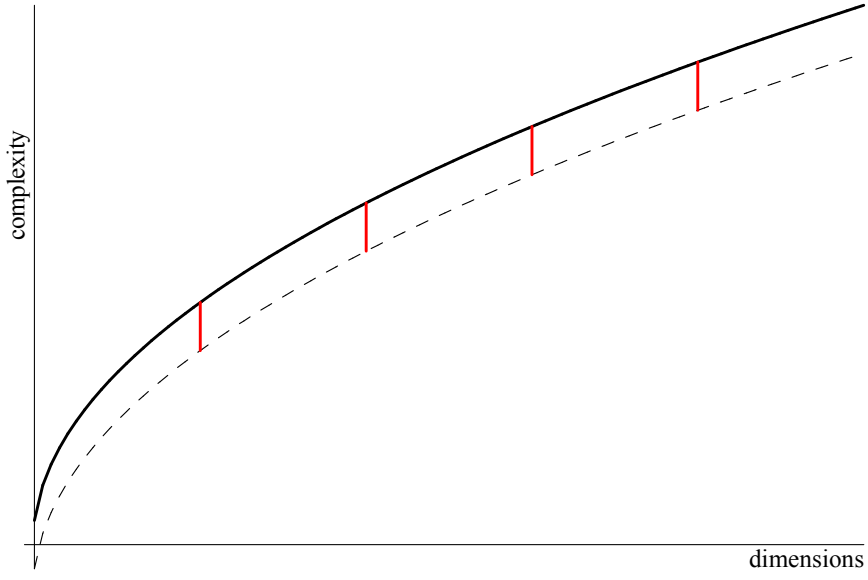


Figure 4. Display of the contour of equal complexity families of joined quantum algorithms.

4. Oracle Algebra and Representations

Definition 2. *Let the set* $\Delta = \{1, 2, ...N\}$, *a subset* $I \subset \Delta$, *and the oracle function* f, *be the characteristic function of* I *with* k *elements, defined as* $f(i) = 1$,*for* $i \in I$, *and* $f(i) = 0$,*for* $i \notin I$. *We define as the matrix oracle algebra* A_f *with respect to the characteristic function* f *of* $I \subset \Delta$, *the set* $A_f = \{A : A = \alpha\Sigma_0(f) + \beta\Sigma_1(f) + \gamma\Sigma_2(f) + \delta\Sigma_3(f)\}$ *where* $\alpha, \beta, \gamma, \delta \in \boldsymbol{R}$ *are arbitrary real [9,15].*

Let also (a) the Hilbert space $l_2(D)$, the vector

$$|x\rangle = \frac{1}{\sqrt{k}} \sum_{i=1}^{N} f(i) \, |i\rangle \, ,$$

and its orthogonal vector

$$\left|x^{\perp}\right\rangle = \frac{1}{\sqrt{N-k}} \sum_{i=1}^{N} (1 - f(i)) \, |i\rangle \, ,$$

with $k = \sum_{i=1}^{N} f(i)$.

(b) the Hilbert space $H_N = span\{|i\rangle\}_{i=1}^{N}$, the matrix $(\widehat{\mathbf{1}}_{st})_{ij} = 1$, $1 \leq i \leq s, 1 \leq j \leq t$, and the N dimensional matrix representation $\pi_N : A_f \to Lin(H_N)$.

Next, we introduce the following $\Sigma_0, \Sigma_1, \Sigma_2, \Sigma_3$, as the generators of A_f :

$$\begin{aligned}
\Sigma_1 &= |x\rangle \left\langle x^{\perp}\right| + \left|x^{\perp}\right\rangle \langle x| \, , \\
\Sigma_2 &= -i \, |x\rangle \left\langle x^{\perp}\right| + i \left|x^{\perp}\right\rangle \langle x| \, , \\
\Sigma_3 &= |x\rangle \langle x| - \left|x^{\perp}\right\rangle \left\langle x^{\perp}\right| \, , \\
\Sigma_0 &= |x\rangle \langle x| + \left|x^{\perp}\right\rangle \left\langle x^{\perp}\right| \, .
\end{aligned}$$

For the oracle function $f(i) = 1, \ 1 \leq i \leq k < N$, and zero otherwise, the representation above reads

$$\pi_{_N}(\Sigma_0) = \begin{pmatrix} \frac{1}{k}\widehat{\mathbf{1}}_{k\times k} & O_{k\times(N-k)} \\ O_{(N-k)\times k} & \frac{1}{N-k}\widehat{\mathbf{1}}_{(N-k)\times(N-k)} \end{pmatrix},$$

$$\pi_{_N}(\Sigma_1) = \begin{pmatrix} O_{k\times k} & \frac{1}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{k\times(N-k)} \\ \frac{1}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{(N-k)\times k} & O_{(N-k)\times(N-k)} \end{pmatrix},$$

$$\pi_{_N}(\Sigma_3) = \begin{pmatrix} \frac{1}{k}\widehat{\mathbf{1}}_{k\times k} & O_{k\times(N-k)} \\ O_{(N-k)\times k} & -\frac{1}{N-k}\widehat{\mathbf{1}}_{(N-k)\times(N-k)} \end{pmatrix},$$

and therefore, for an arbitrary element $A \in A_f$, it holds that

$$\pi_{_N}(\Sigma_2) = \begin{pmatrix} O_{k\times k} & -i\frac{1}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{k\times(N-k)} \\ i\frac{1}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{(N-k)\times k} & O_{(N-k)\times(N-k)} \end{pmatrix},$$

$$\pi_{_N}(\alpha\Sigma_0+\beta\Sigma_1+\gamma\Sigma_2+\delta\Sigma_3) = \begin{pmatrix} \frac{\alpha+\delta}{k}\widehat{\mathbf{1}}_{k\times k} & \frac{\beta-i\gamma}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{k\times(N-k)} \\ \frac{\beta+i\gamma}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{(N-k)\times k} & \frac{\alpha-\delta}{N-k}\widehat{\mathbf{1}}_{(N-k)\times(N-k)} \end{pmatrix}.$$

4.1. Examples

Show cases: Here we show explicitly the vectors and matrices involved in the possible scenarios of joining via merging and/or concatenation for the specific example of three 4-dimensional quantum searches. Let databases $\Delta_{N_1}, \Delta_{N_2}, \Delta_{N_3}$,with $N_1 = N_2 = N_3 = 4$, and let the market items be the first, the third, and the second elements in $\Delta_{N_1}, \Delta_{N_2}, \Delta_{N_3}$ respectively, *i.e.*, $|1\rangle, |7\rangle, |10\rangle$ in $\Delta_{N_1+N_2+N_3}$. The three partitions of 3 are $1 + 1 + 1 = 2 + 1 = 3$, we have three possible joining, *i.e.*, (i) a $3-$merging in database $\Delta_{N_1+N_2+N_3}$, (ii) a 2-merging in $\Delta_{N_1+N_2}$, a single in Δ_{N_3}, and a concatenation, and finally (iii) three single searches in $\Delta_{N_1}, \Delta_{N_2}, \Delta_{N_3}$. We use the symbol $\bullet$ to denote non zero matrix elements, and $\cdot$ for zeros.

4.1.1. 3-Merging $\Delta_{N_1+N_2+N_3}$

The marked items are $|1\rangle, |7\rangle, |10\rangle$, so $\left|x_{12}^{(3)}\right\rangle = \frac{1}{\sqrt{3}}(|1\rangle + |7\rangle + |10\rangle)$, $\left|x_{12}^{(3)\perp}\right\rangle = \frac{1}{\sqrt{9}}(|2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |8\rangle + |9\rangle + |11\rangle + |12\rangle)$, and therefore,

$$
\begin{aligned}
\left|x_{12}^{(3)}\right\rangle &= (\frac{1}{\sqrt{3}}, 0, 0, 0, 0, 0, \frac{1}{\sqrt{3}}, 0, 0, \frac{1}{\sqrt{3}}, 0, 0)^T, \\
\left|x_{12}^{(3)\perp}\right\rangle &= (0, \frac{1}{\sqrt{9}}, \frac{1}{\sqrt{9}}, \frac{1}{\sqrt{9}}, \frac{1}{\sqrt{9}}, \frac{1}{\sqrt{9}}, 0, \frac{1}{\sqrt{9}}, \frac{1}{\sqrt{9}}, 0, \frac{1}{\sqrt{9}}, \frac{1}{\sqrt{9}})^T,
\end{aligned}
$$

$$
\pi_{12}\left(\left|x_{12}^{(3)\perp}\right\rangle\left\langle x_{12}^{(3)}\right|\right) = \begin{pmatrix}
\cdot & & & & & & \cdot & & & \cdot & & \\
\bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot & \cdot & \bullet & \cdot & \cdot \\
\bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot & \cdot & \bullet & \cdot & \cdot \\
\bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot & \cdot & \bullet & \cdot & \cdot \\
\bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot & \cdot & \bullet & \cdot & \cdot \\
\bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot & \cdot & \bullet & \cdot & \cdot \\
\cdot & & & & & & \cdot & & & \cdot & & \\
\bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot & \cdot & \bullet & \cdot & \cdot \\
\bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot & \cdot & \bullet & \cdot & \cdot \\
\cdot & & & & & & \cdot & & & \cdot & & \\
\bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot & \cdot & \bullet & \cdot & \cdot \\
\bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot & \cdot & \bullet & \cdot & \cdot
\end{pmatrix},
$$

$$\pi_{12}\left(\left|x_{12}^{(3)}\right\rangle\left\langle x_{12}^{(3)}\right|\right)=\left(\begin{array}{cccccccccccc}
\bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot & \cdot & \bullet & \cdot & \cdot \\
\cdot & & & & & & \cdot & & & \cdot & & \\
\cdot & & & & & & \cdot & & & \cdot & & \\
\cdot & & & & & & \cdot & & & \cdot & & \\
\cdot & & & & & & \cdot & & & \cdot & & \\
\cdot & & & & & & \cdot & & & \cdot & & \\
\bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot & \cdot & \bullet & \cdot & \cdot \\
\cdot & & & & & & \cdot & & & \cdot & & \\
\cdot & & & & & & \cdot & & & \cdot & & \\
\bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot & \cdot & \bullet & \cdot & \cdot \\
\cdot & & & & & & \cdot & & & \cdot & & \\
\cdot & & & & & & \cdot & & & \cdot & &
\end{array}\right),$$

$$\pi_{12}\left(\left|x_{12}^{(3)\perp}\right\rangle\left\langle x_{12}^{(3)\perp}\right|\right)=\left(\begin{array}{cccccccccccc}
 & \cdot & \cdot & \cdot & \cdot & \cdot & & \cdot & \cdot & & \cdot & \cdot \\
\cdot & \bullet & \bullet & \bullet & \bullet & \bullet & \cdot & \bullet & \bullet & \cdot & \bullet & \bullet \\
\cdot & \bullet & \bullet & \bullet & \bullet & \bullet & \cdot & \bullet & \bullet & \cdot & \bullet & \bullet \\
\cdot & \bullet & \bullet & \bullet & \bullet & \bullet & \cdot & \bullet & \bullet & \cdot & \bullet & \bullet \\
\cdot & \bullet & \bullet & \bullet & \bullet & \bullet & \cdot & \bullet & \bullet & \cdot & \bullet & \bullet \\
\cdot & \bullet & \bullet & \bullet & \bullet & \bullet & \cdot & \bullet & \bullet & \cdot & \bullet & \bullet \\
 & \cdot & \cdot & \cdot & \cdot & \cdot & & \cdot & \cdot & & \cdot & \cdot \\
\cdot & \bullet & \bullet & \bullet & \bullet & \bullet & \cdot & \bullet & \bullet & \cdot & \bullet & \bullet \\
\cdot & \bullet & \bullet & \bullet & \bullet & \bullet & \cdot & \bullet & \bullet & \cdot & \bullet & \bullet \\
 & \cdot & \cdot & \cdot & \cdot & \cdot & & \cdot & \cdot & & \cdot & \cdot \\
\cdot & \bullet & \bullet & \bullet & \bullet & \bullet & \cdot & \bullet & \bullet & \cdot & \bullet & \bullet \\
\cdot & \bullet & \bullet & \bullet & \bullet & \bullet & \cdot & \bullet & \bullet & \cdot & \bullet & \bullet
\end{array}\right)$$

Therefore, the generators of A_f are:

$$\begin{aligned}
\pi_{12}\left(\Sigma_1^{(3)}\right) &= \pi_{12}\left(\left|x_{12}^{(3)}\right\rangle\left\langle x_{12}^{(3)\perp}\right|\right)+H.c., \\
\pi_{12}\left(\Sigma_2^{(3)}\right) &= \pi_{12}\left(-i\left|x_{12}^{(3)}\right\rangle\left\langle x_{12}^{(3)\perp}\right|\right)+H.c., \\
\pi_{12}\left(\Sigma_3^{(3)}\right) &= \pi_{12}\left(\left|x_{12}^{(3)}\right\rangle\left\langle x_{12}^{(3)}\right|\right)-\pi_{12}\left(\left|x_{12}^{(3)\perp}\right\rangle\left\langle x_{12}^{(3)\perp}\right|\right), \\
\pi_{12}\left(\Sigma_0^{(3)}\right) &= \pi_{12}\left(\left|x_{12}^{(3)}\right\rangle\left\langle x_{12}^{(3)}\right|\right)+\pi_{12}\left(\left|x_{12}^{(3)\perp}\right\rangle\left\langle x_{12}^{(3)\perp}\right|\right).
\end{aligned}$$

4.1.2. 2-Merging $\Delta_{N_1+N_2}$, single Δ_{N_3}, and Concatenation

The marked items are $|1\rangle, |7\rangle$ in $\Delta_{N_1+N_2}$, and $|2\rangle$ in Δ_{N_3}, so

$$\begin{aligned}
\left|x_8^{(2,1)}\right\rangle &= \frac{1}{\sqrt{2}}(|1\rangle+|7\rangle)=(\frac{1}{\sqrt{2}},0,0,0,0,0,\frac{1}{\sqrt{2}},0)^T, \\
\left|x_8^{(2,1)\perp}\right\rangle &= \frac{1}{\sqrt{6}}(|2\rangle+|3\rangle+|4\rangle+|5\rangle+|6\rangle+|8\rangle)=(0,\frac{1}{\sqrt{6}},\frac{1}{\sqrt{6}},\frac{1}{\sqrt{6}},\frac{1}{\sqrt{6}},\frac{1}{\sqrt{6}},0,\frac{1}{\sqrt{6}})^T, \\
\left|x_4^{(2,1)}\right\rangle &= |2\rangle=(0,1,0,0)^T, \left|x_4^{(2,1)\perp}\right\rangle=\frac{1}{\sqrt{3}}(|1\rangle+|3\rangle+|4\rangle)=(\frac{1}{\sqrt{3}},0,\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}})^T,
\end{aligned}$$

and

$$\left|x_{12}^{(2,1)}\right\rangle = (\frac{1}{\sqrt{2}}, 0, 0, 0, 0, 0, \frac{1}{\sqrt{2}}, 0, 0, 1, 0, 0)^T,$$

$$\left|x_{12}^{(2,1)\perp}\right\rangle = (0, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, 0, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{3}}, 0, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}})^T,$$

$$\pi_8\left(\left|x_8^{(2,1)\perp}\right\rangle\left\langle x_8^{(2,1)}\right|\right) = \begin{pmatrix} \cdot & & & & & & \cdot & \\ \bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot \\ \bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot \\ \bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot \\ \bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot \\ \bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot \\ \cdot & & & & & & \cdot & \\ \bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot \end{pmatrix},$$

$$\pi_8\left(\left|x_8^{(2,1)}\right\rangle\left\langle x_8^{(2,1)}\right|\right) = \begin{pmatrix} \bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot \\ \cdot & & & & & & \cdot & \\ \cdot & & & & & & \cdot & \\ \cdot & & & & & & \cdot & \\ \cdot & & & & & & \cdot & \\ \cdot & & & & & & \cdot & \\ \bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \bullet & \cdot \\ \cdot & & & & & & \cdot & \end{pmatrix}$$

$$\pi_8\left(\left|x_8^{(2,1)\perp}\right\rangle\left\langle x_8^{(2,1)\perp}\right|\right) = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \bullet & \bullet & \bullet & \bullet & \bullet & \cdot & \bullet \\ \cdot & \bullet & \bullet & \bullet & \bullet & \bullet & \cdot & \bullet \\ \cdot & \bullet & \bullet & \bullet & \bullet & \bullet & \cdot & \bullet \\ \cdot & \bullet & \bullet & \bullet & \bullet & \bullet & \cdot & \bullet \\ \cdot & \bullet & \bullet & \bullet & \bullet & \bullet & \cdot & \bullet \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \bullet & \bullet & \bullet & \bullet & \bullet & \cdot & \bullet \end{pmatrix}$$

Single Δ_{N_3}

$$\pi_4\left(\left|x_4^{(2,1)\perp}\right\rangle\left\langle x_4^{(2,1)}\right|\right) = \begin{pmatrix} \cdot & \bullet & \cdot & \cdot \\ & \cdot & & \\ \cdot & \bullet & \cdot & \cdot \\ \cdot & \bullet & \cdot & \cdot \end{pmatrix},$$

$$\pi_4\left(\left|x_4^{(2,1)}\right\rangle\left\langle x_4^{(2,1)}\right|\right) = \begin{pmatrix} & \cdot & & \\ \cdot & \bullet & \cdot & \cdot \\ & \cdot & & \\ & \cdot & & \end{pmatrix}$$

$$\pi_4\left(\left|x_4^{(2,1)\perp}\right\rangle\left\langle x_4^{(2,1)\perp}\right|\right) = \begin{pmatrix} \bullet & & \bullet & \bullet \\ \cdot & & \cdot & \cdot \\ \bullet & & \bullet & \bullet \\ \bullet & & \bullet & \bullet \end{pmatrix}$$

In this case, we can compute the generators of A_f, e.g., $\pi_{12}\left(\Sigma_1^{(2,1)}\right)$ as follows.

Since $\left|x_{12}^{(2,1)}\right\rangle = \left|x_8^{(2,1)}\right\rangle \oplus \left|x_4^{(2,1)}\right\rangle$ and $\left|x_{12}^{(2,1)\perp}\right\rangle = \left|x_8^{(2,1)\perp}\right\rangle \oplus \left|x_4^{(2,1)\perp}\right\rangle$, we have that:

$$\pi_{12}\left(\Sigma_1^{(2,1)}\right) = \pi_{12}\left(\left|x_{12}^{(2,1)}\right\rangle\left\langle x_{12}^{(2,1)\perp}\right|\right) + H.c. = \pi_8\left(\Sigma_1^{(2,1)}\right) \oplus \pi_4\left(\Sigma_1^{(2,1)}\right)$$

Similarly, $\pi_{12}\left(\Sigma_a^{(2,1)}\right) = \pi_8\left(\Sigma_a^{(2,1)}\right) \oplus \pi_4\left(\Sigma_a^{(2,1)}\right)$, for all $a = 0, 1, 2, 3$.

4.1.3. Single Δ_{N_1}, Single, Δ_{N_2}, and Single Δ_{N_3} in Concatenation

The marked items are $|1\rangle$ in Δ_{N_1}, $|3\rangle$ in Δ_{N_2}, and $|2\rangle$ in Δ_{N_3}, and it holds that

$$\left|x_{12}^{(1,1,1)}\right\rangle = (1,0,0,0,0,0,1,0,0,1,0,0)^T,$$

$$\left|x_{12}^{(1,1,1)\perp}\right\rangle = (0,\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},0,\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},0,\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}})^T,$$

$\left|x_4^{(1,1,1)}\right\rangle = (1,0,0,0)^T \in \Delta_{N_1}$, $\left|x_4^{(1,1,1)}\right\rangle = (0,0,1,0)^T \in \Delta_{N_2}$, $\left|x_4^{(1,1,1)}\right\rangle = (0,1,0,0)^T \in \Delta_{N_3}$.

