

Orthogonal vector computations

Karl Svozil

*Institute for Theoretical Physics, Vienna University of Technology,
Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria**

Quantum computation is the suitable orthogonal encoding of possibly holistic functional properties into state vectors, followed by a projective measurement.

PACS numbers: 03.65.Ca, 02.50.-r, 02.10.-v, 03.65.Aa, 03.65.Aa, 03.67.Ac

Keywords: quantum theory, probability theory, quantum logic, quantum algorithms, parity

I. IDENTIFYING QUANTUM PHYSICAL MEANS FOR COMPUTATION

The hypothesis pursued in this paper is that the power of quantum computation solely resides in a proper “translation” of “holistic” properties of functions—manifesting themselves in the *relational* values for different elements of their domain, or of their entire image—into orthogonal subspaces and their associated perpendicular projections. This is usually facilitated by *quantum parallelism*—the possibility to co-represent and co-encode classically distinct and mutually exclusive clauses into simultaneous coherent superpositions thereof. However, in order to take advantage of parallelism, it is necessary to be able to analyse the resulting quantum state by suitably chosen orthogonal projections. In what follows we shall therefore attempt to enumerate conditions under which a given algorithmic task can be quantum mechanically encoded into orthogonal subspaces, thereby identifying criteria for potential quantum speedups.

This paper is organized as follows: after a brief and somewhat iconoclastic exposition of the standard quantum formalism (which may be amusing to some but considered to be superfluous by others) strategies to encode properties of computable functions into orthogonal subspaces are discussed. This involves the possibility to orthogonalise non-orthogonal vectors of some initial Hilbert space by interpreting them as orthogonal projections of mutually orthogonal vectors in a Hilbert space of greater dimension.

II. LOCATING QUANTUM RESOURCES

Starting with Plack’s [1] (p. 31) “act of despair” it may not be totally unreasonable to state that the newly discovered quantum capacities, unheard of in classical continuum mechanics, caused shock and awe among some of the most prominent creators of quantum mechanics. Most notably Schrödinger struggled with quantum coherence, today known as quantum parallelism, throughout his entire life, bringing forward

seemingly absurd consequences of the formalism, such as the cat paradox, or quantum jellification [2]. In the same series of papers [3] he also mentioned the capacity that multiple quanta may be entangled; a resource related to quantum non-locality, which was put forward by Einstein on various occasions [4, 5] to question the consistency of quantum and relativity theory.

On the formal side, Hilbert space quantum mechanics [6] and, in particular, quantum logic have been conceived [7] as attempts to systematically identify and study the valid, feasible, operational resources and capacities of quantized physical systems in terms of algebraic structures arising in quantum mechanics. Thereby, logical entities are identified with quantum theoretical terms; a typical example being the identification with a binary logical yes-no proposition or property with an orthogonal projection operator; or, equivalently, with the associated linear subspace, which, in the one-dimensional case, is spanned by a single (unit) vector. In what follows some of these identifications will explicitly be enumerated.

Subsequently, and possibly motivated by single-quantum experiments which have become experimentally feasible, quantum information and communication research attempts to exploit mostly non-classical capacities of quantized systems, such as parallelism, entanglement, or other quantum resources [8–11]. (A *caveat*: we refrain here from a detailed, more comprehensive list of references, as this might transcend this brief review.)

A. State as Context

In the Dirac-von Neumann formalism of quantum mechanics a *pure state* is completely characterized by a unit vector $|\psi\rangle$ (or, equivalently, by the associated one-dimensional subspace spanned by $|\psi\rangle$; or by the orthogonal projection operator $\mathbf{E}_\psi = |\psi\rangle\langle\psi|$) in a Hilbert space, which essentially (disregarding completeness) is a vector space equipped with a scalar product. In what follows we shall disregard mixed states completely—according to the *Church of the Larger Hilbert Space* any mixed state is purely epistemic (but not ontic), and originates from some unknown pure state which can be reconstructed, subject to some (usually non-unique) purification by “reverting” (by disclosing “additional information”) the introduction of ignorance (enforced by a non-unitary many-

* svozil@tuwien.ac.at; <http://tph.tuwien.ac.at/~svozil>

to-one state evolution) through partial traces. Every state will thus assumed to be pure.