4.1.4. Single e.g., for Δ_{N_1}

The marked item is the vector $|1\rangle$, therefore

$$\left|x_4^{(1,1,1)}\right\rangle = (1,0,0,0)^T, \left|x_4^{(1,1,1)\perp}\right\rangle = (0,\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}})^T,$$

and

$$\pi_4\left(\left|x_4^{(1,1,1)}\right\rangle\left\langle x_4^{(1,1,1)\perp}\right|\right) = \begin{pmatrix} \cdot & \bullet & \bullet & \bullet \\ & \cdot & \cdot & \cdot \\ & \cdot & \cdot & \cdot \\ & \cdot & \cdot & \cdot \end{pmatrix},$$

$$\pi_4\left(\left|x_4^{(1,1,1)}\right\rangle\left\langle x_4^{(1,1,1)}\right|\right) = \begin{pmatrix} \bullet & \cdot & \cdot & \cdot \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \end{pmatrix},$$

$$\pi_4\left(\left|x_4^{(1,1,1)\perp}\right\rangle\left\langle x_4^{(1,1,1)\perp}\right|\right) = \begin{pmatrix} & \cdot & \cdot & \cdot \\ \cdot & \bullet & \bullet & \bullet \\ \cdot & \bullet & \bullet & \bullet \\ \cdot & \bullet & \bullet & \bullet \end{pmatrix}.$$

In order to compute the generators $\pi_{12}\left(\Sigma_a^{(1,1,1)}\right)$, $a = 0, 1, 2, 3$, we proceed in an analogous manner to the previous case. For simplicity, we also introduce the following shorthand notation, to denote direct sums of vectors $\left|u_4^{(1,1,1)}\right\rangle$ in databases $\Delta_{N_1}, \Delta_{N_2}, \Delta_{N_3}$ respectively, as well as direct sums for other operators and the corresponding Σ's.

$$\bigoplus_{\Delta_{1,2,3}} \left|u_4^{(1,1,1)}\right\rangle = \left|u_4^{(1,1,1)}\right\rangle \oplus \left|u_4^{(1,1,1)}\right\rangle \oplus \left|u_4^{(1,1,1)}\right\rangle,$$

$$\bigoplus_{\Delta_{1,2,3}} \pi_4\left(\Sigma_a^{(1,1,1)}\right) = \pi_4\left(\Sigma_a^{(1,1,1)}\right) \oplus \pi_4\left(\Sigma_a^{(1,1,1)}\right) \oplus \pi_4\left(\Sigma_a^{(1,1,1)}\right).$$

Since $\left|x_{12}^{(1,1,1)}\right\rangle = \bigoplus_{\Delta_{1,2,3}} \left|x_4^{(1,1,1)}\right\rangle$ and $\left|x_{12}^{(1,1,1)\perp}\right\rangle = \bigoplus_{\Delta_{1,2,3}} \left|x_4^{(1,1,1)\perp}\right\rangle$, for e.g., $\pi_{12}\left(\Sigma_1^{(1,1,1)}\right)$ we obtain that:

$$\begin{aligned} \pi_{12}\left(\Sigma_1^{(1,1,1)}\right) &= \pi_{12}\left(\left|x_{12}^{(1,1,1)}\right\rangle\left\langle x_{12}^{(1,1,1)\perp}\right|\right) + H.c. \\ &= \bigoplus_{\Delta_{1,2,3}} \pi_4\left(\left|x_4^{(1,1,1)}\right\rangle\left\langle x_4^{(1,1,1)\perp}\right|\right) + \bigoplus_{\Delta_{1,2,3}} H.c. \\ &= \bigoplus_{\Delta_{1,2,3}} \pi_4\left(\left|x_4^{(1,1,1)}\right\rangle\left\langle x_4^{(1,1,1)\perp}\right| + H.c.\right) = \bigoplus_{\Delta_{1,2,3}} \pi_4\left(\Sigma_1^{(1,1,1)}\right). \end{aligned}$$

5. Discussion

An important follow up of this work concerns the fact that the collective quantum search can be cast in the language of cooperative game theory, and so wider problems of search complexity reduction can be addressed. In fact, cooperative game theory is an area where multi-agent entities choose to collaborate in various schemes in order to take advantage from the collaboration in lowering some computational load which would enable them to achieve a desirable shared objective, see e.g., [16], for a wealth of

principles and examples. For this connection, particularly useful would be the special joining schemes determined by the partitions $\pi = \pi^*$, π_{th} and π_{max}, as tools for studying coalition formation of merging teams of searches aiming to trade collectivity for less search complexity. This appears to be a favorite context for implementing and applying the idea of merging. In particular quantum search by merging as outlined here could also be applied in applications where quantum simulation of quantum searching is carried out by multi-particle Hamiltonian models (see e.g., [17] and references therein). These prospects will be taken up elsewhere.

Acknowledgments

One of us (Ch.K) acknowledges a PhD Scholarship from the Technical University of Crete.

Author Contributions

Both authors contributed to conceive, obtain and interpret the results, and make the preparation of this work. Both authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Grover, L.K. Quantum Mechanics Helps in Searching for Needle in a Haystack. *Phys. Rev. Lett.* **1997**, *79*, 325.
2. Grover, L.K. Quantum Computers Can Search Rapidly by Using Almost any Transformation. *Phys. Rev. Lett.* **1998**, *80*, 4329.
3. Brassard, G. Searching a Quantum Phone Book. *Science* **1997**, *275*, 627–628.
4. Rossi, M.; Bruss, D.; Macchiavello, C. Scale Invariance of Entanglement Dynamics in Grover's Quantum Search Algorithm. *Phys. Rev. A* **2013**,*87*, 022331.
5. Reitzner, D.; Ziman, M. Two Notes on Grover's Search: Programming and Discriminating. **2014**, arXiv:1406.6391.
6. Vrana, P.; Reeb, D.; Reitzner, D.; Wolf, M.M. Fault-Ignorant Quantum Search. *New J. Phys.* **2014**, *16*, 073033.
7. Yoder, T.J.; Low, G.H.; Chuang, I.L. Fixed-Point Quantum Search with an Optimal Number of Queries. *Phys. Rev. Lett.* **2014**, *113*, 210501.
8. Portugal, R. *Quantum Walks and Search Algorithms*; Springer: Berlin, Germany, 2013.
9. Ellinas, D.; Konstandakis, C. Parametric Quantum Search Algorithm by CP Maps: Algebraic, Geometric and Complexity Aspects. *J. Phys. A* **2013**, *46*, 415303.
10. Marshall, A.W.; Olkin, I. *Inequalities: Theory of Majorization and Its Applications*; Academic Press: Waltham, MA, USA, 1975.
11. Macdonald, I.G. *Symmetric functions and Hall polynomials*, 2nd ed.; Oxford University Press: Oxford, UK, 1995.

12. Knuth, D.E. Big Omicron and Big Omega and Big Theta. *ACM Sigact News* **1976**, *8*, 18–24.
13. Merris, R.; Roby, T. The Lattice of Threshold Graphs. *J. Inequal. Pure Appl. Math.* **2005**, *6*, 2.
14. Needham, T. A Visual Explanation of Jensen's Inequality. *Am. Math. Mon.* **1993**, *100*, 768–771.
15. Ellinas, D.; Konstandakis, C. Matrix Algebra for Quantum Search Algorithm: Non Unitary Symmetries and Entanglement. In Proceedings of the Tenth International Conference on Quantum Communication, Measurement and Computation, Queensland, Australia, 19–23 July 2010; pp. 73–76, doi: 10.1063/1.3630150.
16. Chalkiadakis, G.; Elkind, E.; Wooldridge, M. Computational Aspects of Cooperative Game Theory. Synth. *Lectures Artif. Intell. Mach. Learn.* **2011**, *5*, 1–168.
17. Ellinas, D.; Konstandakis, C. Parametric Quantum Search Algorithm as Quantum Walk: A Quantum Simulation. **2015**, submitted.

PARAMETRIC QUANTUM SEARCH ALGORITHM AS QUANTUM WALK: A QUANTUM SIMULATION

DEMOSTHENES ELLINAS and CHRISTOS KONSTANDAKIS

Technical University of Crete,
Department of Electronic & Computer Engineering QLab,
GR 731 00 Chania, Crete, Greece
(e-mails: ellinas@ece.tuc.gr, konstandakis@science.tuc.gr)

(*Received May 8, 2015 – Revised November 2, 2015*)

Parametric quantum search algorithm (PQSA) is a form of quantum search that results by relaxing the unitarity of the original algorithm. PQSA can naturally be cast in the form of quantum walk, by means of the formalism of oracle algebra. This is due to the fact that the completely positive trace preserving search map used by PQSA, admits a unitarization (unitary dilation) a la quantum walk, at the expense of introducing auxiliary quantum coin-qubit space. The ensuing QW describes a process of spiral motion, chosen to be driven by two unitary Kraus generators, generating planar rotations of Bloch vector around an axis. The quadratic acceleration of quantum search translates into an equivalent quadratic saving of the number of coin qubits in the QW analogue. The associated to QW model Hamiltonian operator is obtained and is shown to represent a multi-particle long-range interacting quantum system that simulates parametric search. Finally, the relation of PQSA-QW simulator to the QW search algorithm is elucidated.

Keywords: quantum search, quantum walk, quantum simulation, CP map, Lie algebra.

1. Introduction

General setting. Let us recall the fast quantum search algorithm [1–4], with searching matrix $U_G = -U J_s U^\dagger J_x$, used to search for $1 \leq k \ll N$ entries encoded in vectors $\{|j\rangle \mid 1 \leq j \leq k\}$ among N orthonormal others, that span the complex Hilbert space of an unsorted quantum database of vectors $l_2(\Delta) = \text{span}\{|i\rangle\}_{i=1}^N$, all enumerated by index set $\Delta = \{1, 2, \ldots, N\}$. Here U is an undetermined general $U(N)$ unitary matrix, and $J_s = \mathbf{1} - 2|s\rangle\langle s|$, and $J_x = \mathbf{1} - 2|x\rangle\langle x|$ are reflection operators with respect to vectors $|s\rangle$ and $|x\rangle$. Vector

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle$$

is the uniform superposition state of all database vectors,

$$|x\rangle = \frac{1}{\sqrt{k}} \sum_{j=1}^{k} |j\rangle$$

the uniform superposition of all marked vectors, and

$$|x^{\perp}\rangle = \frac{1}{\sqrt{N-k}} \sum_{j=1}^{k} |j\rangle$$

is the uniform superposition of all unmarked vectors in $l_2(\Delta) = \text{span}\{|i\rangle\}_{i=1}^{N}$, also $\mathcal{V}_x = \text{span}\{|x\rangle, |x^{\perp}\rangle\} \approx \mathbb{C}^2$, where $U \in U(N)$ (see Appendix A for definitions). Remarkably, while classical search requires $O(N/k)$ trials for finding the target item $|x\rangle$, the quantum algorithm is quadratically faster since it determines the items after only $O(\sqrt{N/k})$ queries (see [5] for a recent review and e.g. [6, 7], for some recent developments).

Several authors have investigated the influence on algorithm's complexity of random imperfections both in diffusion operation generated by reflection J_s, and in black-box query generated by reflection J_x, in models that preserve the unitary character of search, i.e. the pureness of density operator [8–10]. Also more recent works [12, 13], have considered search which takes into account possible errors in reporting the correct marked entry with certain failure probabilities. The errors can concern all or some of the marked items, and are modelled by randomization of the oracle operator J_x, resulting into mixed density matrices. In all these generalized search models the account of noise is destructive for the effectiveness of search (for a summary see e.g. [11]). Designated under the common name *parametric quantum search* (PQS), various possibilities of introducing errors, inaccuracies and noise in the algorithm are summarized in the diagrammatic display below.

	random diffusion J_s	random oracle J_x
pure state	[8–10]	[8–10]
mixed state	[18, 19]	[12, 13]

Examples of parametric search models.

The row of the diagram labels the states of search system (pure, mixed), resulting after the introduction of errors, inaccuracies or noise, in either of the two constituents of the algorithm (diffusion process, oracle query), labelling the columns. The randomization of the diffusion operator J_s as well as the randomization of the oracle operator J_x, is introduced in various models with various theoretical and implementational motivations and justifications. Actually these randomizations introduce a number of extra parameters into the algorithm which in some generalized models becomes an open quantum system [14–16], whose state is a density matrix evolving in discrete time. Also we notice that all these generalized search models preserve a basic feature of initial algorithm, namely the $2D$ sub-space $\mathcal{V}_x = \text{span}\{|x\rangle, |x^{\perp}\rangle\} \approx \mathbb{C}^2$; any failure of the qubit registers encoding states $|x\rangle$, $|x^{\perp}\rangle$, e.g. by loosing some qubits, would be an additional source of errors that would go beyond the PQSA scheme discussed here (for a recent study of such cases see [17], and reference therein).

Motivations. The work of this paper is to investigate the inter-relation of Grover's quantum search algorithm with the quantum walk (QW) algorithm (for an original work exploring the search capabilities of a quantum walk see [20]), and to show in particular that a new version of quantum search can be simulated quantum mechanically by a QW. The suggested simulation is based on the fact that the two algorithms share the same computational advantage. In more concrete terms our motivation for putting forward the quantum simulation stems from fact that both algorithms achieve their computational goal by a quadratic factor (the goal corresponds to the reduction of search time for Grover algorithm, and to increase the diffusion rate for QW; generically we refer to the "complexity of the algorithms" hereafter). This is depicted in the scheme.

	classical search	quantum search
quantum walk	$O(N)$	
classical walk		$O(\sqrt{N})$

In this scheme moving diagonally upwards we go from the complexity of classical random walk $O(\sqrt{N})$ (understood as the order of magnitude for the diffusion extend, quantified by the second statistical moment), to the quadratically enhanced complexity $O(N)$, while moving downwards we go from the complexity $O(N)$ of classical search for an item in an unstructured database, to the complexity $O(\sqrt{N})$ for Grover algorithm.

Despite this similarity among the algorithms (i.e. improving each process by improving quadratically the figure of merit of its performance), their possible mathematical inter-relation is not obvious how to be addressed given that search involves a unitary evolution while the QW involves a CPTP map (a stochastic unitary channel). However, the extension of quantum search to the parametric quantum search algorithm (PQSA, see below), which in fact results after allowing for a faulty oracle, and which also operates by means of a stochastic unitary channel, permits now an investigation of the inter-relation, by studying the CP maps of QW and PQSA. This work is to carry out such an investigation. More explicitly in this work a generalization of unitary search algorithm, named parametric quantum search algorithm (PQSA) that has been introduced and studied previously in [18, 19]), is investigated further (Section 2), and its inter-relation to the quantum walk is shown (Section 3). Within the framework of the above diagrammatic display for PQS algorithms, the specific PQSA studied here can be characterized as a random diffusion model, which specifically modifies the reflection operator J_s by a randomization unitary transformation viz. $UJ_sU^\dagger$, as follows $UJ_sU^\dagger \to \sum_i p_i U_i J_s U_i^\dagger$ (see below for details). The resulting search algorithm describes a discrete time evolving open system which is shown to be simulated by a quantum walk.

The following description introduces the subject matter of the paper: PQS is an open-system generalization of unitary quantum search that employs a unitary CP quantum channel type of map to locate a marked density matrix in a set of

such matrices. In the discretized version of PQSA studied in this work the CP search map is parametrized by a single real parameter that admits various limiting values in which PQSA alternatively, either returns to its original unitary form, or becomes slower than that, or finally retains the quadratically reduced complexity of that. Further treating PQSA map as a quantum channel that generally can be unitarized in an extended Hilbert space, such a unitary dilation of the type of QW is found and investigated. The ensuing QW describes a process of Brownian motion in the form of monotonic rotations generated by unitary $\widetilde{V}_0$, $\widetilde{V}_1$ (see below), around y-axis (designated $\widetilde{\Sigma}_2$ in the text). The unitary dilation of the n-th time step of this QW, is generated by a Hamiltonian that describes the interactions of an $n+1$ multi-particle quantum system. This system suggests itself as quantum simulator for PQSA, that relates the search complexity with the number n of quantum coins needed for the simulation. Finally, the relation of PSQA–QW to the QW search algorithm is elucidated for the case of QW on a complete graph that gives rise to a double lane quantum search algorithm.

2. From quantum search to parametric quantum search

The problem. Find $1 \leq k \ll N$ marked elements from the set $\Delta = \{1, 2, \ldots, N\}$, by improving the classical complexity $O(N)$ of the search.

Let us reconsider the concept of quantum database: initially we promoted the n binary strings $(a_1, a_2, \ldots, a_n)$ which constitute the elements of classical database with size $N = 2^n$, to a set of basis elements $\{|a_1, a_2, \ldots, a_n\rangle\}$ of an N-dimensional Hilbert space $H = (H_2)^{\otimes n}$, where $H_2 = \text{span}\{|0\rangle, |1\rangle\}$. In decimal enumeration of state vectors we write $|a_1, a_2, \ldots, a_n\rangle \equiv |i\rangle$, $i = 1, 2, \ldots, N$, which is the $l_2(\Delta)$ database used in the beginning. From the $l_2(\Delta)$ elements we next construct the projection operators in H, i.e. $P_{(a_1,a_2,\ldots,a_n)} = |a_1, a_2, \ldots, a_n\rangle\langle a_1, a_2, \ldots, a_n|$, by the map $e^{i\phi}|a_1, a_2, \ldots, a_n\rangle \to P_{(a_1,a_2,\ldots,a_n)}$, where $0 \leq \phi < 2\pi$. This leads to the database $\Pi = \{|i\rangle\langle i|\}_{i=1}^N = \{\rho_i\}_{i=1}^N \approx l_2(\Delta)/U(1)$ consisting of a collection of N pure density matrices obtained by the database state vector up to a exponential phase factor viz. an element of U(1) group.

Let us introduce the following operation: given unitary matrices A, B, let the adjoint map $\text{Ad}(A) : \Pi \to \Pi : \rho \to \text{Ad}(A)(\rho) = A\rho A^\dagger$, satisfying $\text{Ad}(AB)(\rho) = \text{Ad}(A)\text{Ad}(B)(\rho)$. Then the following adjoint action of $U_G = -UJ_sU^\dagger J_x = UJ_sU^\dagger J_{x^\perp}$, reads

$$\text{Ad}(U_G)(\rho_s) = U_G\rho_s U_G^\dagger = \text{Ad}(U)\text{Ad}(J_s)\text{Ad}(U^\dagger)\text{Ad}(J_x)(\rho_s), \tag{1}$$

and it is the natural extension of Grover's search map from the database of states $l_2(\Delta)$, into the database Π of projection operators.

Next, let the oracle function f be introduced as the characteristic function of subset $I \subset \Delta$ of marked items. The density matrices ρ_x, ρ_s, for the marked and initial vectors, are expressed in terms of vectors $|x\rangle$, $|x^\perp\rangle$, and

$$|s\rangle = \sqrt{\frac{k}{N}}\,|x\rangle + \sqrt{\frac{N-k}{N}}|x^{\perp}\rangle \in \mathcal{V}_x,$$

and Σ matrices as (see Appendix A),

$$\rho_x \equiv |x\rangle\langle x| = s_3^{(x)}\Sigma_3 + s_0^{(x)}\Sigma_0, \tag{2}$$

with the Bloch vector components $(s_0^{(x)} = \frac{1}{2}, s_1^{(x)} = 0, s_2^{(x)} = 0, s_3^{(x)} = \frac{1}{2})$, and

$$\rho_s = |s\rangle\langle s| = \frac{1}{2}\Sigma_0 + s_1^{(0)}\Sigma_1 + s_3^{(0)}\Sigma_3, \tag{3}$$

with components

$$s_1^{(0)} = \frac{\sqrt{k(N-k)}}{N}, \qquad s_2^{(0)} = 0, \qquad s_3^{(0)} = -\frac{N-2k}{2N}.$$

Also the reflections operators with respect to $|s\rangle$ and $|x\rangle$ are respectively,

$$J_s = \frac{N-2k}{N}\Sigma_3 - \frac{2\sqrt{k(N-k)}}{N}\Sigma_1, \tag{4}$$

$$J_x = \mathbf{1}_{\mathcal{V}_x} - 2\,|x\rangle\langle x| = -\Sigma_3. \tag{5}$$

The unitary search matrix equals $U_G = -U J_s U^{\dagger} J_x$, where $U \in \mathrm{U}(N)$, a general unitary operator manifests the $\mathrm{U}(N)$ invariance of Grover algorithm. For $U = \mathbf{1}_{\mathcal{V}_x}$,

$$U_G = \frac{N-2k}{N}\Sigma_0 + i\frac{2\sqrt{k(N-k)}}{N}\Sigma_2, \tag{6}$$

or, by omitting the trivial part proportional to the unit matrix, $U_G = \exp(i\theta\Sigma_2)$, with $\theta = \arcsin(-2\sqrt{k(N-k)}/N)$. For any $n \in \mathbb{N}$, it holds that $U_G^n = \exp(in\theta\Sigma_2)$ and then

$$\rho^{(n)} := U_G^n \rho_s U_G^{n\dagger} = \frac{1}{2}\Sigma_0 + s_1^{(n)}\Sigma_1 + s_3^{(n)}\Sigma_3, \tag{7}$$

where the Bloch vector components $s^{(n)} = (s_1^{(n)}, s_2^{(n)}, s_3^{(n)})$ read as

$$s_1^{(n)} = -\frac{1}{2}\sin(2n\theta - 2\alpha), \qquad s_2^{(n)} = 0, \qquad s_3^{(n)} = \frac{1}{2}\cos(2n\theta - 2\alpha), \tag{8}$$

and $\alpha = \arccos(\sqrt{k/N})$. For $A \in \mathrm{End}(\mathcal{V}_x)$, the trace is evaluated as $\mathrm{Tr}(A) = \langle x|\,A\,|x\rangle + \langle x^{\perp}|A|x^{\perp}\rangle$, so algorithm's success probability is

$$p_n = \mathrm{Tr}(\rho^{(n)}\,|x\rangle\langle x|) = \cos^2(n\theta - \alpha), \tag{9}$$

and $p_n = 1$ iff $\cos^2(n\theta - \alpha) = 1$, for $N \gg 1$, $k < N$, i.e. the complexity of the algorithm is $O(\sqrt{N/k})$.

REMARK. For $n \in \mathbb{N}$, density matrix $\rho^{(n)}$ lies in the $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$ plane, where $\widetilde{\Sigma}_a$ will denote the axis corresponding to operator Σ_a.

Errors in quantum search. This subsection serves the purpose to motivate further the work of this paper by introducing kinds of possible errors in search algorithm, one of which (cf. the PQSA) will subsequently be investigated below.

Referring to the $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$ plane, on which the trajectory of search is traced we can motivate visually different forms of errors that could happen to the search algorithm. One such possible error would be to affect the cyclic trajectory on its plane. This can be caused due to modification of the operator U_G. One such example is when the unitary operator U involved in U_G takes e.g. n different values $U \to U_k = e^{i\phi_k \Sigma_2}$, $k = 1, 2, \ldots, n$, according to a probability distribution $q = \{q_k; k = 1, 2, \ldots, n\}$, in such a way so as to have the substitution of U_G by a CP map, i.e.

$$\mathrm{Ad}U_G \to \mathcal{E}_{\mathrm{error}} = \sum_{k=1}^{n} q_k \mathrm{Ad}U_{G;k}. \tag{10}$$

Then the search map $\mathcal{E}_{\mathrm{error}}$ is an ensemble of unitary search operators $\{q_k; \mathrm{Ad}U_{G;k} \equiv \mathrm{Ad}U_k \mathrm{Ad}J_s \mathrm{Ad}U_k^{\dagger} \mathrm{Ad}J_x\}$, chosen randomly according to a distribution q, therefore it represents itself at the level of Bloch vector by a random disruptive rotation of this vector on the $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$ plane. Here (see below) we will investigate the example of $n = 2$.

Referring next to Fig. 1, we can suggest a different kind of error which contrary to the previous one, where the search trajectory was retained in its plane, now this plane may change according to some specific rule. In particular, let us consider the change of a simple rotation of $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$ plane around axis $\widetilde{\Sigma}_3$ which is the carrier axis of vector $|x\rangle$ (see Fig. 1 for a schematic display of the error as rotation of the plane of the dynamics $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$). The implementation of this error at the vector space would be $V : V_x \to V_x^U \equiv \mathrm{span}\left(|x\rangle, V|x^{\perp}\rangle\right)$, i.e. $|x\rangle \to |x\rangle$ and $|x^{\perp}\rangle \to V|x^{\perp}\rangle$, where $V \in U(N)$. Such a change will obviously leave J_x unaffected and change reflection as $J_s \to J_{s'}$, where

$$\left|s'\right\rangle = V\,|s\rangle = \sqrt{\frac{k}{N}}\,|x\rangle + \sqrt{\frac{N-k}{N}}\,V|x^{\perp}\rangle. \tag{11}$$

The diagram below summarizes the possible types of errors analysed before.

change in search	change of search map
	$\mathrm{Ad}U_G \to \mathcal{E}_{\mathrm{error}} = \sum_{k=1}^{n} q_k \mathrm{Ad}U_{G;k}$
$\mathcal{V}_x \to \mathcal{V}_x$	Bloch vector plane
	$(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$ plane
change in search space	change of search map
	$\mathrm{Ad}U_G \to \mathrm{Ad}V\mathrm{Ad}J_s\mathrm{Ad}V^{\dagger}\mathrm{Ad}J_x = \mathrm{Ad}J_{Vs}\mathrm{Ad}_x$
$\mathcal{V}_x \to \mathcal{V}_x^U$	Bloch vector plane
	$(\widetilde{\Sigma}_1', \widetilde{\Sigma}_3)$ plane

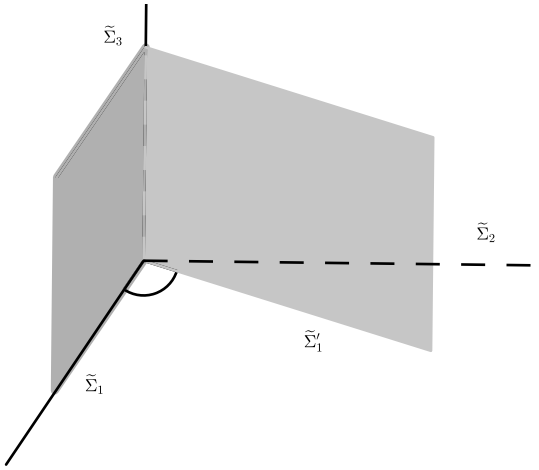


Fig. 1. A schematic display of the error as rotation of the plane of the dynamics $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$by arbitrary angle.

PQSA general framework. On general grounds the introduction of parametric quantum search algorithm is based on the above general setting of search map $\mathrm{Ad}(U_G) = \mathrm{Ad}(-UJ_sU^\dagger J_x) = \mathrm{Ad}(UJ_sU^\dagger J_{x^\perp})$, and it consists in using free unitary U, as an indeterminate variable taking values over a certain set. The aim of this consideration is a generalization of search algorithm in a way that relaxes the unitarity of the map $\rho \to \mathrm{Ad}(U_G)\rho$, which is turned into a completely positive trace preserving map $\mathcal{E}$, i.e. $\rho \to \mathcal{E}(\rho)$. Such generalization would offer a rigidity test of unitary algorithm with respect to modifications, a task served if we endow $\mathcal{E}$ with certain adjustable parameters. Examples of such adjustable parameters are:

(i) A continuous (cf. $p(\theta) \geq 0$, $\theta \in \Omega$, $\int_\Omega p(\theta)d\mu(\theta) = 1$, w.r.t. to measure $d\mu(\theta)$) probability distribution function. First the substitution $\mathrm{Ad}U \to \mathrm{Ad}U(\theta)d\mu(\theta)$, is introduced, which induces via Eq. (1), the substitution $\mathrm{Ad}(U_G) \to \mathrm{Ad}U_G(\theta)d\mu(\theta)$, and then the stochastic averaging is performed, w.r.t. probability distribution $p(\theta)$ and its measure $d\mu(\theta)$, which leads to a new search map

$$\rho \to \mathcal{E}(\rho) = \int_\Omega p(\theta)U_G(\theta)\rho U_G^\dagger(\theta)d\mu(\theta). \tag{12}$$

(ii) A discrete probability distribution, cf. $(q_i > 0, \sum_{i\in I} q_i = 1)$, is considered with associated set of unitary operators $\{V_i(\chi)\}_{i\in I}$, for some parameter $\chi \in X$. First the substitution $\mathrm{Ad}U \to \{\mathrm{Ad}V_i(\chi)\}_{i\in\Omega}$ is introduced, which induces via Eq. (1), the substitution $\mathrm{Ad}(U_G) \to \mathrm{Ad}\widetilde{V}_i = \mathrm{Ad}(V_iJ_sV_i^\dagger J_{x^\perp})$, and then the stochastic averaging is performed, w.r.t. probability distribution q_i, which leads to a new search map

$$\rho \to \mathcal{E}(\rho) = \sum_{i\in I} q_i \mathrm{Ad}\widetilde{V}_i(\rho). \tag{13}$$

The probability distributions and their measures, together with the unitary $\{\mathrm{Ad}U(\theta);\, p(\theta),\ d\mu(\theta)\}$, and $\{p_i, \widetilde{V}_i(\chi)\}_{i\in I}$, in each of the above examples, can be chosen according to some criteria. In the case where the unitary are general elements of $\mathrm{U}(N)$ or form a smaller continuous or discrete subgroup of it, the stochastic averaging is simplified and then iterative actions of the map $\mathcal{E}$ can be computed, especially with all maps' generators commuting. In fact in [19], the second of the two cases, i.e. a set of unitary $\{\widetilde{V}_i(\chi)\}_{i\in I}$, with $I = \{0, 1\}$, a solvable PQSA has been constructed and its complexity has been investigated as function of a free parameter χ.

Finally, within the framework of the PGSA idea, the two cases of modifying search algorithm, i.e. the case of random (faulty) queries and the case of random diffusion can be interrelated by means of the identities

$$\mathrm{Ad}\,(J_{Vs}J_x) = \mathrm{Ad}\,(V)\circ\mathrm{Ad}(J_sJ_{V^\dagger x})\circ\mathrm{Ad}\left(V^\dagger\right), \tag{14}$$

$$\mathrm{Ad}(J_sJ_{V^\dagger x}) = \mathrm{Ad}(V^\dagger)\circ\mathrm{Ad}\,(J_{Vs}J_x)\circ\mathrm{Ad}\,(V)\,. \tag{15}$$

Randomization of V, i.e. $\mathrm{Ad}\,(V)\to\sum_i p_i\mathrm{Ad}\,(R_i)$ (see below for the construction of R_i's) gives rise to a search map with randomized diffusion operator i.e. $\mathrm{Ad}\,(J_{Vs}J_x)\to\sum_i p_i\mathrm{Ad}\left(J_{R_is}J_x\right)$ or equivalently to a search map with randomized oracle, i.e.

$$\mathrm{Ad}(J_sJ_{V^\dagger x})\to\sum_{ijk}p_ip_jp_k\mathrm{Ad}(R_i^\dagger)\circ\mathrm{Ad}(J_{R_js}J_x)\circ\mathrm{Ad}\,(R_k)\,. \tag{16}$$

Next (see also [19]), we introduce one-parameter toy model relaxation of the unitarity of a quantum search algorithm, and we construct the consequent R_i's. In effect we have the following construction procedure until we reach the Rs.

Introduce a CP map, parametrized by a real parameter $\chi\geq 0$ (to be referred hereafter as "the parameter"). If $\mathcal{V}_x$ is taken to be the state space of a quantum system, let us called it the "search system", then we consider an auxiliary qubit system with state space $H_{\mathrm{aux}} = \mathrm{span}\{|0\rangle, |1\rangle\}\approx\mathbb{C}^2$. This auxiliary system is now taken to interact with the "search system" via a Hamiltonian operator that generates the ϕ-rotation, i.e. $\mathcal{H}_\phi = \phi\Sigma_2$, by an interaction term $\mathcal{H}_{\mathrm{int}}(\chi)$ depending on χ, so that $\mathcal{H}_R = \mathcal{H}_\phi + \mathcal{H}_{\mathrm{int}}(\chi) = \mathbf{1}_{\mathrm{aux}}\otimes\mathcal{H}_\phi + \mathcal{H}_{\mathrm{int}}(\chi)$; for a specific form of such a Hamiltonian see [19]. From this Hamiltonian we obtain the evolution operator $U_R = \exp(-i\mathcal{H}_R)$, (for $\hbar = 1$) where χ is the strength of interaction between the search and auxiliary systems. Operator U_R, after projecting via partial tracing on the auxiliary space, becomes now a CP map $\mathcal{E}_R$ that replaces the unitary ϕ-rotation V_ϕ. The map $\mathcal{E}_R$ reads

$$\rho\to\mathcal{E}_R(\rho) = \mathrm{Tr}_{\mathrm{aux}}\left(U_R\,|m\rangle\langle m|\otimes\rho U_R^\dagger\ \right) = \sum_{i=0}^{s}R_i\rho R_i^\dagger, \tag{17}$$

where (cf. [24, 25]),

$$R_i = \mathrm{Tr}_{\mathrm{aux}}\,(U_R\,|m\rangle\langle i\,|) = \langle i\,|\,U_R\,|m\rangle\,, \tag{18}$$

with $i = 1, \ldots, s$ for a chosen number s, and $|m\rangle$ a basis vector in H_{aux}, are the resulting Kraus generators satisfying the completeness relation $\sum_{i=1}^{s} R_i^\dagger R_1 = \mathbf{1}_{\mathcal{V}_x}$, where all Kraus generators are unitary, or not. In the case that Rs are not all unitary, we can facilitate the limit of PQSA to the original unitary search algorithm by bringing the map $\mathcal{E}_R$ "closer" to the original unitary V_ϕ. To this aim a unitary precondition can be introduced, if needed, by replacing the generators Rs by the *nearest* unitary matrix of each one, in the sense of the Frobenius norm [19]. The preconditioning proceeds as follows:

(a) Recall the following well-known statement: for any arbitrary $N \times N$ matrix R_i, the nearest unitary matrix is the one involved in its polar decomposition[21], i.e.

$$V_i = (R_i R_i^\dagger)^{-1/2} R_i, \qquad i = 0, 1, 2, \ldots, s \tag{19}$$

(for details, references, and an example/application, see [19]).

(b) For the parameter χ introduce a particular set G of "good" values such that: the complexity of the algorithm is $O(\sqrt{N})$ iff $\chi \in G$. In the case $\chi \notin G$, a possible efficient search strategy can developed as it is the case in [19].

PQSA random rotation case. Starting with $\text{Ad}(U_G) = \text{Ad}(U J_s U^\dagger J_{x^\perp})$, we choose U to be a one-parameter subgroup element of $\text{U}(N)$, e.g. a rotation matrix around the axis $\widetilde{\Sigma}_2$, i.e. $U \equiv V_\phi = \exp(i\phi\Sigma_2)$. The adjoint action $\text{Ad}V$ is subsequently replaced by a rotation CP map, i.e. $\text{Ad}V \to q_0 \text{Ad}R_0 + \cdots + q_s \text{Ad}R_s \equiv E_R$. This map is next approximated by $\{q_0 \text{Ad}V_0, \ldots, q_s \text{Ad}V_s\}$, which uses the nearest unitary matrices of generators R_i designated as V_i, i.e. $\min_{S \in U(N)} \|R_a - S\| = V_a$, [21]. Once the unitary generators are obtained, the new search map is constructed as

$$\text{Ad}(U_G) = \text{Ad}(U J_s U^\dagger J_{x^\perp}) \to \sum_{a=0}^{s} q_a \text{Ad}(V_a J_s V_a^\dagger J_{x^\perp}) \equiv \mathcal{E}_V. \tag{20}$$

Schematically we have

$$\begin{gathered} \{\text{Ad}R_0, \ldots, \text{Ad}R_s\} \\ \downarrow \\ \{\text{Ad}V_0, \ldots, \text{Ad}V_s\} \\ \downarrow \\ \left\{\text{Ad}\widetilde{V}_0, \ldots, \text{Ad}\widetilde{V}_s\right\}. \end{gathered}$$

This finally leads to the unitary random channel map [26],

$$\mathcal{E}_V = \sum_{k=0}^{s} q_k \text{Ad}(V_k J_s V_k^\dagger J_{x^\perp}) = q_0 \text{Ad}\widetilde{V}_0 + \cdots + q_s \text{Ad}\widetilde{V}_s. \tag{21}$$

THEOREM 1. *The PQSA in its unitary CP map version is a contractive map of the Bloch vector of a density matrix that traces a trajectory in the interior of the Bloch sphere. Specifically, for $s = 1$ and $q_0 = q_1 = 1/2$, the trajectory is a sequence of points lying on a planar curve identified with the logarithmic spiral.*

Proof: For $\chi \in [0, +\infty)\backslash G_1$, let the CPTP map be $\rho \to \mathcal{E}_V(\rho)$, where

$$\mathcal{E}_V = \frac{1}{2}\mathrm{Ad}(V_0 J_s V_0^\dagger J_x + \frac{1}{2}\mathrm{Ad}(V_1 J_s V_1^\dagger J_x), \tag{22}$$

with the unitary Kraus generators

$$V_0 = (R_0 R_0^\dagger)^{-1/2} R_0 = \exp i(\psi(\chi) - \frac{\chi}{2})\Sigma_2, \tag{23}$$

$$V_1 = (R_1 R_1^\dagger)^{-1/2} R_1 = \exp i(-\frac{\chi}{2}\Sigma_2), \tag{24}$$

and

$$\cos\psi(\chi) = |\cos\mu(\chi)|\,[\cos^2\mu(\chi) + \frac{x^2}{4}\delta^2(\chi)]^{-1/2}, \tag{25}$$

$$\delta(\chi) = \frac{\sin\mu(\chi)}{\mu(\chi)}, \mu(\chi) = \sqrt{\frac{\chi^2}{4} + \varphi^2}. \tag{26}$$

see [19]. For all $m = 0, 1, 2, 3, \ldots$ we have that

$$\mathcal{E}_V^m(\rho_s) = \frac{1}{2}\begin{pmatrix} 1 + \cos^m(2\psi(\chi))\cos T & \cos^m(2\psi(\chi))\sin T \\ \cos^m(2\psi(\chi))\sin T & 1 - \cos^m(2\psi(\chi))\cos T \end{pmatrix}, \tag{27}$$

where

$$T = 2m\psi(\chi) - 2m(\pi + \chi - \theta) - 2a,$$
$$a = \cos^{-1}(1/\sqrt{N}), \theta = \sin^{-1}(-2\sqrt{N-1}/N).$$

If $(x_1^{(m)}, x_2^{(m)}, x_3^{(m)})^T$ is the corresponding Bloch vector for $\mathcal{E}_V^m(\rho_s)$, then

$$x_i^{(m)} = \mathrm{Tr}[\mathcal{E}_V^m(\rho_s)\Sigma_i]. \tag{28}$$

Moreover $(x_1^{(0)}, x_2^{(0)}, x_3^{(0)})^T = \left(\frac{\sqrt{N-1}}{N}, 0, -\frac{N-2}{N}\right)^T$, and thus

$$\begin{pmatrix} x_1^{(m)} \\ x_2^{(m)} \\ x_3^{(m)} \end{pmatrix} = \begin{pmatrix} \cos^m 2\psi(x)\sin T \\ 0 \\ \cos^m 2\psi(x)\cos T \end{pmatrix}. \tag{29}$$

For fixed $\chi \in [0, +\infty)\backslash G_1$, we introduce the variable $t \equiv T(m) = Am + B$, where $A = 2(\psi(\chi) - \pi - \chi + \theta)$, $B = -2a$, and rewrite $x_3^{(m)}$ equivalently as

$$x_3^{(m)} = \cos^m 2\psi(x)\cos T, \tag{30}$$

$$x_3^{(m)} = \exp(m\ln(\cos 2\psi(x))\cos(Am + B), \tag{31}$$

and

$$x_3^{(t)} = \exp\left(\frac{-B}{A}\ln(\cos 2\psi(x))\right)\exp\left(\frac{\ln(\cos 2\psi(x))}{A}t\right)\cos t. \tag{32}$$

Similarly

$$x_1^{(t)} = \exp\left(\frac{-B}{A}\ln(\cos 2\psi(x))\right)\exp\left(\frac{\ln(\cos 2\psi(x))}{A}t\right)\sin t. \tag{33}$$

Recalling next that the parametric equations of the logarithmic (equiangular) spiral are

$$x(t) = a\exp(bt)\cos t, \tag{34}$$

$$y(t) = a\exp(bt)\sin t, \tag{35}$$

it follows that the sequence of points $(x_3^{(t)}, x_1^{(t)})$ is lying on a planar curve that is identified with a translated logarithmic spiral centred at the origin $O(0,0)$, via the parameter identifications

$$a = \exp\left(\frac{-B}{A}\ln(\cos 2\psi(x))\right), \tag{36}$$

$$b = \frac{1}{A}\ln(\cos 2\psi(x)). \qquad \square \tag{37}$$

REMARK. Designing the simulation it must be necessary to secure that the step operators would evolve the QW density matrix in a monotonic way towards the north pole of Bloch sphere. The step operators of the simulator are Grover's operators themselves i.e. $U_G(\varphi_i) = -V_i J_s V_i^{\dagger} J_x$ with $V_i(\varphi_1) = \exp(i\varphi_i \Sigma_2)$, satisfying the composition rule $U_G(\varphi_1)U_G(\varphi_2) = U_G(\varphi_i + \varphi_2)$. This closure property suggests that the higher step of QW simulator involves convex combination of products of $U_G(\varphi_i)$s that all translate monotonically the density matrix towards its target state.