Alternatively it may be preferable [12] to define a state via a context, or, equivalently, an orthonormal basis, or a maximal observable [13] (§ 84, Theorem 1) whose spectral sum is non-degenerate. Any such context represents a Boolean subalgebra (formed by mutually orthogonal and thus commuting projections) of a quantum logic; a kind of “greatest classical mini-universe” which is co-preparable.

B. Observable as Context

Every maximal *observable* or context corresponds to the non-degenerate spectral sum of one-dimensional mutually orthogonal (and thus commuting) projections whose sum is a resolution of the identity. Within operational capacities, those bases can be chosen freely by the experimenter. They correspond to quasi-classical mini-universes of mutually commuting, compatible observables.

Once a particular maximal observable is chosen, the respective orthonormal basis $\mathfrak{B}_n = \{|\mathbf{e}_1\rangle, |\mathbf{e}_2\rangle, \dots, |\mathbf{e}_n\rangle\}$ facilitates a *particular view* on the state $|\psi\rangle$. If one basis element coincides with the state $|\psi\rangle$, then the measurement of \mathfrak{B}_n is deterministic: a single proposition associated with the orthogonal projection operator identical to $|\psi\rangle\langle\psi|$ is true; and all the other propositions represented by the remaining basis elements are false. In this case we may say that this observable reflects a physical *property* of that state [14] (thereby affirming the dual use of orthogonal projections both for pure states as well as for propositions).

Otherwise, if there is a mismatch between the state preparation and the query, *context translation* introduces stochasticity through the many degrees of freedom of quasi-classical measurement devices [15]. The epistemic interpretation of maximal observables as views on the state $|\psi\rangle$ alleviates Schrödinger’s continued concerns regarding the ontological existence of coherent superpositions, so vividly put forward in the cat paradox or by quantum jellification mentioned in his lesser known Dublin seminars [2].

C. Probability

Gleason’s theorem [16] states that (for dimensions larger than two, allowing intertwining orthogonal bases) the quantum probabilities follow from the requirement that on all contexts the quantum probabilities should be identical with their respective classical probabilities (in particular, σ -additivity of probabilities of mutually exclusive events). That is, within classical mini-universes of a quantum logic, classical probabilities rule.

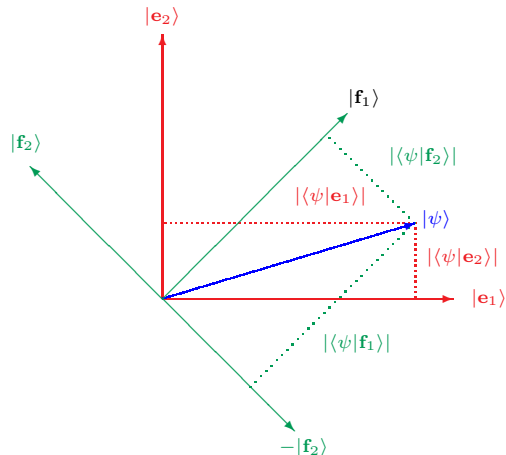


FIG. 1. Different orthonormal bases $\{|\mathbf{e}_1\rangle, |\mathbf{e}_2\rangle\}$ and $\{|\mathbf{f}_1\rangle, |\mathbf{f}_2\rangle\}$ offer different “views” on the pure state $|\psi\rangle$. As $|\psi\rangle$ is a unit vector it follows from the Pythagorean theorem that $|\langle\psi|\mathbf{e}_1\rangle|^2 + |\langle\psi|\mathbf{e}_2\rangle|^2 = |\langle\psi|\mathbf{f}_1\rangle|^2 + |\langle\psi|\mathbf{f}_2\rangle|^2 = 1$, thereby motivating the use of the absolute value (modulus) squared of the amplitude for quantum probabilities on pure states.

Although most of his paper is devoted to proving necessity of the Born rule (including mixed states) from this assumption, already in the second paragraph Gleason observed that, as long as one is concerned merely about pure states it is possible to construct a *probability measure* on the Hilbert space via an elementary geometric construction, suggesting the squared norm of the orthogonal projections of these pure states onto the vectors of some orthonormal basis as quantum probability measure. One could again say that the pure state is “viewed from” the maximal operator corresponding to the aforementioned basis.