3. Parametric quantum search simulated by quantum walk

In this section we show how a parametric quantum search algorithm with unitary preconditioning being performed on its Kraus generators, would lead to a model that admits implementation in terms of quantum walk. In more physical terms we will show the simulation of PQS by a QW (for a basic theory of QWs see the reviews [31, 32]). On general grounds the simulation of quantum systems by other quantum systems, is considered as one of the main goals of Quantum Information Science [27–30] (see also e.g. [38, 39] for quantum simulation of a quantum walk operating at the asymptotic limit, and a quantum simulation of phylogenetic trees, respectively). The quantum simulation of a parametric quantum search by a quantum walk, put forward in this chapter, is along the lines of this more general simulation project, and provides actually a way to establish a correspondence among two of the most basic algorithms, i.e. quantum search in its PQS form and QW.

Specifically we will show that the algorithm described by the map $\mathcal{E}_V \equiv \{q_k, \mathrm{Ad}\widetilde{V}_k\}_{k=0}^{s}$, with the unitary Kraus generators $\widetilde{V}_k$, and probabilities q_k, can be described by a QW map. The $\mathcal{E}_V$ used in the sequel for the sake of generality has $q_k \neq 1/(s+1)$, i.e. it is more general than the unbiased case where $q_k = 1/(s+1)$.

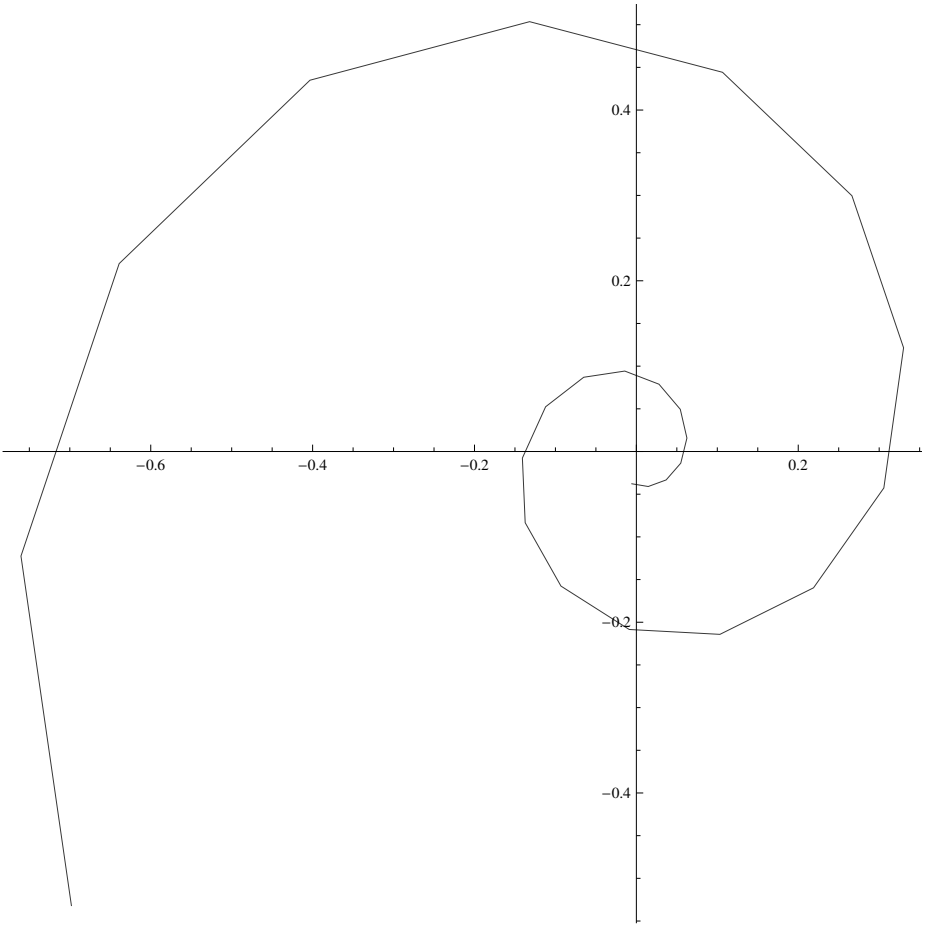


Fig. 2. Display of the logarithmic spiral for the database size $N = 2^{10}$, $\varphi = \pi/4$, parameter $\chi = 0.5$, $q_0 = q_1 = 1/2$, and $0 \leq m \leq \frac{\pi}{4}\sqrt{N}$ iterations. The starting point ($m = 0$) is in the 3rd quadrant.

Recall that the action of the CP map $\mathcal{E}_V$ on a pure (i.e. projective density matrix, i.e. $\rho^2 = \rho$), results in general into a mixture state (i.e. $\rho^2 \neq \rho$, $\rho \in D$ where $D =$ convex hull(pure states), see Appendix A).

The connection to QW is based on the property of a CPTP map (quantum channel) with the unitary Kraus generators to admit a unitary dilation representation of the type of quantum walk [40]. As said, the replacement $\underset{\sim}{U} \to \{V_k(\chi)\}_k$ occurring with probabilities q_k leads to a search map $\mathcal{E}_V \equiv (q_k, \mathrm{Ad}\widetilde{V}_k)_{k=0}^{s}$, with the unitary Kraus $\widetilde{V}_k := V_k J_s V_k^{\dagger} J_{x^\perp} = J_{V_k s} J_{x^\perp}$. The map $\mathcal{E}_V$ factorizes

$$\mathcal{E}_V = \Big(\sum_k q_k \mathrm{Ad} J_{V_k s}\Big)\mathrm{Ad} J_{x^\perp} \equiv \mathcal{E}_r \circ \mathrm{Ad} J_{x^\perp}, \tag{38}$$

where $E_r \equiv \sum_k q_k \mathrm{Ad} J_{V_k s}$ is a conditional reflection map. This implies that the search map $\mathcal{E}_V$ decomposes into an adjoint reflection w.r.t. the vector $|x^{\perp}\rangle$, followed by reflections w.r.t. the vectors $V_k|s\rangle$ operating randomly on density matrix, and the combined action is averaged with probabilities q_k. These actions constitute the map $\mathcal{E}_V$ which repeatedly acts upon $|s\rangle\langle s|$ a number of times, before the resulting density matrix is finally projected in the density matrix $|x\rangle\langle x|$, corresponding to the wanted entry x. Next we specify e.g. to the case $s = 2$, and proceed to show the equivalence to a quantum walk.

To this end we introduce together with the space $\mathcal{V}_x$, which is now identified with the "walker" space, also the "coin" Hilbert space $H_{\mathrm{c}} = \mathrm{span}\{|0\rangle, |1\rangle, \ldots, |n-1\rangle\} \approx \mathbb{C}^n$. A unitary operator $Y_V : H_{\mathrm{c}} \otimes \mathcal{V}_x \to H_{\mathrm{c}} \otimes \mathcal{V}_x$, is then introduced in such a way that

$$\mathcal{E}_V(\rho) = \mathrm{Tr}_{\mathrm{c}} Y_V(\rho_{\mathrm{c}} \otimes \rho) Y_V^{\dagger} = \sum_k q_k \widetilde{V}_k \rho \widetilde{V}_k^{\dagger}, \tag{39}$$

and the unitary dilation operator Y_V is taken as

$$Y_V = \sum_k (P_k \otimes \widetilde{V}_k)(Q \otimes \mathbf{1}_{\mathcal{V}_x}). \tag{40}$$

The matrix $Q \in \mathrm{SU}(n)$ (to be specified shortly) is unitary and acts on the coin space H_{c}, and $P_k = |k\rangle\langle k|$ are rank-1 projection operators offering an orthogonal partition in H_{c}, i.e. $\sum_k P_k = \mathbf{1}_{H_{\mathrm{c}}}$. Then the following equivalent forms Y_V are obtained,

$$Y_V = \sum_k (P_k \otimes J_{V_k s} J_{x^{\perp}})(Q \otimes \mathbf{1}_{\mathcal{V}_x}) \tag{41}$$

$$= \sum_k (P_k \otimes J_{V_k s})(Q \otimes \mathbf{1})(\mathbf{1}_{\mathrm{c}} \otimes J_{x^{\perp}}) \tag{42}$$

$$\equiv Y_r(\mathbf{1}_{\mathrm{c}} \otimes J_{x^{\perp}}). \tag{43}$$

The probabilities $q_k = \mathrm{Tr}(P_k Q \rho_{\mathrm{c}} Q^{\dagger})$ of the associated QW of $\mathcal{E}_V$ are determined by the unitary *reshuffling matrix* Q [38], and the coin density matrix ρ_{c}. Let $\rho_{\mathrm{c}} = |c\rangle\langle c|$, with $|c\rangle$ a basis vector in H_{c}. The matrix Q is not unique and is chosen so that it gives rise to the uni-stochastic matrix $Q \circ Q^*$[41, 42], along the $|c\rangle$ column of which the probabilities q_ks are located, i.e.

$$q_k = \mathrm{Tr}(P_k Q \rho_{\mathrm{c}} Q^{\dagger}) = \langle k| \, Q \circ Q^* \, |c\rangle \, . \tag{44}$$

In fact, since $Q \circ Q^* = DQ \circ (DQ)^*$ for any diagonal matrix D, the reshuffling matrix $Q \in \mathrm{SU}(n)/\mathrm{U}(1)^{\otimes n} \approx CP^n$.

Let $n = 2$. Then, since $Q \circ Q^* = DQ \circ (DQ)^*$ for any diagonal matrix D, the reshuffling matrix $Q \in \mathrm{SU}(2)/\mathrm{U}(1) \approx CP^1$ (cf. [43]). In this case let $Q = \begin{pmatrix} \sqrt{q_0} & \sqrt{q_1} \\ -\sqrt{q_1} & \sqrt{q_0} \end{pmatrix}$, which gives rise to the double stochastic matrix

$$Q \circ Q^* = \begin{pmatrix} q_0 & q_1 \\ q_1 & q_0 \end{pmatrix}; \tag{45}$$

(cf. the definition of the Hadamard or element-wise product $(A \circ B)_{ij} = A_{ij}B_{ij}$, of two square matrices A, B [21]).

The matrix $Q \circ Q^*$ is a convex combination of the two permutation elements of the symmetry group S_2, i.e. $Q \circ Q^* = q_0\mathbf{1} + q_1\sigma_1$ (Birkhoff's theorem [21, 44]). Then the choice of uniform coin distribution, i.e. $q_0 = q_1 = \frac{1}{2}$, implies for the reshuffling matrix $Q = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = e^{i\frac{\pi}{4}\sigma_2}$.

Further, if we denote $\rho_x \equiv \mathrm{Ad}J_{|x^\perp\rangle}(\rho)$, to be the reflected density matrix with respect to the unknown vector $|x^\perp\rangle$, we obtain the following expression for $\mathcal{E}_V$,

$$\mathcal{E}_V(\rho) = \mathrm{Tr}_c Y_V(\rho_c \otimes \rho)Y_V^\dagger \tag{46}$$

$$= \mathrm{Tr}_c Y_r(\rho_c \otimes \rho_x)Y_r^\dagger = \mathcal{E}_r(\rho_x). \tag{47}$$

In the last equation the map $\mathcal{E}_V$ acting on ρ is expressed as the action of a conditional reflection map $\mathcal{E}_r \equiv (q_k, \mathrm{Ad}J_{V_k s})_{k=1}^2$, on the reflected density matrix $\rho_x \equiv \mathrm{Ad}J_{x^\perp}(\rho)$. The map $\mathcal{E}_r = \mathrm{Tr}_c\mathrm{Ad}Y_r$ for $Y_r = \sum_k (P_k Q \otimes J_{V_k s})$, then reads

$$\mathcal{E}_r(\rho_x) = \mathrm{Tr}_c \sum_{k,j} (P_k Q \otimes J_{V_k s})(\rho_c \otimes \rho_x)(Q^\dagger P_j \otimes J_{V_j s}), \tag{48}$$

and provides an equivalent form for $\mathcal{E}_V$

$$\mathcal{E}_V(\rho) = \mathcal{E}_r(\rho_x) = \sum_{i,j} \mathrm{Tr}(P_k Q \rho_c Q^\dagger P_j) J_{V_k s}\rho_x J_{V_j s}^\dagger \tag{49}$$

$$= \sum_{k,j} \mathrm{Tr}(P_k Q \rho_c Q^\dagger P_j)\widetilde{V}_k \rho \widetilde{V}_j^\dagger. \tag{50}$$

Therefore, the following theorem has been established.

THEOREM 2. . *From all unitary dilation representations for the CPTP search map* $\mathcal{E}_V \equiv \{q_k, \mathrm{Ad}\widetilde{V}_k\}_{k=1}^n$ *with the unitary Kraus generators* $\widetilde{V}_k$*, and probabilities* q_k*, there is one of the type of quantum random walk, with the unitary dilation as in Eq.* (40) *and probabilities as in Eq.* (44)*, and thus parametric quantum search can be simulated by a quantum walk.*

REMARKS. (1) Summarizing we have found the following decomposition for the basic map

$$\mathcal{E}_V = \mathrm{Tr}_c\mathrm{Ad}Y_V = \mathrm{Tr}_c\mathrm{Ad}(Y_r(\mathbf{1}_c \otimes J_{x^\perp})) = \mathrm{Tr}_c[\mathrm{Ad}Y_r \circ \mathrm{Ad}(\mathbf{1}_c \otimes J_{x^\perp})]. \tag{51}$$

Moreover, $\mathcal{E}_V$ can be displayed in the form of a quantum circuit[25] as in Fig. 3.

(2) The role of the reshuffling matrix Q in the unitary dilation $Y_V = \sum_k (P_k \otimes \widetilde{V}_k)(Q \otimes \mathbf{1})$ is to reshuffle by a unitary rotation the basis vectors in the coin space, before the subsequent action of the controlled-$\widetilde{V}$ operator in the walker space. This reshuffling is indispensable for having quantum effects, namely the enhanced diffusion rate in a QW, as has been shown in [38]. The lack of

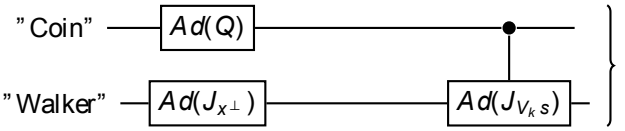


Fig. 3. In this display, the two horizontal lines denote the density matrices of the "coin" system (control space H_c), and the "walker" system (target space $\mathcal{V}_x$). The map $\mathrm{Ad}J_{x^\perp}$ acts locally on "walker" system, then comes the local action of $\mathrm{Ad}(Q)$ on the "coin" space, followed by the conditional reflection map $\sum_k \mathrm{Ad}(P_k \otimes J_{V_k s})$.

nondiagonal unitary Q matrix amounts to a classical random walk, therefore Q plays the role of Planck quantization like a constant in the context of quantization of a classical random walk. In our present case Q is determined by the probability weights of the map $\mathcal{E}_V$, which in turn acquires these weights due to randomization of the rotation operator V_ϕ [19]. Given that the PQSA as introduced in the preceding chapter is based on this randomization e.g. in the scenario of discrete probability distribution see eq. (13), the number of Kraus generators and their associated probabilities equals the cardinality $|I|$ of the index set I, we conclude that in this more general case of PQSA, the reshuffling matrix Q is expected to be a square matrix of size $|I|$. Finally it is easy to prove the following limiting behaviour:

(3) The action of the search map $\mathcal{E}_V \equiv (q_k, \mathrm{Ad}\widetilde{V}_k)_{k=0}^1$ on a density matrix ρ induces on its Bloch vector components $(\lambda_1, \lambda_2, \lambda_3)$ rotations in the $\left(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3\right)$ plane by a random angle α, taking the values α_0 and α_1, according to the probability distribution $\{q_0, q_1\}$. In the limit $\chi \to 0$ for the parameter, we have that the Kraus generators $\widetilde{V}_0$, $\widetilde{V}_1$ become both equal to U_G, and Bloch vector rotates monotonically in the plane $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$.

(4) The detrimental effect of nonzero parameter χ would cause replacement of the monotonic rotation of the Bloch vector in the plane $(\widetilde{\Sigma}_1, \widetilde{\Sigma}_3)$, by erratic rotations due to the Kraus generators of $\mathcal{E}_V$ in the same plane.

4. Multi-qubit chain model for a parametric quantum search via QW

In this section we deal with the case of only two Kraus generators in the map $\mathcal{E}_V$. Our purpose next is to provide a multi-qubit chain model realization for a parametric search algorithm, by deriving an exponential form for the unitary dilation matrix Y_V generating the map $\mathcal{E}_V$ and its powers $\mathcal{E}_V^n$; such a Hamiltonian generator for unitary Y_V would also suggest possible implementation for the QW. Indeed, the exponential form of Y_V obtained, can enable a chain model Hamiltonian description. This model will describe an interaction of a quantum system with a Hilbert space $\mathcal{V}_x$, designated as the "search system" or the "walker system", with a set of n qubits, forming a kind of bath of "coin qubits". Tracing out $n \geq 1$ of these bath coins leads to the evolution map $\mathcal{E}_V$, for the walker system at the time step n, i.e. $\mathcal{E}_V^n$. This identification then implies that the number of steps in the search picture equals the number of qubit coins in the QW picture.

THEOREM 3. *The unitary dilation matrix* $Y_V^{\otimes n}$ *acting on the space* $H_c^{\otimes n} \otimes \mathcal{V}_x$, *is determined via the exponentiation of the Hamiltonian operator*

$$\mathcal{H}=\frac{1}{2^n}\sum_{k_1,\ldots,k_n}\alpha_{k_1,\ldots,k_n}\bigotimes_{\alpha=1}^{n}(\mathbf{1}+(-1)^{1+k_\alpha}\sigma_3)\otimes\Sigma_2 \tag{52}$$

in the form

$$Y_V^{\otimes n}=e^{i\mathcal{H}}e^{\frac{i\pi}{4}(\sigma_2^1+\cdots+\sigma_2^n)}\otimes\mathbf{1}, \tag{53}$$

where $\sigma_2^\nu=\mathbf{1}^{\otimes\nu-1}\otimes\sigma_2\otimes\mathbf{1}^{\otimes n-\nu}$, $\nu=1,2,\ldots,n$.

Proof: In order to cast the unitary dilation matrix Y_V in exponential form we assume for simplicity the uniform distribution of $\mathrm{Ad}\widetilde{V}_0$ and $\mathrm{Ad}\widetilde{V}_1$ in the convex sum forming $\mathcal{E}_V$, so $Q=e^{i\frac{\pi}{4}\Sigma_2}$, and use the identity

$$\mathrm{diag}(e^{A_0},e^{A_1})=e^{P_0\otimes A_0+P_1\otimes A_1} \tag{54}$$

$$=e^{\frac{1}{2}\mathbf{1}\otimes(A_0+A_1)+\frac{1}{2}\sigma_3\otimes(A_0-A_1)}, \tag{55}$$

valid for any two square finite matrices of equal size A_0, A_1, to obtain Y_V as a product of two exponential operators. Next express the search map $\mathcal{E}_V^n$ for any step n as

$$\mathcal{E}_V^n(\rho_{in})=\mathrm{Tr}^{\otimes n}\otimes\mathrm{id}(Y_V^{\otimes n}\rho_c^{\otimes n}\otimes\rho_{\mathrm{in}}Y_V^{\otimes n\dagger}). \tag{56}$$

The above equation suggests a physical implementation of $\mathcal{E}_V^n$, as describing the Hamiltonian interaction of the "search" or "walker" system, living in $\mathcal{V}_x$, initially in some state ρ_{in}, with a bath of n coin qubits, which subsequently gets decoupled from the bath, and ends up in a state described by $\mathcal{E}_V^n(\rho_{\mathrm{in}})$. Explicitly we obtain for the n-th composition of the search map

$$\mathcal{E}_V^n(\rho)=\sum_{k_1,\ldots,k_n}(q_{k_1}q_{k_2}\ldots q_{k_n})\mathrm{Ad}(\widetilde{V}_{k_1}\widetilde{V}_{k_2}\ldots\widetilde{V}_{k_n})(\rho) \tag{57}$$

$$=\mathrm{Tr}^{\otimes n}\otimes\mathrm{id}\left(\mathrm{Ad}Y_V^{\otimes n}(\rho_c^{\otimes n}\otimes\rho)\right). \tag{58}$$

This equivalently implies the map (abbreviation $\mathrm{Tr}_c^{\otimes n}\equiv\mathrm{Tr}^{\otimes n}\otimes\mathrm{id}$)

$$\mathcal{E}_V^n=\mathrm{Tr}_c^{\otimes n}\sum_{k_1,\ldots,k_n}\mathrm{Ad}\Big(\Big(\bigotimes_{m=1}^{n}P_{k_m}Q\Big)\otimes\Big(\prod_{m=1}^{n}\widetilde{V}_{k_m}\Big)\Big). \tag{59}$$

Here probabilities $q_{k_1}q_{k_2}\ldots q_{k_n}$ are extracted from the $|c\rangle^{\otimes n}$ column of the n-fold tensor product of double stochastic matrix $Q\circ Q^*$ i.e.

$$\prod_{m=1}^{n}q_{k_m}=\langle k_1|\,Q\circ Q^*\,|c\rangle\ldots\langle k_n|\,Q\circ Q^*\,|c\rangle \tag{60}$$

$$=\Big(\bigotimes_{m=1}^{n}\langle k_m|\Big)(Q\circ Q^*)^{\otimes n}(|c\rangle^{\otimes n}). \tag{61}$$

The unitary dilation matrix $Y_V^{\otimes n}$ acting in the space $H_c^{\otimes n} \otimes \mathcal{V}_x$ then takes the equivalent forms

$$Y^{\otimes n} = \sum_{k_1,\ldots,k_n} P_{k_1} Q \otimes P_{k_2} Q \otimes \cdots P_{k_n} Q \otimes \widetilde{V}_{k_1} \widetilde{V}_{k_2} \ldots \widetilde{V}_{k_n} \tag{62}$$

$$= \sum_{k_1,\ldots,k_n} P_{k_1,\ldots,k_n} \otimes \widetilde{V}_{k_1} \widetilde{V}_{k_2} \ldots \widetilde{V}_{k_n} (Q^{\otimes n} \otimes \mathbf{1}) \tag{63}$$

$$\equiv \sum_{k_1,\ldots,k_n} P_{k_1,\ldots,k_n} \otimes e^{i(\alpha_{k_1}+\cdots+\alpha_{k_n})\Sigma_2} (Q^{\otimes n} \otimes \mathbf{1}). \tag{64}$$

In the last expression the abbreviation $P_{k_1,\ldots,k_n} \equiv P_{k_1} \otimes P_{k_2} \otimes \cdots \otimes P_{k_n}$ has been used.