In contrast to the full proof of Gleason’s theorem, the argument for the sufficiency of the squared norm probability measures (satisfying classicality within contexts) is elementary; thereby the absolute squares of the probability amplitudes $\langle\psi|\mathbf{e}_i\rangle$ result from the Pythagorean theorem: since $|\psi\rangle$ is a unit vector and the $|\mathbf{e}_i\rangle$ represent vectors of an orthonormal basis, all absolute squares of $\langle\psi|\mathbf{e}_i\rangle$ sum up to one; that is, $\sum_{i=1}^n |\langle\psi|\mathbf{e}_i\rangle|^2 = 1$. A construction of such a Gleason-type measure in two-dimensional real vector space is depicted in Figure 1.

By construction, this probability measure satisfies the requirement of the validity of classical probabilities within all classical mini-universes. This is remarkable because of the absence of (sufficiently many) global two-valued measures [17] whose positive convex combinations form all classical probability measures [18].

D. Entanglement

Pointedly stated, quantum entanglement is a consequence of the inseparability of not-so-individual quanta. In general, quantum states do not allow the decomposition into product states of constituents. For instance, a general three partite state of three bits $|\psi\rangle = \sum_{i,j,k=0}^1 \alpha_{ijk} |ijk\rangle$ is entangled if and only if it cannot be written as a single product state of the three constituents; a non-entangled product state of three particles requires [19] (p. 18) that all of the following equations are satisfied: $\alpha_{000}\alpha_{011} = \alpha_{001}\alpha_{010}$, $\alpha_{000}\alpha_{101} = \alpha_{001}\alpha_{100}$, $\alpha_{000}\alpha_{110} = \alpha_{010}\alpha_{100}$, $\alpha_{000}\alpha_{111} = \alpha_{011}\alpha_{100}$, $\alpha_{001}\alpha_{110} = \alpha_{011}\alpha_{100}$, $\alpha_{001}\alpha_{111} = \alpha_{011}\alpha_{101}$, $\alpha_{010}\alpha_{101} = \alpha_{011}\alpha_{100}$, $\alpha_{010}\alpha_{111} = \alpha_{011}\alpha_{110}$, $\alpha_{100}\alpha_{111} = \alpha_{101}\alpha_{110}$.

As a consequence, unlike classical properties, entangled states encode (not purely individual but) *relational* properties of multiple quanta [20, 21]. It is thus futile to request, as Einstein maintained in a letter communicated to Schrödinger [4, 5, 22], that the sub-state of an entangled state is not affected by any change of another sub-state if the two involved entangled sub-systems are spatially separated.

E. Evolution as Permutation

The quantum evolution is postulated to be an isometry (that is, a distance preserving map); or, stated differently, a permutation—a one-to-one mapping—preserving the scalar product. This can be formalized by unitary transformations [23]: suppose $\mathfrak{B}_n = \{|\mathbf{e}_1\rangle, |\mathbf{e}_2\rangle, \dots, |\mathbf{e}_n\rangle\}$ and $\mathfrak{B}'_n = \{|\mathbf{f}_1\rangle, |\mathbf{f}_2\rangle, \dots, |\mathbf{f}_n\rangle\}$ are orthonormal bases, then $\mathbf{U}_{fe} = \sum_{i=1}^n |\mathbf{f}_i\rangle\langle\mathbf{e}_i|$ yields a unitary transformation; conversely, any unitary transformation can be represented by such a change of orthonormal bases. So, stated pointedly, the quantum evolution amounts to a (generalized) rotation either of the state vector (the active, Schrödinger representation), or of the coordinate frame (passive, Heisenberg picture) relative to which the state is viewed.

Much of the conceptual progress in the foundations of quantum mechanics owes to the exploitation of this one-to-one permutation scheme in various scenarios: to name just three examples, take quantum teleportation [24], induced coherence [25], and the quantum erasure [26–28]. Indeed, as has already been pointed out by Everett [29] (p. 454) (see also Wigner [30]) there is no such thing as an “irreversible measurement” if quantum theory is assumed universally and uniformly valid: what we fapp [31] call “measurement” is means relative [32], epistemic, and could, at least in principle, be undone if our operational capacities permit.

F. Computational Resources

Quantum theory offers or identifies a single state vector, or orthonormal systems of vectors, which can be rotated or viewed from various perspectives, and on which projection measurements can be made, as the quantum resource for computations. Related alleged capacities, such as “quantum parallelism” associated with coherent superposition induced by views on this vector which do not coincide with it, or *ex nihilo* randomness induced by the quasi-stochasticity of the resulting measurement results through context translations, or entanglement originating from the pretension that the state of subsystems which are spatially apart must be separable, are implications which need to be carefully revised [33, 34] in order to re-evaluate the quantum capacities for computation.

III. RENDITIONS VIA ORTHOGONAL SUBSPACES

So far the stage has been set for concrete proposals to utilize quantized systems for “optimized” computation: in particular, by “looking at a pure state from a proper perspective;” that is, from an orthonormal basis of which it is not an element. In such a basis, the pure state has a composition in terms of more than one basis vectors—in quantum mechanical terms, the state is in a *coherent superposition* of these basis vectors. If the basis is associated with classical bit states, such as $\mathfrak{B}_2 = \{|0\rangle, |1\rangle\}$, one could claim that a quantum state such as $\alpha_0|0\rangle + \alpha_1|1\rangle$ with non-vanishing α_0, α_1 is “in both states $|0\rangle$ and $|1\rangle$ simultaneously.” This may nurture hopes that the simultaneous co-processing of an arbitrary amount of data or clauses might become quantum feasible by introducing a “sufficient” amount of bits in superposition.

One fundamental issue which has to be accounted for is the fact that any recursive function is completely characterized by its input-output behaviour. In order to perform an evaluation (of the recursive function), this behaviour must be coded into a physical operation *simulacron* [35].

However, there is a fundamental limit to quantum computation which resides in one of the basic relations between vectors in Hilbert space: their (non-)orthogonality. This translates into the criterion that a query is quantum mechanically feasible if and only if it can be encoded into orthogonal subspaces. As the unitary evolution preserves angles, and thus orthogonality, within the same Hilbert space there is nothing one can do about “orthogonally separating” two non-orthogonal subspaces, because a Gram-Schmidt orthogonalisation is quantum infeasible when it is most needed; that is, if the initial vectors are not orthogonal (just as the cloning of an arbitrary quantum state is impossible for the same reason—unitarity of the quantum state evolution).

A. Example

Recall the supposition (or rather speculation) mentioned earlier: that the result of any kind of (binary) decision problem can be obtained by taking “enough” qubits to “cover all cases” through the coherent superposition of all classical cases by a single quantum query. Indeed, for the sake of temporal speedups, we could be so bold as to attempt to quantum encode an algorithm as the “parallel” (weighted by relative phases and amplitudes) sum (not the product); that is, the coherent superposition, of all conceivable classical clauses. (Never mind computation space; that is, the amount of qubits, as long as this resource is bounded. Memory space is also required in order to render the computation one-one; that is, a permutation, if the evaluated functions are not invertible.)

For the sake of an example of this strategy, consider Deutsch’s problem for computing the parity of a binary function of a single bit. there, two bits—the input bit and an auxiliary bit (to take care of injectivity in case the function is constant)—which are initially classical, are spread out by Hadamard gates into a proper (the relative phases are relevant) coherent superposition of all classical states.

At the heart of this algorithm is a way to subdivide the four-dimensional state space of the two bits into two orthogonal subspaces associated with parity ± 1 , respectively, thereby rendering parity in a single query. (See [36] for a different finding.) The quantum *versus* classical trade-off is the ignorance of the precise function (out of four) after this single quantum query.

How can this exactly be achieved? Suppose we identify with the classical bit states 0 and 1 the quantum states, represented by the two vectors of a Cartesian basis \mathfrak{B}_2 , $0 \equiv |0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $1 \equiv |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, respectively.