We now aim at obtaining an expression for $Y_V^{\otimes n}$ by means of exponentiation of a Hamiltonian operator, similar to that for the first step. To this end we can use a generalization of the matrix identity in Eq. (54), valid for any n square finite equal size matrices $A_{k_1}, A_{k_2}, \ldots, A_{k_n}$, where A_{k_a} are identified with $\widetilde{V}_{k_a}$, to obtain

$$\mathrm{diag}(\widetilde{V}_{k_1}, \cdots, \widetilde{V}_{k_n}) = e^{i \sum_{k_1,\ldots,k_n} \alpha_{k_1,\ldots,k_n} P_{k_1,\ldots,k_n} \otimes \Sigma_2}, \tag{65}$$

where in the last expression the abbreviation $\alpha_{k_1,\ldots,k_n} \equiv \alpha_{k_1} + \alpha_{k_2} + \cdots + \alpha_{k_n}$ has been used.

As a result we obtain that $Y_V^{\otimes n} = e^{i\mathcal{H}} e^{\frac{i\pi}{4}(\sigma_2^1+\cdots+\sigma_2^n)} \otimes \mathbf{1}$, where $\sigma_2^\nu = \mathbf{1}^{\otimes \nu-1} \otimes \sigma_2 \otimes \mathbf{1}^{\otimes n-\nu}$, $\nu = 1, 2, \ldots, n$, and $\mathcal{H}$ be the multi-qubit Hamiltonian

$$\mathcal{H} = \sum_{k_1,\ldots,k_n} \alpha_{k_1,\ldots,k_n} \bigotimes_{\alpha=1}^{n} |k_\alpha\rangle\langle k_\alpha| \otimes \Sigma_2 \tag{66}$$

$$= \frac{1}{2^n} \sum_{k_1 \ldots k_n} \alpha_{k_1,\ldots,k_n} \bigotimes_{\alpha=1}^{n} (\mathbf{1} + (-1)^{1+k_\alpha} \sigma_3) \otimes \Sigma_2. \tag{67}$$

Also in last expression for the Hamiltonian, the projection operators in the coin space H_c, i.e.

$$P_\alpha = |\alpha\rangle\langle\alpha| = \mathrm{diag}(1, (-1)^{1+\alpha}) \tag{68}$$

$$= \frac{1}{2}(\mathbf{1} + (-1)^{1+\alpha}\sigma_3), \quad \alpha = 0, 1, \tag{69}$$

have been used, and this ends the proof. □

5. QW search algorithm and double lane quantum search

Recall the structure of the unitary evolution operator of a coined quantum walk, $V_q = V_{\mathrm{cl}}(U \otimes \mathbf{1}_{\mathrm{w}})$ acting on $H_c \otimes H_w$, the coin and walker Hilbert spaces, where V_{cl} is a conditional unitary in $H_c \otimes H_w$ and U the so-called reshuffling unitary matrix acting in coin space. The terminology V_{cl} stems from the fact that V_{cl}

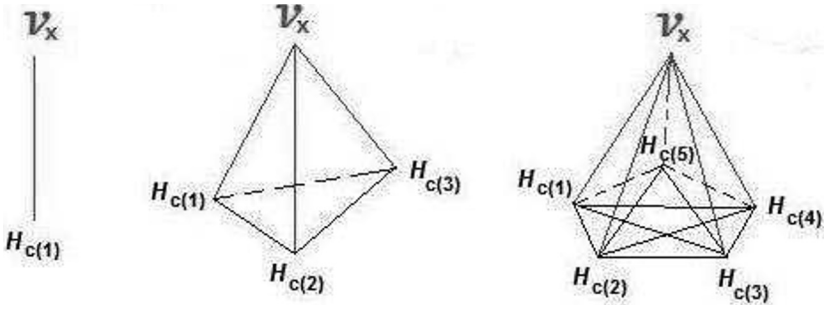


Fig. 4. Display of the full graph form of couplings between quantum systems forming the multi-particle interaction system simulating the quantum walk equivalent of the parametric quantum search algorithm (see the text for details).

alone, i.e. without the involvement of U (i.e. $U = \mathbf{1}$ or U a diagonal unitary), reproduces simply the dynamics of a classical RW in the walker space H_{w}. This has been shown for the case of QW on integers in [38], where the role of U was assimilated with $\hbar$, as a cause generating quantum effects such as speed up in diffusion rate of QW compared to CW. This "U-quantization" of the walk is uniform in walker's space, i.e. the term $U \otimes \mathbf{1}_{\mathrm{w}}$ requires each walker's site $|i\rangle \in H_{\mathrm{w}}$ to associate to the same H_{c} base vectors i.e. the same "head" and "tail" coin sides. This restriction can be relaxed considering e.g. an orthogonal decomposition of walker's space, i.e. $\mathbf{1}_{\mathrm{w}} = P_x + P_{x^\perp}$, for some vector $|x\rangle \in H_{\mathrm{w}}$, and assigning different reshuffling matrices to those orthogonal subspaces of H_{w}. This framework can be exploited to achieve quantum certain computational targets [47]. The same framework of QW with conditionally reshuffled coin has been applied in [20], for a QW in complete graph $G = (V, E)$, in order to demonstrate its equivalence with Grover's algorithm.

In the rest of the section we review this result in the notation of the paper and emphasize the complementary research directions, i.e. while this work explores the direction "quantum search $\rightarrow$ QW", the work in [20] explores the opposite one, "QW$\rightarrow$quantum search".

Let us consider a general QW with conditionally reshuffled coin according to the partition $\mathbf{1}_{\mathrm{w}} = P_x + P_{x^\perp}$, with the step operator W_q where

$$W_q = V_{\mathrm{cl}}(C_0 \otimes P_{x^\perp} + C_1 \otimes P_x). \tag{70}$$

The choices $C_1 = -C_0$ leads to $W_q = V_{\mathrm{cl}}(C_0 \otimes (\mathbf{1}_{\mathrm{w}} - 2P_x))$, which upon choosing $C_0 = -U J_s U^\dagger$, leads to $W_q = V_{\mathrm{cl}}(U J_s U^\dagger \otimes J_{x^\perp})$. Assuming a self-loop attached at each vertex of the complete graph leads to $H_{\mathrm{w}} \approx H_{\mathrm{c}} \approx \mathbb{C}^{|V|}$ and further $V_{\mathrm{cl}} \equiv S$ can be identified with the swap operator $S = \sum_{i \in V} \sum_{j \in V} |j\rangle\langle i| \otimes |i\rangle\langle j|$, [20]. Using the action of the swap map and its idempotency $S^2 = \mathbf{1}$ leads to

$$W_q = (J_{x^\perp} \otimes U J_s U^\dagger) S = S(U J_s U^\dagger \otimes J_{x^\perp}). \tag{71}$$

Successive actions are obtained by inducing

$$W_q^{2k} = (U J_{x^\perp} U^\dagger J_s)^k \otimes U_G^k, \tag{72}$$

$$W_q^{2k+1} = S(U J_s U^\dagger \otimes J_{x^\perp})((U J_{x^\perp} U^\dagger J_s)^k \otimes U_G^k), \qquad k = 0, 1, 2, \ldots . \tag{73}$$

Note that at even steps $2k$ of the QW, in its second space, the search operator U_G^k of step k is realized. In this way the quadratic gain in QW diffusion speed is transferred to a quadratic gain of the laden quantum search taking place in the second Hilbert space. In fact, in the first space the Hermitian conjugate Grover operator is implemented. Indeed, the relation $\left(U J_{x^\perp} U^\dagger J_s\right)^k = J_{x^\perp} U_G^k J_{x^\perp}$ leads to

$$W_q^{2k} = J_x \otimes \mathbf{1} (U_G^k \otimes U_G^k) J_x \otimes \mathbf{1}, \tag{74}$$

which due to the oracle algebra relations

$$\begin{aligned} J_x \otimes \mathbf{1} &= (\mathbf{1}_{\mathrm{w}} - 2|x\rangle\langle x|) \otimes \mathbf{1} = \left(|x\rangle\langle x| + |x^\perp\rangle\langle x^\perp| - 2|x\rangle\langle x|\right) \otimes \mathbf{1} \\ &= \Sigma_3 \otimes \mathbf{1}, \end{aligned} \tag{75}$$

implying that $\Sigma_3 U_G \Sigma_3 = \Sigma_3 \exp(i\lambda\Sigma_2)\, \Sigma_3 = \exp(-i\lambda\Sigma_2) = U_G^\dagger$, leads to

$$W_q^{2k} = U_G^{k\dagger} \otimes U_G^k. \tag{76}$$

This expression justifies the choice of the name *double lane quantum search* for the even steps of QW driven by W_q, and implies that at an extra cost of two additional queries to the oracle the even step evolution of the QW is equivalent to a *double lane quantum search*. The initial state at each lane is taken to be the equal weighted state $|s\rangle$, so the evolved state

$$W_q^{2k} |s\rangle \otimes |s\rangle = U_G^{k\dagger} \otimes U_G^k (|s\rangle \otimes |s\rangle) = U_G^{k\dagger} |s\rangle \otimes U_G^k |s\rangle, \tag{77}$$

after $2k \approx \mathcal{O}(\sqrt{N})$ steps reaches the target state, i.e. $W_q^{2k} |s\rangle \otimes |s\rangle = |x\rangle \otimes |x\rangle$. This is the result obtained in [20] completed by showing that Grover's operator $U_G = U J_s U^\dagger J_{x^\perp}$ appears at both spaces (lanes), and that it is determined up to a SU(N) unitary U matrix (due to the general choice $C_0 = -U J_s U^\dagger$), as is the case in the original algorithm.

As with a single PQSA, in the double lane quantum search both unitary $U_G^k \otimes U_G^{k\dagger}$ can be affected by quantum noise along lines presented before. More explicitly, the transformation $\mathrm{Ad}U_G^{k\dagger} \otimes \mathrm{Ad}U_G^k(\rho_s \otimes \rho_s) \to \mathcal{E}_{2k}(\rho_s \otimes \rho_s)$ would implement the passage from the unitary evolution of QW search algorithm to an evolution driven my a unitary CP map, i.e. $W_q^{2k} \to \mathcal{E}_{2k}$, which would read as

$$\mathcal{E}_{2k} := \int_\Omega p(\theta) \mathrm{Ad}U_G^{k\dagger}(\theta) \otimes \mathrm{Ad}U_G^k(\theta) d\theta, \tag{78}$$

which suggest that $\mathcal{E}_{2k}$ describes a randomization of unitary evolution of QW via a continuous random variable $\theta \in \Omega$, following a $p(\theta) \geq 0$, $\int_\Omega p(\theta) d\mu(\theta) = 1$,

with the measure $d\mu(\theta)$). The map $\mathcal{E}_{2k}$ introduces a statistically correlated action of Grover's operators at both lanes, but other scenarios are also possible. Some of the studies of previous chapters with PQSA can be extended to this case.

Appendix A. Oracle algebra

The oracle-algebra A_f**.** Let the set $\Delta = \{1, 2, \ldots, N\}$, a subset $I \subset \Delta$, and the oracle function f be the characteristic function of I with k elements, defined as $f(i) = 1$, for $i \in I$, and $f(i) = 0$, for $i \notin I$. Let also the Hilbert space $l_2(\Delta)$, the vector

$$|x\rangle = \frac{1}{\sqrt{\nu}} \sum_{i=1}^{N} f(i)\,|i\rangle\,, \tag{79}$$

and its orthogonal vector

$$|x^{\perp}\rangle = \frac{1}{\sqrt{\nu^{\perp}}} \sum_{i=1}^{N} (1 - f(i))\,|i\rangle\,, \tag{80}$$

with $\nu = \sum_{i=1}^{N} f(i)$, and $\nu^{\perp} = \sum_{i=1}^{N}(1 - f(i))$. Next, introduce the $\Sigma_0, \Sigma_1, \Sigma_2$ and Σ_3 as the generators of A_f,

$$\Sigma_1 = |x\rangle\langle x^{\perp}| + |x^{\perp}\rangle\langle x|\,,\ \Sigma_2 = -i\,|x\rangle\langle x^{\perp}| + i|x^{\perp}\rangle\langle x|\,, \tag{81}$$

$$\Sigma_3 = |x\rangle\langle x| - |x^{\perp}\rangle\langle x^{\perp}|,\ \Sigma_0 = |x\rangle\langle x| + |x^{\perp}\rangle\langle x^{\perp}|. \tag{82}$$

DEFINITION. We define the *matrix oracle algebra* A_f with respect to the characteristic function f of $I \subset \Delta$ as set

$$A_f = \{A : A = \alpha\Sigma_0(f) + \beta\Sigma_1(f) + \gamma\Sigma_2(f) + \delta\Sigma_3(f);\ \alpha, \beta, \gamma, \delta \in \mathbb{R}\}, \tag{83}$$

where $\Sigma_{0,1,2,3}$ are Hermitian and satisfy the commutation relations $[\Sigma_a, \Sigma_b] = 2i\,\Sigma_c$ (cyclically), and $[\Sigma_0,$ everything$] = 0$. It follows that the set $\{\Sigma_0, \Sigma_1, \Sigma_2, \Sigma_3\}$ is analogous to the set of Pauli matrices and $A_f \approx \mathbf{u}(2)$, i.e. oracle algebra is isomorphic to the $\mathbf{u}(2)$ matrix algebra.

Representation theory: Let $H_2 \equiv \mathcal{V}_x = \text{span}\{|x\rangle\,, |x^{\perp}\rangle\}$ and $H_N = \text{span}\{|i\rangle\}_{i=1}^{N}$. There are two basic matrix representations: the two dimensional $\pi_2 : A_f \to \text{Lin}(H_2)$, and the N dimensional reducible one $\pi_N : A_f \to \text{Lin}(H_N)$. For the oracle function defined as before these representations read as $\pi_2(A) \equiv \pi_2(\alpha\Sigma_0 + \beta\Sigma_1 + \gamma\Sigma_2 + \delta\Sigma_3)$, where

$$\pi_2(A) = \begin{pmatrix} (\alpha + \delta) & (\beta - i\gamma) \\ (\beta + i\gamma) & (\alpha - \delta) \end{pmatrix}, \tag{84}$$

and $\pi_N(A) \equiv \pi_N(\alpha\Sigma_0 + \beta\Sigma_1 + \gamma\Sigma_2 + \delta\Sigma_3)$, where

$$\pi_N(A) = \begin{pmatrix} (\alpha + \delta)\frac{1}{k}\widehat{\mathbf{1}}_{k\times k} & (\beta - i\gamma)\frac{1}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{k\times(N-k)} \\ (\beta + i\gamma)\frac{1}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{(N-k)\times k} & (\alpha - \delta)\frac{1}{N-k}\widehat{\mathbf{1}}_{(N-k)\times(N-k)} \end{pmatrix}, \tag{85}$$

and $(\widehat{\mathbf{1}}_{st})_{ij} = 1,\ 1 \le i \le s, 1 \le j \le t$.

Numerical examples:

(i) For $N = 4$, $k = 1$, with $f(1) = 1$ and zero elsewhere, we obtain

$$\pi_4(\Sigma_1) = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \qquad \pi_4(\Sigma_-) = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\pi_4(\Sigma_2) = \frac{i}{\sqrt{3}} \begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}, \qquad \pi_4(\Sigma_+) = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \tag{86}$$

$$\pi_4(\Sigma_3) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1/3 & -1/3 & -1/3 \\ 0 & -1/3 & -1/3 & -1/3 \\ 0 & -1/3 & -1/3 & -1/3 \end{pmatrix}, \quad \pi_4(\Sigma_0) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/3 & 1/3 & 1/3 \\ 0 & 1/3 & 1/3 & 1/3 \\ 0 & 1/3 & 1/3 & 1/3 \end{pmatrix}.$$

(ii) In Appendix of [19] the matrices of the oracle algebra generators for $N = 8$, $k = 2$, with $f(1) = 1$, $f(2) = 1$, have been explicitly presented.

REMARK. The N-dimensional representation for the elements $U_j = \exp(i\varphi_j \Sigma_j)$, $j = 1, 2, 3$ of oracle algebra $A_f \subset \mathbf{su}(N)$, is

$$\pi_N(U_j) = \pi_N(\exp(i\varphi_j \Sigma_j)) = \exp(i\varphi_j \pi_N(\Sigma_j)) \tag{87}$$

$$= \pi_N(\Sigma_0)\cos\varphi_j + i\pi_N(\Sigma_j)\sin\varphi_j, \tag{88}$$

namely

$$\pi_N(U_1) = \begin{pmatrix} \frac{1}{k}\widehat{\mathbf{1}}_{k\times k}\cos\varphi_1 & i\frac{1}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{k\times(N-k)}\sin\varphi_1 \\ i\frac{1}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{(N-k)\times k}\sin\varphi_1 & \frac{1}{N-k}\widehat{\mathbf{1}}_{(N-k)\times(N-k)}\cos\varphi_1 \end{pmatrix}, \tag{89}$$

$$\pi_N(U_2) = \begin{pmatrix} \frac{1}{k}\widehat{\mathbf{1}}_{k\times k}\cos\varphi_2 & \frac{1}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{k\times(N-k)}\sin\varphi_2 \\ -\frac{1}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{(N-k)\times k}\sin\varphi_2 & \frac{1}{N-k}\widehat{\mathbf{1}}_{(N-k)\times(N-k)}\cos\varphi_2 \end{pmatrix}, \tag{90}$$

and

$$\pi_N(U_3) = \begin{pmatrix} \frac{1}{k}\exp(i\varphi_3)\widehat{\mathbf{1}}_{k\times k} & \widehat{\mathbf{0}}_{k\times(N-k)} \\ \widehat{\mathbf{0}}_{(N-k)\times k} & \frac{1}{N-k}\exp(-i\varphi_3)\widehat{\mathbf{1}}_{(N-k)\times(N-k)} \end{pmatrix}. \tag{91}$$

Appendix B. CP maps

CPTP maps. Let us take a finite dimensional Hilbert space H and let the set of endomorphisms $\mathrm{End}(H)$. A *positive* map $\mathcal{E} : \mathrm{End}(H) \to \mathrm{End}(H)$, gives $\mathcal{E}(X) \geq 0$ for any positive element $X \in \mathrm{End}(H)$. Given a (normalized) element $|\Psi\rangle \in H$, its rank one projection operator is $\rho_\Psi = |\Psi\rangle\langle\Psi|$. Let P be the set of all such ρ_Ψ elements. Let further $D =$ convex hull(P) be the set of density matrices $\rho \in D$, where any ρ is positive, Hermitian and of unit trace. Those elements describe the *state* of a quantum system in H.