Suppose further that the four binary functions of a single classical bit are the two constant functions $f_0(x) = 0$ and $f_3(x) = 1$, as well as the identity $f_1(x) = x$ and the negation $f_2(x) = 1 \oplus x$, where $x \in \{0, 1\}$ and \oplus represents the addition modulo 2. By forming a unitary quantum oracle $\mathbf{U}_{f_i}|\mathbf{x}\mathbf{y}\rangle = |\mathbf{x}[y \oplus f_i(\mathbf{x})]\rangle$, $i \in \{0, 1, 2, 3\}$, and by taking $|\mathbf{x}\rangle = |\mathbf{y}\rangle = (1/\sqrt{2})|0-1\rangle$ one obtains (by omitting normalization factors; the superscript T indicates transposition, and “ \pm ” stands for “ ± 1 ,” respectively)

$$\begin{aligned} \mathbf{U}_{f_0}|(0-1)(0-1)\rangle &= |++--\rangle^T \\ \mathbf{U}_{f_1}|(0-1)(0-1)\rangle &= |+-+-\rangle^T \\ \mathbf{U}_{f_2}|(0-1)(0-1)\rangle &= |-+--\rangle^T \\ \mathbf{U}_{f_3}|(0-1)(0-1)\rangle &= |--+-\rangle^T \end{aligned} \quad (1)$$

If one is being presented with an unknown function f_i and is given the task to identify [37, 38] it, the following two-(binary)-valued query is associated with

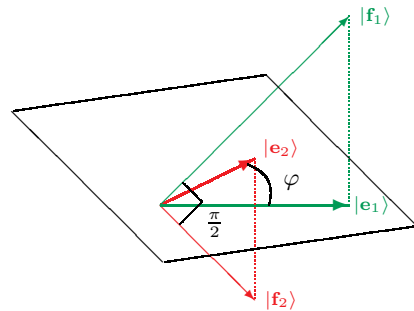


FIG. 2. Demonstration of the orthogonalisation by dimensional lifting for two planar vectors $|e_1\rangle$ and $|e_2\rangle$ which are “lifted” into two orthogonal vectors $|f_1\rangle$ and $|f_2\rangle$ in three dimensions which orthogonally project onto $|e_1\rangle$ and $|e_2\rangle$.

functional parity: in terms of subspaces in four-dimensional Hilbert space with the basis $\mathfrak{B}_2 \equiv \{|e_1\rangle, |e_2\rangle\} \equiv \left\{ (1/2)(1, -1, -1, 1)^T, (1/2)(1, -1, 1, -1)^T \right\}$, and written as spectral sum $\mathbf{P} = |e_1\rangle\langle e_1| - |e_2\rangle\langle e_2|$ corresponding to a partitioning [39–41] of functions $\{\{f_0, f_3\}, \{f_1, f_2\}\}$.

It might not be too critical to call the coincidence between the particular “modulo two” oracle and parity of a binary function of one bit *ad hoc*.

B. Generalized Gram-Schmidt Process

In the previous example the input-output behaviour $\{\{0, 0\}, \{0, 1\}, \{1, 0\}, \{1, 1\}\}$ of a functional class has been translated into the appropriate orthogonal subspaces; the trade-off being the enlargement of Hilbert space by two extra dimensions. The question arises if it is always possible to do so.

As an illustration consider two non-orthogonal and non-collinear planar vectors depicted in Figure 2. Suppose we “extend” those vectors into the three-dimensional space such that the direction and length of the two new non-planar vectors is chosen such that (i) they are orthogonal, and at the same time (ii) their orthogonal projections onto the plain are identical with the original planar vectors.

In the following we shall prove the formal (but not quantum physical) possibility of *orthogonalisation by dimensional lifting*: An arbitrary number k of nonzero vectors $\{|e_1\rangle, \dots, |e_k\rangle\}$ of n -dimensional Hilbert space can be (non-uniquely) interpreted as the orthogonal projections (onto the original Hilbert space) of a set of mutually orthogonal (*i.e.*, $\langle f_i | f_j \rangle = 0$ for $i \neq j$) vectors $\{|f_1\rangle, \dots, |f_k\rangle\}$ in an Hilbert space of dimension $m \geq n$.

For the sake of an explicit example, suppose that, for two vectors (*i.e.*, $k = 2$) and arbitrary finite dimension n , we start with $|e_1\rangle \equiv (x_{11}, \dots, x_{1n})^T$, and

$|\mathbf{e}_2\rangle \equiv (x_{21}, \dots, x_{2n})^T$. It is not too difficult to construct two vectors

$$\begin{aligned} |\mathbf{f}_1\rangle &\equiv (x_{11}, \dots, x_{1n}, 1)^T \\ |\mathbf{f}_2\rangle &\equiv (x_{21}, \dots, x_{2n}, -[x_{11}x_{21} + \dots + x_{1n}x_{2n}])^T \end{aligned} \quad (2)$$

which are orthogonal vectors in $n+1$ dimensions and project onto $|\mathbf{e}_1\rangle$ and $|\mathbf{e}_2\rangle$, respectively. The configuration for $n=2$ is depicted in Figure 2.

The general proof by construction is iterative and follows an “inverse” (in the sense of “adding” some dimension rather than “subtracting” existing vector projections) generalized Gram-Schmidt process: suppose all the k vectors of n -dimensional space are non-collinear and non-orthogonal. Then, by a series of combinations, whose number is determined by the binomial coefficient $\binom{k}{2}$, of two vector orthogonalizations as above, while at the same time, by taking the new vector component of all the other $k-2$ vectors zero, one can construct a set of k mutually orthogonal vectors in $\left[k + \binom{k}{2}\right]$ -dimensional vector space whose orthogonal projections on the original space are the original vectors. Another orthogonalisation by dimensional lifting requiring merely $n+k$ dimensions due to Havlicek [42] will be discussed in a forthcoming paper.

A necessary and sufficient condition for a generalized Gram-Schmidt process to be representable by a quantum evolution is its correspondence to some unitary operation from the initial into the final state. Unfortunately, by design this generalized Gram-Schmidt process is not unitary *per se*. (However, this also is true for the functional encoding of bits before the introduction of a quantum oracle: *a priori* the introduction of auxiliary bits is not guaranteed to be representable by a unitary transformation.) Recall that, as has been mentioned earlier, a necessary and sufficient condition for a unitary transformation is that, by $\mathbf{U}_{fe} = \sum_{i=1}^n |\mathbf{f}_i\rangle\langle\mathbf{e}_i|$ any orthonormal basis $\mathfrak{B}_n \equiv \{|\mathbf{e}_1\rangle, |\mathbf{e}_2\rangle, \dots, |\mathbf{e}_n\rangle\}$ is transformed into another one $\mathfrak{B}'_n \equiv \{|\mathbf{f}_1\rangle, |\mathbf{f}_2\rangle, \dots, |\mathbf{f}_n\rangle\}$ [23]. However, in our case, neither are the original vectors orthogonal, nor needs the target system to be a basis. (This latter deficiency could, in principle, be remedied by adding basis vectors, thereby creating an eutactic star [43, 44].) So, unless the vectors resulting from (i) are not already properly orthogonal (for the particular quantum query), the generalized Gram-Schmidt process (ii) has no quantum mechanical realization.

Moreover, unitary transformations preserve the angles among vectors. Therefore, if the functional behaviour, subjected to a quantum oracle, cannot separate different functional properties by orthogonal subspaces, not much can be gained by a straightforward generalized Gram-Schmidt processes.

Nevertheless, let us, for the sake of another

example of dimensional lifting, come back to Deutsch’s problem, and consider another *ad hoc* quantum oracle, namely $\mathbf{V}_{f_i}|\mathbf{x}\mathbf{y}\rangle = |\mathbf{x}f_i(\mathbf{y})\rangle$, $i \in \{0, 1, 2, 3\}$, resulting in

$$\begin{aligned} \mathbf{V}_{f_0} |(0+1)(0+1)\rangle &= | +00+10\rangle \equiv (+0+0)^T \\ \mathbf{V}_{f_1} |(0+1)(0+1)\rangle &= | +00+11\rangle \equiv (+00+)^T \\ \mathbf{V}_{f_2} |(0+1)(0+1)\rangle &= | +01+10\rangle \equiv (0++0)^T \\ \mathbf{V}_{f_3} |(0+1)(0+1)\rangle &= | +01+11\rangle \equiv (0+0+)^T \end{aligned} \quad (3)$$

By appending four extra dimensions it is not difficult to *ad hoc* orthogonalise this set of vectors (two pairs are already orthogonal); namely

$$\begin{aligned} &(+0+0+000)^T \\ &(+00+-+00)^T \\ &(0++0--++)^T \\ &(0+0+0---)^T \end{aligned} \quad (4)$$

so that, provided a suitable quantum oracle could be found which maps the functional behaviour into the orthogonal subspaces spanned by the vectors in Equation (4), an unknown function f_i could be identified uniquely by a single query (encoding the orthogonal projections corresponding to this latter set of orthogonal vectors).