A completely positive trace preserving (CPTP) map $\mathcal{E} : D \to D$ transforms density matrices into themselves, namely $\mathcal{E}(\rho)$ is positive, Hermitian and trace one matrix. Additionally it is *completely positive*, namely for any $n \in \mathbb{N}$, the extension map $\mathrm{id}_n \otimes \mathcal{E}$ acting on $M_n \otimes D$, where M_n is the algebra of square matrices of dimension n, is again positive [25, 45].

There are two possible ways to represent a CPTP map $\mathcal{E}$. One is the *operator sum representation (OPS):* there is a set of operators $\{S_i\}_{i=1}^n$ (the so-called Kraus generators), with the normalization $\sum_{i=1}^n S_i^\dagger S_i = \mathbf{1}$, such that $\mathcal{E}(\rho) = \sum_{i=1}^n S_i \rho S_i^\dagger$. The operator sum representation has a unitary freedom (the unitary equivalence of Kraus generators) [25], namely, for two sets of Kraus generators $\{S_i\}_{i=1}^n$ and $\{S_i'\}_{i=1}^n$, the equality $\mathcal{E}(\rho) = \sum_{i=1}^n S_i \rho S_i^\dagger = \sum_{i=1}^n S_i' \rho S_i'^\dagger$ holds iff there is a unitary matrix $U = [u_{kl}]$ such that, $S_i' = \sum_{l=1}^n u_{il} S_l$.

The second representation is the *unitary dilation representation (UDL):* let us take an auxiliary Hilbert space H_A of some finite dimension and let us take a quantum system with state space H_A, and let ρ_A be its density matrix, then there is a unitary operator V acting on $H_A \otimes H$ such that $\mathcal{E}(\rho) = \mathrm{Tr}_A V(\rho_A \otimes \rho) V^\dagger$, where Tr_A is the partial trace with respect to the auxiliary space H_A[25, 46]. The interrelation between OPS and UDL representations is given by choosing $\rho_A = |a\rangle\langle a|$ for some basis vector in H_A, and then we obtain for the Kraus generators $S_i = \langle i|U|a\rangle$, i.e. they are located in the a column of unitary U.

Acknowledgement

One of us (Ch. K) acknowledges the PhD Scholarship from the Technical University of Crete.

REFERENCES

[1] L. Grover: Quantum mechanics helps in searching for needle in a haystack, *Phys. Rev. Lett.* **78** (1997), 325–328.

[2] L. Grover: A fast quantum mechanical algorithm for database search, *Proc. 28th Ann. ACM Symp. on the Theory of Computing*, ACM Press, pp. 212–218. New York 1996.

[3] L. Grover: Quantum computers can search rapidly by using almost any transformation, *Phys. Rev. Lett.* **80** (1998), 4329–4332.

[4] M. Boyer, G. Brassard, P. Hoyer and A. Tapp: Tight bounds on quantum searching, *Proc. of 4th Workshop on Physics and Computation*, pp. 36–43 (1996).

[5] A. Ambainis: Quantum search algorithms, *SIGACT News* **35** (2) (2004), 22–35.

[6] J. Janmark, D. A. Meyer and T. G. Wong,: Global symmetry is unnecessary for fast quantum search, *Phys. Rev. Lett.* **112** (2014), 210502.
[7] S. D. Berry and J. B. Wang: Quantum-walk-based search and centrality, *Phys. Rev. A* **82** (2010), 042333.
[8] D. Shapira, S. Mozes and O. Biham: The effect of unitary noise on Grover's quantum search algorithm, *Phys. Rev. A* **67** (4) (2003), 042301.
[9] N. Shenvi, K. P. Brown and K. B. Whaley: Effects of noisy oracle on search algorithm complexity, *Phys. Rev. A* **68** (2003), 052313.
[10] H. Buhrman et al.: Robust polynomials and quantum algorithms, *STACS 2005*, Eds. V. Dickert et al., LNCS, Vol. 3404, pp. 503. Springer, Heidelberg 2005.
[11] P. Gawron, J. Klamka and R. Winiarczyk: Noise effects in the quantum search algorithm from the viewpoint of computational complexity, *Int. J. Appl. Math. Comp. Sci.* **22** (2) (2012), 493.
[12] O. Regev and L. Schiff: *Impossibility of a Quantum Speed-Up with a Faulty Oracle*, Eds. L. Aceto et al. ICALP 2008, Part I. LNCS,Vol. 5125, pp. 773-781. Springer, Heidelberg 2008.
[13] A. Ambainis, A. Backurs, N. Nahimovs and A. Rivosh: *Grover's Algorithm with Errors*, MEMICS, 180–189 (2012).
[14] E. B. Davies: *The Quantum Theory of Open Systems*, Academic Press, London 1976.
[15] R. Alicki and K. Lendi: *Quantum Dynamical Semigroups and Their Applications*, Springer, Berlin 1987.
[16] H. P. Breuer and F. Petruccione: *The Theory of Open Quantum Systems*, Oxford Univ. Press, Oxford 2002.
[17] D. D. Bhaktavatsala and M. Mølmer: Effect of qubit losses on Grover's quantum search algorithm, *Phys. Rev.* **86** (2012), 04231..
[18] D. Ellinas and C. Konstandakis: *Oracle Lie algebra for quantum search algorithm: non unitary symmetries and entanglement*, *QCMC 2010, AIP Conference Proceedings Series*, eds. T. Ralph and P. K. Lam, pp. 4 (2011).
[19] D. Ellinas and C. Konstandakis: Parametric quantum search algorithm by CP maps: algebraic, geometric and complexity aspects, *J. Phys. A: Theoretical and Mathematical* **46** (2013), 415303.
[20] A. Ambainis, J. Kempe and A. Rivosh: Coin make quantum walks faster, *Proc. 16th ACM-SIAM SODA*, p. 1099–1108 (2005).
[21] R. A. Horn and C. R. Johnson: *Matrix Analysis*, Cambridge University Press, Cambridge (1990).
[22] I. L. Chuang and Y. Yamamoto: Creation of a persistent bit using error correction, *Phys. Rev. A.* **55** (1997), 114.
[23] R. Jozsa: *Searching in Grover's Algorithm*, ArXiv. http://arxiv.org/abs/quant-ph/9901021 (1999).
[24] K. Kraus: *States, Effects and Operations*, Springer, Berlin 1983.
[25] M. A. Nielsen and I. L. Chuang: *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge 2000.
[26] K. M. R. Audenaert and S. Scheel: On random unitary channels, *New J. Phys.* **10** (2008), 023011.
[27] R. Feynman: Simulating physics with computers, *Int. J. Theor. Phys.* **21** (1982), 467–488.
[28] S. Lloyd: Universal quantum simulators, *Science* **273** (1996), 1073–1078.
[29] I. Buluta and F. Nori: Quantum Simulators, *Science* **326** (2009), 108–111.
[30] R. Somma, G. Ortiz, J. E. Gubernatis, E. Knill and R. Laflamme: Simulating physical phenomena by quantum networks, *Phys. Rev. A* **65** (2002), 042323.
[31] J. Kempe: Quantum random walks-an introductory overview, *Contemp. Phys.* **44** (2003), 302.
[32] N. Konno: *Quantum Walks*, In: *Quantum Potential Theory*. Franz, Schürmann eds., Lecture Notes in Mathematics, Vol. 1954, pp. 309–452. Springer, Berlin-Heidelberg-New York 2009.
[33] Y. Aharonov, L. Davidovich and N. Zagury: Quantum random walks, *Phys. Rev. A* **48** (1993), 1687.
[34] A. Ambainis, E. Bach, A. Nayak, A. Vishwanath and J. Watrous: One-dimensional quantum walks, *Proc. 33rd Annual ACM STOC*, 37–49 (2001).
[35] E. Bach, S. Coppersmith, M. P. Goldschen, R. Joynt, and J. Watrous: *One-dimensional quantum walks with absorbing boundaries*, ArXiv. http://arxiv.org/abs/quant-ph/0207008.
[36] D. Aharonov, A. Ambainis, J. Kempe and U. V. Vazirani: Quantum walks on graphs, *Proceedings of the 33rd Annual ACM symposium on Theory of Computing*, 50–59 (2001).

[37] N. Konno: One-dimensional discrete-time quantum walks on random environments, *Quantum Inf. Process* **8** (2009), 387–399.
[38] D. Ellinas and I. Smyrnakis: Quantum optical random walk: quantization rules and quantum simulation of asymptotics, *Phys. Rev. A* **76** (2007), 022333.
[39] D. Ellinas and P. D. Jarvis: Quantum simulation of phylogenetic trees, ArXiv. http://xxx.tau.ac.il/abs/1105.1582.
[40] D. Ellinas: *Convex geometry of quantum walks*, work in progress.
[41] A. W. Marshall and I. Olkin: Inequalities: *Theory of Majorization and Its Applications*, Academic Press, New York 1979.
[42] A. Horn: Doubly stochastic matrices and the diagonal of a rotation matrix, *Am. J. Math.* **76** (1954), 620–630.
[43] D. Ellinas, A. J. Bracken and I. Smyrnakis: Discrete randomness in discrete time quantum walk: study via stochastic averaging, *Rep. Math. Phys.* **70** (2012), 221.
[44] G. Birkhoff: Tres observaciones sobre el algebra lineal, *Univ. Nac. Tucumán Rev. Ser. A,* **5** (1946), 147–151.
[45] M. D. Choi: Completely positive linear maps on complex matrices, *Linear Algebra Appl.* **10** (1975), 285.
[46] W. F. Stinespring: Positive functions on C*-algebras, *Proc. Amer. Math. Soc.* **6** (1955), 211.
[47] D. Ellinas: 2015 unpublished.

Fast Counting Fuelled by Entanglement: Quantum Search new Harness

Demosthenes Ellinas* and Christos Konstandakis**
Technical University of Crete
School of Electrical & Computer Engineering QLab
GR 731 00 Chania Crete Greece
* *ellinas@ece.tuc.gr*, ** *konstandakis@science.tuc.gr*

Counting the size of a set requires as many counts as set's cardinality, say N. Employing single item search algorithm of N dimensional database and the entanglement between any two parts of database space during search leads to fast counting. Demonstrating the periodic projectivity of reduced density matrix ensuing by decoupling fraction of qubits from database state and monitoring entanglement measures being periodically vanishing with period O(sqrt(N)) leads to quadratic speed up of counting. By rigging marked item initial probability a hyper-quadratic acceleration of counting is achieved.

Introduction : Counting the number of elements of given finite set $\mathcal{S}$ requires a number of counts equal to the cardinality N of the set itself, one count for each element, as common sense asserts.

Fast counting is a novel method to address this problem in the quantum setting, achieving counting in quadratically less than N counts, in the worse case scenario, by casting the counting problem in the language of quantum algorithms. This work shows fast counting to be possible by employing Grover's search algorithm [1–4], reformulated mathematically in terms of the so called "oracle matrix algebra" [5–7], by treating set $\mathcal{S}$ as a search-able database with no additional structure. Within this formalism, search appears as a $SU(2)$ periodic orbit, formed by a collection of qubits encoding algorithm's database which is identified with set $\mathcal{S}$. We assume, as a rule of the game, that the number N is known to a search-algorithm builder which is solicited to set up a quantum search procedure with a single marked item in a database of size N. The output of searching, expressed by the quantum entanglement developed between two arbitrary parts of database space, in the form of a sequence wrt to iteration number, can be utilized for fast counting. Indeed it is shown that entanglement quantified by various measures have a periodic vanishing behaviour during specific moments of searching, with a period of order $\mathcal{O}(\sqrt{N})$ for $N \gg 1$. Hence a quantum measurement of the entanglement enables the determination of cardinality N quadratically faster than classical counting.

In more concrete terms the main result is expressed by saying that quantum search can alternatively be harnessed to quadratically accelerate the finding the size of a set by mining the multi-particle entanglement built among database qubits in the course of search. This is accomplished by demonstrating and exploiting the periodic projectivity of the reduced density matrix ensuing by de-coupling a fraction of qubits from the total database state. The effect is quantified by showing that a general set of entanglement measures (e.g. Renyi, von Neumann and Wooters) [8–10], are vanishing periodically at identical moments during search, with period $\mathcal{O}(\sqrt{N})$ wrt the number of iterations which are identified with counts of cardinality. A Hamiltonian model and an appropriate observable are constructed which provide an operational way of simulating the measurements of quantum entanglement. Finally going beyond the quadratic speed up of counting it is shown that by rigging the initial probability of the marked item, (stemmed either by prior information or guess about the item), a hyper-quadratic shortening of the classical counting complexity of the cardinality is achieved.

I. QUANTUM SEARCH WITH RIGGED MARKED ITEM PROBABILITY

Define $\mathcal{D}_M = \{\rho \in \mathcal{M}_M(\mathbb{C}); \rho^\dagger = \rho, \rho > 0, Tr\rho = 1\}$. Let $\{p_j\}_{j=1}^N$ be the initial distribution of items-vector in database Hilbert space. Mark a single item $|x\rangle$ with probability $p_x \equiv p \in (0,1)$, so that the initial vector $|\widetilde{s}\rangle = \sum_{j=1}^N \sqrt{p_j}\,|j\rangle$ equals $|\widetilde{s}\rangle = (\cos\widetilde{\alpha})\,|x\rangle + (\sin\widetilde{\alpha})\,|x^\perp\rangle$, where $|x^\perp\rangle = \frac{1}{\sqrt{1-p}}\sum_{j\neq x}\sqrt{p_j}\,|j\rangle$, and $\widetilde{\alpha} = \cos^{-1}(\sqrt{p})$. Operating m times on the initial state $\pi_N(\widetilde{\rho}_s) = |\widetilde{s}\rangle\langle\widetilde{s}|$, with search operator $\pi_N(\widetilde{U_G}) = \exp(i\widetilde{\theta}\pi_N(\Sigma_2))$, where $\widetilde{\theta} = \pi - 2\widetilde{\alpha}$, yields a state that projects on target item $\pi_N(\widetilde{\rho}_x) = |x\rangle\langle x|$, with probability

$$\widetilde{p}(m) = Tr\left[\pi_N(\widetilde{\rho}(m))\pi_N(\widetilde{\rho}_x)\right] = \cos^2(\widetilde{\alpha} - m\widetilde{\theta}).$$

At m-th step the density matrix is

$$\begin{aligned}\pi_N(\widetilde{\rho}(m)) &\equiv \widetilde{U_G}^m \pi_N(\widetilde{\rho}_s)\widetilde{U_G}^{m\dagger} \\ &= \frac{1}{2}\left(\pi_N(\Sigma_0) + \widetilde{s}_1(m)\pi_N(\Sigma_1) + \widetilde{s}_3(m)\pi_N(\Sigma_1)\right)\end{aligned} \tag{1}$$

with $\widetilde{s}_1(m) \equiv \langle \Sigma_1 \rangle = -\sin(2m\widetilde{\theta} - 2\widetilde{\alpha})$, $\widetilde{s}_3(m) \equiv \langle \Sigma_3 \rangle = \cos(2m\widetilde{\theta} - 2\widetilde{\alpha})$, where $\langle \Sigma_{1,3} \rangle = \pi_S(\widetilde{\rho}^{(s)}\Sigma_{1,3})$ the mean values of the algebra generators, abbreviated to $\widetilde{s}_i \equiv \langle \Sigma_i \rangle$. The first time when $\widetilde{p}(m) = 1$, equals $m = \widetilde{m}(p) = \frac{\widetilde{\alpha}}{\widetilde{\theta}} = \frac{\cos^{-1}(\sqrt{p})}{\sin^{-1}(2\sqrt{p-p^2})}$. Initial and target states are unitarily related i.e. $|\widetilde{s}\rangle = \pi_N(\widetilde{R})\,|x\rangle \equiv \exp(-i\widetilde{\alpha}\pi_N(\Sigma_2))\,|x\rangle$. The evolved state $\left|\widetilde{s}^{(m)}\right\rangle = \pi_N(\widetilde{U_G}^m)\,|\widetilde{s}\rangle$, projects on the target state with probability $\widetilde{p}(m) = |\left\langle x|\widetilde{s}^{(m)}\right\rangle|^2$, determined exclusively by the xx- matrix element of the combined unitary operators $\pi_N(\widetilde{U_G}^m \cdot \widetilde{R})$, explicitly $\widetilde{p}(m) = \langle x|\,[\pi_N(\widetilde{U_G}^m \cdot \widetilde{R}) \circ \pi_N(\widetilde{U_G}^m \cdot \widetilde{R})^*]\,|x\rangle$, i.e. by the xx-matrix element of its element-wise product with its complex conjugate. This suggests that any unitary transformation on the initial vector $|\widetilde{s}\rangle \to V\,|\widetilde{s}\rangle$ that accepts the marked vector as fixed point up to a phase i.e. $V\,|x\rangle = e^{i\phi}\,|x\rangle$, gives an equal complexity search algorithm; such transformations belong to $U(1) \otimes U(N-1)$ group, hence the algorithm's search evolution orbit $\left|s^{(m)}\right\rangle$ belongs to the $U(N)/U(1) \otimes U(N-1) = CP^{N-1}$ Grassmannian space (see also the hidden subgroup problem aspects of Grover's algorithm [11]).

The asymptotic limit when $0 < p \ll 1$ and $N \to \infty$, yields $\widetilde{\theta}(p) = \mathcal{O}(p^{\frac{1}{2}})$ and $\widetilde{m}(p) = \mathcal{O}(\frac{\pi}{4\sqrt{p}})$. Some indicative choices of probability p would provide new possibilities for search complexity and associated counting time. The following cases of p are interesting for $\widetilde{p}(\widetilde{m}(p)) = 1$: i) in general for $0 < p \ll 1$, we obtain $\widetilde{m} \approx \mathcal{O}(1/\sqrt{p})$; ii) for $p = 1/N$ and $N \gg 1$ we obtain the standard optimal result $\widetilde{m} \approx \mathcal{O}(\frac{\pi}{4}\sqrt{N})$; iii) For quadratically larger item probability $p = 1/\sqrt{N}$ and $N \gg 1$, we obtain a quadratic speed up of search complexity $\widetilde{m} \approx \mathcal{O}(\frac{\pi}{4}N^{1/4})$; iv) slowing down parameter $\widetilde{m}$ below its classical value (with $p = 1/N$), is also possible: e.g. the choice $p = 1/N^2$ yields $\widetilde{m} \approx \mathcal{O}(N)$, while if $p = 1/N^3$ then $\widetilde{m} \approx \mathcal{O}(N\sqrt{N})$.

II. REDUCED SYSTEMS OF DATABASE QUBITS

Let $N = 2^n$, $k = 1$ (one marked item, e.g. $|1\rangle$), and $R = 2^r$, and let $L = N/R$. We get the r-qubit reduced density matrix $\pi_R(\widetilde{\rho}^{(r)}(m))$ from the n-qubit one by tracing out $(n-r)-$qubits (without including the marked item). Adopting a unifying way of describing the density matrix for the $s = n$ total qubits or $s = r$ remaining qubits which correspond to dimensions $S = N, R$, we write

$$\pi_S(\widetilde{\rho}^{(s)}) = \tfrac{1}{2}(\pi_S(\Sigma_0) + (x^{(s)} - (S-1)w^{(s)})\pi_S(\Sigma_3) + 2y^{(s)}\sqrt{S-1}\pi_S(\Sigma_1)).$$

The following outline shows the parameters relevant to the two cases:

$$\begin{array}{c} x^{(n)}, y^{(n)}, w^{(n)} \\ \updownarrow \\ x^{(r)}, y^{(r)}, w^{(r)} \end{array} \begin{array}{c} \searrow \\ \\ \nearrow \end{array} \widetilde{a}(k,p), \widetilde{b}(k,p) \longleftrightarrow \langle \Sigma_{1,3} \rangle \,.$$

The two sets of Bloch vector components are related as: $x^{(n)} = \widetilde{a}^2, y^{(n)} = \widetilde{a}\widetilde{b}, w^{(n)} = \widetilde{b}^2$ and $x^{(r)} = x^{(n)} + (L-1)w^{(n)}, y^{(r)} = \sqrt{x^{(n)}w^{(n)}} + (L-1)w^{(n)}$, and $w^{(r)} = Lw^{(n)}$, where $\widetilde{a}(m) = \cos(\widetilde{\alpha} - m\widetilde{\theta})$, and $\widetilde{b}(m) = \frac{1}{\sqrt{N-1}}\sin(\widetilde{\alpha} - m\widetilde{\theta})$. Explicitly the S dimensional density matrix reads

$$\pi_S(\widetilde{\rho}^{(s)}(m)) = \begin{pmatrix} x^{(s)} & y^{(s)} & ... & y^{(s)} \\ y^{(s)} & w^{(s)} & ... & w^{(s)} \\ \vdots & \vdots & \ddots & \vdots \\ y^{(s)} & w^{(s)} & ... & w^{(s)} \end{pmatrix},$$

where $x^{(s)} = \frac{1}{2}(1 + \langle \Sigma_3 \rangle)$, $y^{(s)} = \frac{1}{\sqrt{S-1}}\langle \Sigma_1 \rangle$, $w^{(s)} = \frac{1}{2(S-1)}(1 - \langle \Sigma_3 \rangle)$.