C. Counterexample and (In-)Sufficiency

Our hypothesis has been that it is not totally unreasonable to speculate that any functional behaviour can somehow be mapped into orthogonal subspaces through the application of a single functional call whose argument is the (equal-weighted) superposition of all possible classical variations of arguments. More specifically, if reversibility is guaranteed by the introduction of auxiliary bits, different functional behaviours on such arguments result in mutually different (non-orthogonal) vectors; which then might be “lifted” into mutually orthogonal subspaces in Hilbert spaces of greater dimensions than the original Hilbert space. Any query, performed on this higher-dimensional Hilbert space, could be realized by “bundling” (formally by adding) the associated projections appropriately.

Indeed, it might be possible (in contrast to findings using different assumptions and oracles [36]) with this method to solve the parity problem by a single quantum query, through separating the parity even and odd functions into two orthogonal subspaces, whose direct sum is the entire Hilbert space.

However, the unitary quantum state evolution imposes strong restrictions on such queries, because it essentially amounts to isometries; that is, to rotations of state vectors: the functional properties must be encoded into these rotations; and the subspaces associated with the

particular functional classes which need to be distinguished from one another must be rotated in such ways that their relative separation amounts to orthogonality.

Therefore there exist collections of functions which, relative to some particular quantum oracles, in particular, $\mathbf{U}_i(|\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{y}\rangle) = |\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{y} \oplus f_i(\mathbf{x}_1, \dots, \mathbf{x}_n)\rangle$, cannot be orthogonally separated.

For an indication consider [45], as a generalization of Deutsch's problem discussed earlier, two particular binary functions of two bits with different parity, namely $f_0(xy) = 0$ for all $x, y \in \{0, 1\}$, and $f_8(00) = f_8(01) = f_8(10) = 0$, as well as $f_8(11) = 1$. A similar calculation

as in Equation (1) yields

$$\begin{aligned} & \mathbf{U}_{f_0}|(0-1)(0-1)(0-1)\rangle \\ &= | +000 - 001 - 010 + 011 - 100 + 101 + 110 - 111 \rangle \\ &\equiv (+ - - + - + + -)^T \\ & \mathbf{U}_{f_8}|(0-1)(0-1)(0-1)\rangle \\ &= | +000 - 001 - 010 + 011 - 100 + 101 - 110 + 111 \rangle \\ &\equiv (+ - - + - + - +)^T \end{aligned} \quad (5)$$

f_0 and f_8 represent functional parity +1 and -1; and yet their respective quantum oracles \mathbf{U}_{f_0} and \mathbf{U}_{f_8} do not map the state $|(0-1)(0-1)(0-1)\rangle$ into orthogonal states (indeed, non-orthogonality may come as no surprise).

Note that, although the relative phases of the coherent superposition of the three input bits have been chosen to be π , other phases could result in orthogonal vectors as desired. For the sake of demonstration, consider the general case (with $|a_i|^2 + |b_i|^2 = 1$)

$$\begin{aligned} & \mathbf{U}_{f_0} (a_1|0\rangle + b_1|1\rangle) (a_2|0\rangle + b_2|1\rangle) (a_3|0\rangle + b_3|1\rangle) \\ &= a_1a_2a_3|000\rangle + a_1a_2b_3|001\rangle + a_1b_2a_3|010\rangle + a_1b_2b_3|011\rangle + \\ & \quad b_1a_2a_3|100\rangle + b_1a_2b_3|101\rangle + b_1b_2a_3|110\rangle + b_1b_2b_3|111\rangle \\ &\equiv (a_1a_2a_3, a_1a_2b_3, a_1b_2a_3, a_1b_2b_3, b_1a_2a_3, b_1a_2b_3, b_1b_2a_3, b_1b_2b_3)^T \\ & \mathbf{U}_{f_8} (a_1|0\rangle + b_1|1\rangle) (a_2|0\rangle + b_2|1\rangle) (a_3|0\rangle + b_3|1\rangle) \\ &= a_1a_2a_3|000\rangle + a_1a_2b_3|001\rangle + a_1b_2a_3|010\rangle + a_1b_2b_3|011\rangle + \\ & \quad b_1a_2a_3|100\rangle + b_1a_2b_3|101\rangle + b_1b_2a_3|110\rangle + b_1b_2b_3|111\rangle \\ &\equiv (a_1a_2a_3, a_1a_2b_3, a_1b_2a_3, a_1b_2b_3, b_1a_2a_3, b_1a_2b_3, b_1b_2a_3, b_1b_2b_3)^T \end{aligned} \quad (6)$$

The scalar product of these vector vanishes for the particular value assignments $a_1 = a_2 = a_3 = 0$ and thus $b_1 = b_2 = b_3 = 1$. Alas, this particular value assignment is improper to separate other cases such as, for instance, f_8 and $f_{15} = 1$ orthogonally.