Remarks: 1) Consider the particular cases $k = 1, 3$ (one, three marked items), with vectors $|1\rangle$, and $\{|2\rangle, |3\rangle, |4\rangle\}$

respectively. The density matrix $\pi_N(\widetilde{\rho}^{(n)}(m))$ in its N dimensional representation reads respectively,

$$\pi_N(\widetilde{\rho}(m)) = \begin{pmatrix} \bigstar & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \cdots \\ \blacksquare & \blacktriangledown & \blacktriangledown & \blacktriangledown & \blacktriangledown & \cdots \\ \blacksquare & \blacktriangledown & \blacktriangledown & \blacktriangledown & \blacktriangledown & \cdots \\ \blacksquare & \blacktriangledown & \blacktriangledown & \blacktriangledown & \blacktriangledown & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix},$$

$$\pi_N(\widetilde{\rho}(m)) = \begin{pmatrix} \blacktriangledown & \blacksquare & \blacksquare & \blacksquare & \blacktriangledown & \cdots \\ \blacksquare & \bigstar & \bigstar & \bigstar & \blacksquare & \cdots \\ \blacksquare & \bigstar & \bigstar & \bigstar & \blacksquare & \cdots \\ \blacksquare & \bigstar & \bigstar & \bigstar & \blacksquare & \cdots \\ \blacktriangledown & \blacksquare & \blacksquare & \blacksquare & \blacktriangledown & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix},$$

where the following notation has been introduced: $\bigstar = \frac{1}{2} + \frac{1}{2}\widetilde{s}_3(m) = \cos^2(\widetilde{\alpha} - m\widetilde{\theta}), \blacktriangledown = \frac{1}{N-1}(\frac{1}{2} - \frac{1}{2}\widetilde{s}_3(m)) = \frac{1}{N-1}\sin^2(\widetilde{\alpha} - m\widetilde{\theta})$, and $\blacksquare = \frac{1}{\sqrt{N-1}}\widetilde{s}_1(m) = \cos(\widetilde{\alpha} - m\widetilde{\theta})\sin(\widetilde{\alpha} - m\widetilde{\theta})$. Bloch vector components and density matrix $\pi_N(\widetilde{\rho}^{(n)}(m))$ decomposed in oracle algebra as in eq.(1). The structure of the matrix is a cross with cross point filled with $k \times k$ stars and crossing lines decorated with boxes while the rest sites are filled with triangles. While the thickness and position of the crossing box varies depending k the shape of the cross is permanent and characterizes the underline oracle algebra structure of the algorithm.

2) Matrices $\pi_N(\widetilde{\rho}^{(n)}(m))$, $\pi_R(\widetilde{\rho}^{(r)}(m))$ are homogeneous of degree 2 with respect to their arguments $\widetilde{a}$, $\widetilde{b}$.

3) The success probability is periodic wrt m, i.e. $\widetilde{p}(m + \widetilde{T}) = \widetilde{p}(m)$ with period $\widetilde{T} = \pi/\widetilde{\theta}$. This implies that $\widetilde{a}(m), \widetilde{b}(m)$ are periodic functions with period $2\widetilde{T}$; then any homogeneous functions of degree 2 wrt $\widetilde{a}(m), \widetilde{b}(m)$ are also periodic with period $\widetilde{T}$. E.g. the components $\widetilde{s}_{1,3}(m)$ and $\widetilde{s}^{(r)}_{1,3}$ are periodic with period $\widetilde{T}$. This induces periodicity to $\widetilde{\rho}(m)$ and to each of its matrix representations i.e, $\pi_S(\widetilde{\rho}^{(s)}(m + \widetilde{T})) = \pi_S(\widetilde{\rho}^{(s)}(m))$.

4) Analytic functions of $\widetilde{\rho}(m)$ (e.g. entanglement measures) are periodic wrt m with period equal to the period of the smallest non-zero degree monomial in $\widetilde{\rho}(m)$.

5) If $0 < p < 1$, e.g. $p \approx 1$ then $\lim_{p\to 1} \widetilde{m}(p) = \frac{1}{2}$, so practically the target item is reached after a single step.

6) In the uniform case of not rigged probability i.e. $p = \frac{1}{N}$, the tilted parameters become untilded i.e. angles $\widetilde{\alpha}, \widetilde{\theta}$ and parameters $\widetilde{a}(m), \widetilde{b}(m)$, become respectively $\alpha = \arccos(\sqrt{1/N})$, $\theta = \arcsin(2\sqrt{N-1}/N)$, and $a(m) = \cos(\alpha - m\theta), b(m) = \frac{1}{\sqrt{N-1}}\sin(\alpha - m\theta)$. For $N \gg 1$, we have $\widetilde{m} \to \frac{\pi}{4}\sqrt{N} = \mathcal{O}(\sqrt{N})$.

Entanglement in quantum search Next we investigate the periodicity of variation of quantum entanglement in the course of search. Designate by m_* and m_{**} two sequences of *moments of projectivity* of density matrix, meaning steps m, when $\rho(m)$ becomes projective matrix.

Proposition : Let any functional measure $F : \mathcal{D}_N \to \mathbb{C}$, on the density matrix set $\mathcal{D}_N$, either of polynomial or analytic type, such that $F(\rho) = 0$ iff $\rho^2 = \rho$. Consider density matrix $\pi_R(\widetilde{\rho}^n(m)) = \widetilde{U_G}^m |\widetilde{s}\rangle \langle\widetilde{s}|\widetilde{U_G}^{\dagger m}$, when it is reduced to a state of arbitrary r qubits i.e. $\pi_R(\widetilde{\rho}^{(r)}) = Tr_{n-r}\pi_N(\widetilde{\rho}^{(n)})$; the following properties are satisfied by $\widetilde{\rho}^{(r)}(m)$: i) it is a periodic state wrt m, i.e. $\pi_R(\widetilde{\rho}^{(r)}(m+\widetilde{T})) = \pi_R(\widetilde{\rho}^{(r)}(m))$ in any representation π_R of the oracle algebra A_f; ii) during the course of search it becomes a projective state (pure state) for any r i.e. $\left(\pi_R(\rho^{(r)}(\widetilde{m}))\right)^2 = \pi_R(\rho^{(r)}(\widetilde{m}))$ at moments given by arithmetic progressions $\widetilde{m}_* = \{\widetilde{m} + k\widetilde{T}\}_{k=0}^{\infty}$ or $\widetilde{m}_{**} = \{\widetilde{m} - \frac{1}{\widetilde{\theta}}\arctan(\sqrt{N-1}) + k\widetilde{T}\}_{k=0}^{\infty}$. The asymptotic form of these sequences for the case $N \gg 1$, and in general $0 < p \ll 1$, are $\widetilde{m}_*^{\infty} = \{(2k+1)\left\lfloor \frac{\pi}{4\sqrt{p}} \right\rfloor\}_{k=0}^{\infty}$ or $\widetilde{m}_{**}^{\infty} = \{k\left\lfloor \frac{\pi}{2\sqrt{p}} \right\rfloor\}_{k=0}^{\infty}$, and in particular in the uniform case, when $p = \frac{1}{N}$, we have respectively that $\widetilde{m}_*^{\infty} = \{(2k+1)\left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor\}_{k=0}^{\infty}$, or $\widetilde{m}_{**}^{\infty} = \{k\left\lfloor \frac{\pi}{2}\sqrt{N} \right\rfloor\}_{k=0}^{\infty}$.

Entanglement measures : Next we specialize to important cases of entanglement measures, such as: Quantum Renyi (R), von Neumann entropies (vN), and Wooters concurrence (W) [8–10], for reduced density matrix $\rho^{(r)}(m)$. Figures 1 and 2 display the three measures for $p = 1/N$ (Fig. 1), and Renyi entropy for $p = 1/N, 1/\sqrt{N}$ (Fig. 2); details in figure captions. The important point displayed is that all zeros of entropies are placed on the horizontal line of m's and they belong to two inter-lasing sequences $\widetilde{m}_*$ and $\widetilde{m}_{**}$, and this is true for any of the three displayed measures i.e. R, vN and W. The distance between every second zero equals the period $\widetilde{T}$ which is related to probability p via formula $p = \frac{1}{2}(1 \pm \cos(\pi/\widetilde{T}))$, (see Sup. Mat.)

Periodic entropy and fast counting : Once we have determined sequences $\widetilde{m}_*$, $\widetilde{m}_{**}$ and their common period $\widetilde{T}$ and choose p to be equal to one of the discussed values e.g. $p = \frac{1}{N^l}$, then we can observe, by means of suitable quantum

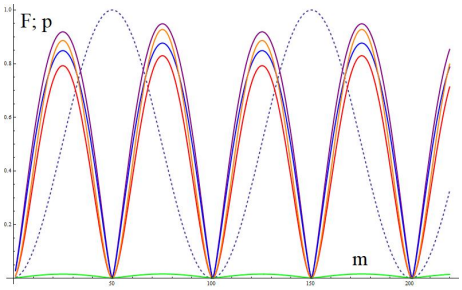


FIG. 1: For $N = 2^{12}$ $p = 1/N$. Lines: Dashed success prob; Entropies: von Neumann, Red: $r = 2$; Orange $r = 3$; Renyi, Blue: $r = 2, a = 0.7$; Purple: $r = 3, a = 0.7$; Concurrence: Green: $C_{1,1}$.

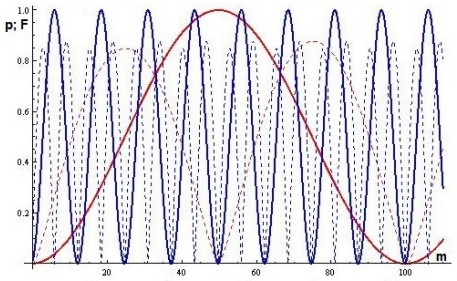


FIG. 2: Lines: Red: success prob. for $p = 1/N$; Blue: success prob. for $p = 1/\sqrt{N}$; Red dashed: Renyi entropy for $p = 1/N, r = 2, a = 0.7$; Blue dashed: Renyi entropy for $p = 1/\sqrt{N}, r = 2, a = 0.7$

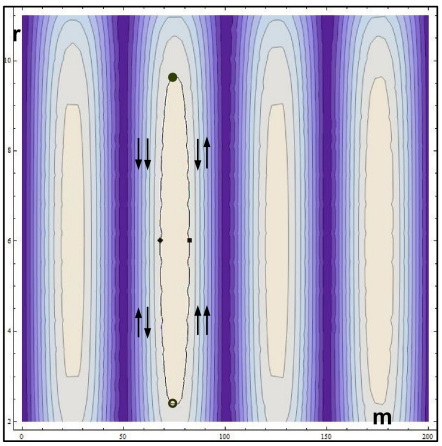


FIG. 3: For $N = 2^{12}$, $a = 0.7$, $2 \leq r \leq 11$, $0 \leq m \leq 200$, Renyi entropy (Contour Plot)

measurement, the period $\widetilde{T}$ of an entropic measure of entanglement, which will enable us to determine the size N via the formula $N = \left\lfloor (\sin^2(\frac{\pi}{2\widetilde{T}}))^{-1/l} \right\rfloor$. This would amount to counting the size of the set in question and in fact relates in a simple way quantum search with the fast counting problem.

Quantum measurement of linear entropy: Next we provide a operation way of obtaining the linear entropy S_L of the reduced density of matrix of quantum search at a step m describing r remaining qubits. Since S_L provides a measure of entanglement between database qubits, then a quantum measurement like access to S_L and its possible implementation would be an indispensable aspect of fast counting algorithm. The following lemma summarizes the operational procedure.

Lemma 1: *The linear entropy* $S_L(\rho)$ *of reduced evolved density matrix* $\rho \equiv \rho^{(m;r)}$ *equals* $S_L(\rho) = 1 - \left\langle \mathcal{E}(\rho^{\otimes 2})(\Sigma_3 \otimes \Sigma_3) \right\rangle$, *where the map* $\mathcal{E}(\rho^{\otimes 2}) = \frac{1}{2}\rho^{\otimes 2} + \frac{1}{2}(\Sigma_2 \otimes \Sigma_2)\rho^{\otimes 2}(\Sigma_2 \otimes \Sigma_2)^\dagger$ *identified as a generalized* Y *channel is unitarily generated as* $\mathcal{E}(\rho^{\otimes 2}) = Tr_{aux} V(\rho_{aux} \otimes \rho^{\otimes 2})V^\dagger$, *where a unitary dilation* $V = e^{iH}$ *is generated by the Hamiltonian* $H = -\arctan(\frac{1}{\sqrt{2}})\sigma_2 \otimes (\Sigma_2 \otimes \Sigma_2)$, *by means of an auxiliary qubit in state* $\rho_{aux} = |0\rangle\langle 0|$.

Renyi entropy periodicity and equal entanglement configurations: The general measure in the form of Renyi entropy requires the powers of the reduced density which are provided, for the case of integer powers, below in lemma 2.

Lemma 2: *Let the* S *dimensional reduced density matrix* $\pi_S(\widetilde{\rho}^{(s)}(m))$, *its* m*-th power for all* $\mathbb{N} \ni m \geq S$ *equals*

$$\pi_S(\widetilde{\rho}^{(s)}(m))^m = f_m(t)\pi_S(\widetilde{\rho}^{(s)}(m))^{S-1} - h_m(t)\pi_S(\widetilde{\rho}^{(s)}(m))^{S-2}$$

where $t \equiv \lambda_1\lambda_2$ *be the product of the non-zero eigenvalues* λ_1, λ_2 *of* $\pi_S(\widetilde{\rho}^{(s)}(m))$, *and* $h_{m+1}(t) = tf_m(t)$, *where* $f_m(t)$ *is related to Chebyshev polynomials of the second kind* $U_m(t)$, *via relation* $b_m(t) = U_{m-1}(\frac{t}{2})$, *with* $f_{m+S}(t) = -\frac{1}{2}\left\{(2t-1)\sqrt{t}^{m-1}b_m(1/\sqrt{t})\right\} + 2^{-m-1}\left((1-\sqrt{1-4t})^m + (1+\sqrt{1-4t})^m\right)$, *with initial conditions* $f_S(t) = 1$ *and* $f_{S+1}(t) = 1 - t$.

The equal entanglement configurations determined by investigating their contours on the r, m plane where various quantum search/counting algorithms are located are displayed in Figure 3. The following statements refer to the

content of that figure: i) The equal Renyi entropy contours are organized in the contour curves wrt the iterations m and the remaining qubits r after database splitting; ii) Tracing any contour provides all pairs (m, r) of fixed entanglement developed after m iterations between the two splitting sets with r and $n-r$ qubits respectively. Starting from e.g. point $(m_{\max}, r)$, of maximal m (box), and tracing counter-clockwise its contour we encounter decreasing and increasing of m and r as it is indicated by up and down arrows $\downarrow, \uparrow$ in the figure. Before returning to the initial point all equal entropy points have been traced out with landmarks the points $(m_d, r_{\max})$ (disk), $(m_{\min}, r_d)$ (diamond) and $(m_d, r_{\min})$ (circle), where m_d, r_d be the middle points. Operationally this indicates the various ways one can generate an equally entangled bipartition of database by fiddling around with *interaction time* m and *splitting dimension* $(R = 2^r, N - R = 2^n - 2^r)$; iii) All m^*, m^{**} periodic zero entanglement instances correspond to straight vertical parallel lines (dark in black-white or blue in color plot), which are independent from the values of r. (c.f. a similar scaling invariance discussed in [12]).

Final comment concerns the behaviour of the entropy vs. #steps graphs of fig.1 and fig. 2. The plots of all entropies are having common intervals of monotonicity, common positions of maxima and minima as well as that their common minima are vanishing points i.e. zeros. Noticeable is fact that the commonality of intervals and points refers only to entropies between them and not between entropies and the success probability graph, c.f. the broken line vs. full lines in fig. 1. This situation is independent from the relative size of the splitting r vs. $n-r$ of database qubits. Therefore we have a *scale invariance* of the position of the zeros for all entropies and all database splitting schemes. Given that splitting generates entanglement and measuring iterations between every second zero determines the N we conclude that the method put forward here for the fast counting is scale invariant and depends only on the total number of database qubits.

Conclusions and Discussion: Quantum search algorithm seen as a judicious construction of a unitary orbit for a pure density matrix harbours more agencies than search complexity reduction only. Bi-portioning the database space and monitoring in the course of search the quantum correlations developed between reduced subsystems, reveals an oscillatory mode of variation for all quantifying measures of entanglement. Periodic vanishing of entanglement with period $\mathcal{O}(\sqrt{N})$ allows harnessing this phenomenon to measure N, which is identified with the unknown size of a finite set. Hence leading to a quadratic reduction of the number of necessary counts. Operationally this is achieved by assuming the existence of an agent that sets up a single item quantum search for a known to her N dimensional database. Things can improve if initial information or good guessing is available about the marked database item.

Is this entanglement period finding phenomenon robust under tri-partition or even successive partitions of database total state vector; how this fast counting protocol could be re-configured in the case of collective quantum search [7], where multiple searchers are combining their algorithms by merging and/or concatenating their oracle algebra representations to achieve novel search complexity reductions? These are some new open questions worth to be addressed.

---

[1] L. K. Grover, Phys. Rev. Let. **79**, 325-328 (1997).
[2] L. K. Grover, in *Proceedings 28th Ann. ACM Symp. on the Theory of Computing*, edited by ACM Press, New York, (1996), pp. 212-218.
[3] L.K. Grover, Phys. Rev. Let. **80**, 4329-4332 (1998).
[4] M. Boyer, G. Brassard, P. Hoyer and A. Tapp, in *Proceedings of 4th Workshop on Physics and Computation* (1996), pp. 36-43
[5] D. Ellinas and Ch. Konstandakis, in *Proceedings of QCMC 2010*, eds. T. Ralph and P. K. Lam, (2011) pp. 4-9.
[6] D. Ellinas and Ch. Konstandakis, J. Phys. A, Theoretical and Mathematical, **46**, 415303 (2013)
[7] D. Ellinas and Ch. Konstandakis, Entropy 2015, **17**, 4838-4862
[8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, (2000).
[9] K. Zyczkowski and I. Bengtsson, *Geometry of Quantum States: An Introduction to Quantum Entanglement*, Cambridge Univ. Press, (2006).
[10] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998)
[11] S.J. Lomonaco and L.H. Kauffman, Quantum Inf. Process, **6**, 461-476, (2007)
[12] M. Rossi, D. Bruss and C. Macchiavello, Phys. Rev. A **87**, 022331 (2013)

Supplemental Material:
Demosthenes Ellinas and Christos Konstandakis
Fast Counting Fuelled by Entanglement: Quantum Search new Harness
Appendix A : Oracle algebra

In the following the definition of the oracle algebra and its representations are presented. *Definition*: Let a Boolean function $f : \mathbb{Z}_N \to \mathbb{Z}_2$, and the orthogonal vectors $|x\rangle = \frac{1}{\sqrt{\nu}} \sum_{i=1}^{N} f(i)\,|i\rangle$ and $\left|x^{\perp}\right\rangle = \frac{1}{\sqrt{\nu^{\perp}}} \sum_{i=1}^{N} (1-f(i))\,|i\rangle$, with $\nu = \sum_{i=1}^{N} f(i)$, and $\nu^{\perp} = \sum_{i=1}^{N}(1-f(i))$, which generate the space $H_2 \equiv \mathcal{V}_x = \mathrm{span}\{|x\rangle, \left|x^{\perp}\right\rangle\} \approx \mathbb{C}^2$, and the unit element $\Sigma_0 = |x\rangle\langle x| + \left|x^{\perp}\right\rangle\left\langle x^{\perp}\right|$. The oracle algebra is defined as the vector space $A_f = \{M \in \mathbb{C}^{N\times N}; M\Sigma_0 M^{\dagger} = \Sigma_0\}$, generated by the elements

$$\begin{aligned}\Sigma_1 &= |x\rangle\left\langle x^{\perp}\right| + \left|x^{\perp}\right\rangle\langle x| \\ \Sigma_2 &= -i\,|x\rangle\left\langle x^{\perp}\right| + i\left|x^{\perp}\right\rangle\langle x| \\ \Sigma_3 &= |x\rangle\langle x| - \left|x^{\perp}\right\rangle\left\langle x^{\perp}\right|,\end{aligned}$$

with $u(2)$ algebra commutation relations $[\Sigma_\alpha, \Sigma_b] = 2i\Sigma_c$ (cyclically), and [Σ_0,everything] = 0, i.e. $A_f \approx u(2)$, oracle algebra is isomorphic to $u(2)$ matrix algebra. There are two basic matrix representations of A_f provided by the algebra homomorphisms π_2 and π_N as follows: the two dimensional $\pi_2 : A_f \to Lin(H_2)$, and the N dimensional $\pi_N : A_f \to Lin(H_N)$, where $H_N = span\{|i\rangle\}_{i=1}^{N}$. Explicitly any element $A \in A_f$ is represented in A_f, by a 2-dim matrix $\pi_2(A) = \pi_2(\Sigma_0)A\pi_2(\Sigma_0^{\dagger})$, or by a N-dim matrix $\pi_N(A) = \pi_N(\Sigma_0)A\pi_N(\Sigma_0^{\dagger})$ respectively.

Examples: Let $A = (A_{ij}) \in A_f$, and if $P_x = |x\rangle\langle x|, P_{x^\perp} = \left|x^{\perp}\right\rangle\left\langle x^{\perp}\right|$, i.e. $\Sigma_0 = P_x + P_{x^\perp}$, then the projection of A in $\mathcal{V}_x$ space via $\pi_2(A) = \pi_2(\Sigma_0)A\pi_2(\Sigma_0^{\dagger}) = (P_x + P_{x^\perp})\,A\,(P_x + P_{x^\perp})$, leads to the matrix $\pi_2(A) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, where the matrix elements are

$$\langle x|\,A\,|x\rangle = \sum_{i,j=1}^{N} \chi_i\chi_j A_{ij} = \sum_{i=1}^{k}\sum_{j=1}^{k} A_{ij} = \alpha,$$

$$\langle x|\,A\left|x^{\perp}\right\rangle = \sum_{i,j=1}^{N} \chi_i(1-\chi_j)A_{ij} = \sum_{i=1}^{k}\sum_{j=k+1}^{N} A_{ij} = \beta$$

$$\left\langle x^{\perp}\right|A\,|x\rangle = \sum_{i,j=1}^{N} (1-\chi_i)\chi_j A_{ij} = \sum_{i=k+1}^{N}\sum_{j=1}^{k} A_{ij} = \gamma$$

$$\begin{aligned}\left\langle x^{\perp}\right|A\left|x^{\perp}\right\rangle &= \sum_{i,j=1}^{N} (1-\chi_i)(1-\chi_j)A_{ij} \\ &= \sum_{i=k+1}^{N}\sum_{j=k+1}^{N} A_{ij} = \delta\end{aligned}$$

As to the N-dim representation we can compute that $\pi_N(A) \equiv \pi_N(\alpha\Sigma_0 + \beta\Sigma_1 + \gamma\Sigma_2 + \delta\Sigma_3)$, where $\alpha = Tr(\pi_N(A)\pi_N(\Sigma_0))$, $\delta = Tr(\pi_N(A)\pi_N(\Sigma_3))$, $\gamma = Tr(\pi_N(A)\pi_N(\Sigma_1))$ and $\delta = Tr(\pi_N(A)\pi_N(\Sigma_2))$, which provides the matrix

$$\pi_N(A) = \begin{pmatrix} (\alpha+\delta)\frac{1}{k}\widehat{\mathbf{1}}_{k\times k} & (\beta - i\gamma)\frac{1}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{k\times(N-k)} \\ (\beta+i\gamma)\frac{1}{\sqrt{k(N-k)}}\widehat{\mathbf{1}}_{(N-k)\times k} & (\alpha-\delta)\frac{1}{N-k}\widehat{\mathbf{1}}_{(N-k)\times(N-k)} \end{pmatrix},$$

where $(\widehat{\mathbf{1}}_{st})_{ij} = 1$, $1 \le i \le s, 1 \le j \le t$.

Additionally regarding the representations of the generic element

$$A = \alpha\,|x\rangle\langle x| + \beta\,|x\rangle\left\langle x^{\perp}\right| + \gamma\left|x^{\perp}\right\rangle\langle x| + \delta\left|x^{\perp}\right\rangle\left\langle x^{\perp}\right|,$$

treated above we can show that

$$\pi_2(A^n) = (\pi_2(A))^n = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^n,$$

as manifestation of the homomorphic property of π_2. Indeed by means of the operators $P_{ab} = |a\rangle\langle b|$, where $a, b = \{x, x^\perp\}$, that satisfy the relations $P_{ab}P_{a'b'} = P_{ab'}\delta_{ba'}$, and their corresponding N-dim matrix representations $\frac{1}{\sqrt{ij}}\widetilde{\mathbf{1}}_{i,j}$, where $i, j \in \{k, N-k\}$,which satisfy the respective relations $\frac{1}{\sqrt{ij}}\widetilde{\mathbf{1}}_{i,j}\frac{1}{\sqrt{i'j'}}\widetilde{\mathbf{1}}_{i',j'} = \frac{1}{\sqrt{ij'}}\widetilde{\mathbf{1}}_{i,j'}\delta_{ji'}$, we can verify that by direct calculation that the matrix form of A in space $\mathcal{V}_x$ satisfies the mentioned property.

Numerical examples: For $N = 4$, $k = 1$, with $f(1) = 1$ and zero elsewhere, we obtain

$$\pi_4(\Sigma_-) = \frac{1}{\sqrt{3}}\begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \pi_4(\Sigma_+) = \frac{1}{\sqrt{3}}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

$$\pi_4(\Sigma_1) = \frac{1}{\sqrt{3}}\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \pi_4(\Sigma_2) = \frac{i}{\sqrt{3}}\begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

$$\pi_4(\Sigma_3) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -\frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} \\ 0 & -\frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} \\ 0 & -\frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} \end{pmatrix}, \quad \pi_4(\Sigma_0) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}.$$

Appendix B : Proofs of Lemmas 1,2

Proof (Lemma 1): Consider the trace inner product $\langle A, B\rangle_{\mathbb{C}^{R\times R}} = \frac{1}{R}TrAB^\dagger$, for $A, B \in \mathcal{M}(\mathbb{C}^R)$. For oracle algebra generators $A_f = span\{\Sigma_i\}_{i=0}^3$, we obtain $\langle \Sigma_i, \Sigma_j\rangle_{\mathbb{C}^{R\times R}} = \delta_{ij}$, so the density matrix $\rho^{(m;r)} = \frac{1}{2}(\Sigma_0 + s_1^{(m;r)}\Sigma_1 + s_3^{(m;r)}\Sigma_3)$, is expressed as $\rho^{(m;r)} = \frac{1}{2}(\Sigma_0 + \langle\Sigma_1\rangle\Sigma_1 + \langle\Sigma_3\rangle\Sigma_3)$, where $s_i^{(m;r)} = \left\langle \Sigma_i, \rho^{(m;r)}\right\rangle_{\mathbb{C}^{R\times R}}$, is abbreviated to $s_i^{(m;r)} \equiv \langle\Sigma_i\rangle$. For powers of Bloch vector components e.g. $(s_i^{(m;r)})^2 \equiv \langle\Sigma_i\rangle^2$, via property $Tr(AB)\times Tr(CD) = Tr(A\otimes B)(C\otimes D)$, we write $(\rho \equiv \rho^{(m;r)})$,

$$\left(Tr\left(\rho\Sigma_i\right)\right)^2 = Tr((\rho\Sigma_i)\otimes(\rho\Sigma_i)) = Tr((\rho\otimes\rho)(\Sigma_i\otimes\Sigma_i)),$$

which after the identification $Tr((\rho\otimes\rho)(\Sigma_i\otimes\Sigma_i)) \equiv \langle\Sigma_i\otimes\Sigma_i\rangle$, with $\langle\Sigma_i\otimes\Sigma_i\rangle$ the expectation value of observable $\Sigma_i\otimes\Sigma_i$ in state $\rho^{\otimes 2}$, one obtains $\langle\Sigma_i\rangle^2 = \langle\Sigma_i\otimes\Sigma_i\rangle$. Applying this same idea to e.g. the linear entropy function for state $\rho^{(m;r)}$ defined as

$$S_L(\rho^{(m;r)}) = 1 - Tr\rho^{(m;r)2} = 1 - [(s_1^{(m;r)})^2 + (s_3^{(m;r)})^2],$$

it is obvious that we need to devise an operational way to obtain the value of entropy in the course of search/counting i.e. the S_L vs. m. To this end we express the linear entropy in terms of the expectation value of observable $\Sigma_3\otimes\Sigma_3 + \Sigma_1\otimes\Sigma_1$, of a doubled version of the initial quantum system being in state $\rho\otimes\rho$, as follows $S_L(\rho^{(m;r)}) = 1 - \langle\Sigma_3\otimes\Sigma_3 + \Sigma_1\otimes\Sigma_1\rangle$. Utilizing the identity, $\Sigma_1 = e^{\frac{i\pi}{2}\Sigma_2}\Sigma_3 e^{-\frac{i\pi}{2}\Sigma_2}$, we write

$$\begin{aligned}\Sigma_1\otimes\Sigma_1 + \Sigma_3\otimes\Sigma_3 &= \Sigma_3\otimes\Sigma_3 + e^{\frac{i\pi}{2}(\Sigma_2\otimes\mathbf{1}+\mathbf{1}\otimes\mathbf{\Sigma}_2)}\Sigma_3 \\ &\otimes\Sigma_3 e^{-\frac{i\pi}{2}(\Sigma_2\otimes\mathbf{1}+\mathbf{1}\otimes\mathbf{\Sigma}_2)} \\ &\equiv \mathcal{E}^*(\Sigma_3\otimes\Sigma_3),\end{aligned}$$

where unitary CP map $\Sigma_3\otimes\Sigma_3 \to \mathcal{E}^*(\Sigma_3\otimes\Sigma_3)$, has been introduced, with generators $\mathcal{E}^* \equiv \{\mathbf{1}, e^{\frac{i\pi}{2}(\Sigma_2\otimes\mathbf{1}+\mathbf{1}\otimes\mathbf{\Sigma}_2)}\}$. The mean value in question is cast in the form

$$\langle\Sigma_1\otimes\Sigma_1 + \Sigma_3\otimes\Sigma_3\rangle = \langle\mathcal{E}^*(\Sigma_3\otimes\Sigma_3)\rangle = \langle\mathcal{E}(\rho\otimes\rho)(\Sigma_3\otimes\Sigma_3)\rangle,$$

where the dual CP map

$$\rho^{\otimes 2} \to \mathcal{E}(\rho^{\otimes 2}) = \tfrac{1}{2}\rho^{\otimes 2} + \tfrac{1}{2}e^{-\frac{i\pi}{2}(\Sigma_2\otimes\mathbf{1}+\mathbf{1}\otimes\mathbf{\Sigma}_2)}\rho^{\otimes 2}e^{\frac{i\pi}{2}(\Sigma_2\otimes\mathbf{1}+\mathbf{1}\otimes\mathbf{\Sigma}_2)}$$

has been introduced.

Next we provide a unitary dilation to the map $\mathcal{E}$ which eventually determines a Hamiltonian for the measurement of entropy. Let an auxiliary quantum system with two states $\mathcal{H}_{aux} = span\{|0\rangle, |1\rangle\}$, described by density matrix $\rho_{aux} = |0\rangle\langle 0|$, and the unitary operator V on $\mathcal{H}_{aux} \otimes \mathcal{H}_{sys} \otimes \mathcal{H}_{sys}$

$$V = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{1}_R \otimes \mathbf{1}_R & -e^{\frac{i\pi}{2}(\Sigma_2 \otimes \mathbf{1} + \mathbf{1} \otimes \mathbf{\Sigma}_2)} \\ e^{-\frac{i\pi}{2}(\Sigma_2 \otimes \mathbf{1} + \mathbf{1} \otimes \mathbf{\Sigma}_2)} & \mathbf{1}_R \otimes \mathbf{1}_R \end{pmatrix}$$
$$= \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{1}_R \otimes \mathbf{1}_R & \Sigma_2 \otimes \Sigma_2 \\ -\Sigma_2 \otimes \Sigma_2 & \mathbf{1}_R \otimes \mathbf{1}_R \end{pmatrix}.$$

If the total system is described initially by $\rho_{aux} \otimes \rho^{\otimes 2}$ and evolves as $\rho_{aux} \otimes \rho^{\otimes 2} \to V(\rho_{aux} \otimes \rho^{\otimes 2})V^\dagger$, and if the interaction is terminated by decoupling auxiliary system from the main system via Tr_{aux}, the partial trace over the auxiliary system), then this leads to map $\mathcal{E}$ i.e. $\mathcal{E}(\rho^{\otimes 2}) = Tr_{aux}V(\rho_{aux} \otimes \rho^{\otimes 2})V^\dagger$.

Due to relation $e^{\pm\frac{i\pi}{2}(\Sigma_2 \otimes \mathbf{1} + \mathbf{1} \otimes \mathbf{\Sigma}_2)} = e^{\pm\frac{i\pi}{2}\Sigma_2} \otimes e^{\pm\frac{i\pi}{2}\Sigma_2} = \pm i\Sigma_2 \otimes \pm i\Sigma_2 = -\Sigma_2 \otimes \Sigma_2$, the map becomes $\mathcal{E}(\rho^{\otimes 2}) = \frac{1}{2}\rho^{\otimes 2} + \frac{1}{2}(\Sigma_2 \otimes \Sigma_2)\rho^{\otimes 2}(\Sigma_2 \otimes \Sigma_2)^\dagger$. In this form $\mathcal{E}$ is identified with a collective Y unitary channel of two system $\mathcal{H}_{sys} \otimes \mathcal{H}_{sys}$ with generators $\mathcal{E} \equiv \{\frac{1}{\sqrt{2}}\mathbf{1}, \frac{1}{\sqrt{2}}\Sigma_2 \otimes \Sigma_2\}$, and a unitary dilation V as in the rhs of the last equation above.

Proof (Lemma 2): The following items are valid (abbreviations: x, y, w stand for $x^{(s)}, y^{(s)}, w^{(s)}$ respectively, and ρ for $\pi_S(\widetilde{\rho}^{(s)}(m))$) :

i) The characteristic equation and the eigenvalues of rank 2 matrix ρ are respectively $\lambda^{S-2}\left(\lambda^2 - \lambda - (S-1)y^2\right) = 0$ and $\lambda_0 = 0$ of multiplicity $S-2$, and $\lambda_{1,2} = \frac{1}{2}(1 \pm \sqrt{1 - 4(wx - y^2)(S-1)})$ with multiplicity 1.

ii) Due to Cayley-Hamilton theorem it holds that $\rho^{S-2}(\rho^2 - \rho - (S-1)y^2\mathbf{1}_S) = \mathbf{0}_S$, namely $\rho^{S-2}(\rho^2 - \rho + t\mathbf{1}_S) = \mathbf{0}_S$, where equality $t = -(S-1)y^2 = \lambda_1\lambda_2$ arises from Vieta's formula $\sum_{i \neq j} x_i x_j = \frac{a_{n-2}}{a_n}$, valid for any n degree polynomial $P(x) = a_n x^n + \cdots + a_1 x + a_0$ with roots x_i, $i = 1, 2, ...n$.

iii) We have that $\rho^S = \rho^{S-1} - t\rho^{S-2}$ and for all $\mathbb{N} \ni m \geq S$ we assume (c.f. [1]),

$$\rho^m = f_m(t)\rho^{S-1} - h_m(t)\rho^{S-2},$$

from which we obtain $h_S(t) = t$, $f_S(t) = 1$ and $f_{S+1}(t) = 1 - t$. Further $\rho^{m+1} = f_m(t)\rho^S - h_m(t)\rho^{S-1} = f_m(t)(\rho^{S-1} - t\rho^{S-2}) - h_m(t)\rho^{S-1}$, so $f_{m+1}(t) = f_m(t) - h_m(t)$, and $h_{m+1}(t) = tf_m(t)$, and thus

$$f_{m+1}(t) = f_m(t) - tf_{m-1}(t).$$

This recurrence relation reminds the Chebyshev polynomials relation viz. $b_{m+1}(t) = tb_m(t) - b_{m-1}(t)$, where the variable term t however appears in the "wrong" side. Motivated by this feature we proceed as follows: we solve our recurrence relation and compare the solution the the Chebyshev polynomial solution. Anticipating the final result we say that the association between our polynomial system and Chebyshev polynomials is in terms of a in-homogeneous relation with variable coefficients and different argument between the two types of polynomials c.f. the stated relation in lemma 2.

To proceed with the solution of our recurrence relation we consider the shifted sequence $f_{m+S}(t)$, $m = 0, 1, 2, ...$, which is identified with the intermediate sequence $a_m(t)$ as $f_{m+S}(t) = a_m(t)$. Solving the recurrence relation obeyed by a_m viz. $a_m(t) = a_{m-1}(t) - ta_{m-2}(t)$, $a_0(t) = 1, a_1(t) = 1 - t$, and compare them with the solution of Chebyshev polynomials of the second kind $U_m(t)$, via another the intermediate sequence $b_m(t) = U_{m-1}(\frac{t}{2})$, we obtain the solution

$$f_{m+S}(t) = -\frac{1}{2}[(2t-1)\sqrt{t}^{m-1}b_m(1/\sqrt{t})] +$$
$$2^{-m-1}\left((1 - \sqrt{1-4t})^m + (1 + \sqrt{1-4t})^m\right)$$

satisfying the initial conditions $f_S(t) = 1$ and $f_{S+1}(t) = 1 - t$.

Appendix C : Proof of Proposition

i) C.f. Remarks: 3;

ii) To show the projectivity of the reduced matrix recall the definition $\pi_R(\rho^{(r)}(\widetilde{m}))^2 = \pi_R(\rho^{(r)}(\widetilde{m}))$. Verifying this relation we obtain that

$$x^2 + (R-1)y^2 = x \tag{2}$$
$$xy + (R-1)yw = y \tag{3}$$
$$y^2 + (R-1)w^2 = w \tag{4}$$

Recall that the definition of x, y, w and the additional relation from the main text (indices have been drop)

$$x = a^2 + (L-1)b^2 \tag{5}$$
$$y = ab + (L-1)b^2 \tag{6}$$
$$w = Lb^2 \tag{7}$$
$$a^2 + (N-1)b^2 = 1 \tag{8}$$

We discern the following cases:
I) If $y = 0$, then

$$x^2 = x \tag{9}$$
$$(R-1)w^2 = w \tag{10}$$
$$ab + (L-1)b^2 = 0 \tag{11}$$

Ia) If $b = 0$ then $a^2 + (N-1)b^2 = 1$ becomes $a^2 = 1$, equivalently $m = \widetilde{m} = \frac{\widetilde{a}}{\widetilde{\theta}}$. Due to the periodicity of $\pi_R(\rho^{(r)}(m))$, we obtain the arithmetic progression $m = \widetilde{m}_* = \{\widetilde{m} + k\widetilde{T}\}_{k=0}^{\infty}$.
Ib) If $b \neq 0$ then, from eq(10) we verify that no new solution exist for m.
II) If $y \neq 0$ then following a similar procedure we find a second arithmetic progression for m viz. $m = \widetilde{m}_{**} = \{\widetilde{m} - \frac{1}{\widetilde{\theta}} \arctan(\sqrt{N-1}) + k\widetilde{T}\}_{k=0}^{\infty}$. The asymptotic forms $\widetilde{m}_*^{\infty}, \widetilde{m}_{**}^{\infty}$ follow directly from the above formulas.

Appendix D: Root finding of entropy functions

Next we prove the following statements:
i) the measures of entropy of entanglement (von Neumann), quantum Renyi entropy and linear entropy mentioned in the main text, vanish simultaneously during search at step m iff $m = \widetilde{m}_*$ or $\widetilde{m}_{**}$. The is direct verification and we only need to recall the eigenvalues reported above in the proof of lemma 2 and the expression of the entropies in terms of the non zero eigenvalues viz. $E_{\mathrm{Ren}} = \frac{1}{1-a} \log_2 \left(\lambda_1^a + \lambda_2^a\right)$, $E_{\mathrm{Neum}} = -\lambda_1 \ln \lambda_1 - \lambda_2 \ln \lambda_2$ and $E_{\mathrm{Lin}} = 1 - \lambda_1^2 - \lambda_2^2$;
ii) the distance between every second zero of the entropies is related to probability p via formula $p = \frac{1}{2}(1 \pm \cos(\pi/\widetilde{T}))$. Indeed, this distance equals the period $\widetilde{T} = \pi/\widetilde{\theta}$, so $4(p - p^2) = \sin^2(\pi/\widetilde{T})$ and the result follows.

---

[1] H. Bacry, Journal of Mathematical Physics **28**, 2259 (1987)