IV. SUMMARY

The main goal of this paper has been a discussion of, and the enumeration of criteria for encoding some algorithmic task into quantum mechanically feasible orthogonal subspaces. This is by no means a trivial task.

With regards to somehow “mapping” a functional behaviour into Hilbert space, such that certain relational or holistic functional properties—manifesting themselves in the *relational* values for different elements of their domain, and only after the evaluation of more than one classical input—reveal themselves through efficient quantum queries, the situation is what may be called “ambivalent.”

On the one hand, relative to some quantum oracle, it is sometimes impossible to decide certain relational or functional properties, simply because this particular quantum oracle is unsuitable to render the appropriate orthogonal subspaces.

On the other, more promising, hand, by the orthogonalisation via dimensional lifting of non-orthogonal vectors, it cannot be excluded that any functional property can be mapped into orthogonal subspaces of some Hilbert space of higher dimension than the space spanned by the original non-orthogonal vectors. In this sense, any functional property, including parity, might be decidable by a single quantum query.

The situation is not dissimilar to the purification of a mixed state, where the “missing information” is (non-uniquely) supplemented by fitting hypotheses or conjectures (about the original pure state). However, this generalized Gram-Schmidt process is not unitary in general, and thus does not correspond to any quantum capacity.

So far, all quantum speedups based on orthogonalisation

tion have been *ad hoc*; no method to convert or translate a general functional behavior encoded by a coherent superposition of functional clauses (and made injective by adding bits) into orthogonal subspaces of a Hilbert space has been found. Also the method of dimensional lifting introduced here is quantum infeasible because it is non-unitary (translating non-orthogonal vector into orthogonal ones). Therefore, the question remains of whether a general unitary method of dimensional lifting, possibly utilizing auxiliary bits, can be found.

ACKNOWLEDGMENTS

Acknowledgments: This work was supported in part by the European Union, Research Executive Agency (REA), Marie Curie FP7-PEOPLE-2010-IRSES-269151-RANPHYS grant.

-
- [1] Armin Hermann, *Frühgeschichte der Quantentheorie (1899-1913)* (Physik Verlag, Mosbach in Baden, 1969) Habilitationsschrift, Naturwissenschaftliche Fakultät der Universität München.
- [2] Erwin Schrödinger, *The Interpretation of Quantum Mechanics. Dublin Seminars (1949-1955) and Other Unpublished Essays* (Ox Bow Press, Woodbridge, Connecticut, 1995).
- [3] Erwin Schrödinger, “Die gegenwärtige Situation in der Quantenmechanik,” *Naturwissenschaften* **23**, 807–812, 823–828, 844–849 (1935).
- [4] Albert Einstein, “Letter to Schrödinger,” (1935), old Lyme, dated 19.6.35, Einstein Archives 22-047 (searchable by document nr. 22-47).
- [5] Don Howard, “Einstein on locality and separability,” *Studies in History and Philosophy of Science Part A* **16**, 171–201 (1985).
- [6] Paul A. M. Dirac, *The Principles of Quantum Mechanics* (Oxford University Press, Oxford, 1930).
- [7] Garrett Birkhoff and John von Neumann, “The logic of quantum mechanics,” *Annals of Mathematics* **37**, 823–843 (1936).
- [8] E. Bernstein and U. Vazirani, “Quantum complexity theory,” in *Proceedings of the 25th Annual ACM Symposium on Theory of Computing, San Diego, California, May 16-18, 1993* (ACM Press, 1993) pp. 11–20.
- [9] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani, “Strengths and weaknesses of quantum computing,” *SIAM Journal on Computing* **26**, 1510–1523 (1997), arXiv:quant-ph/9701001.
- [10] Lance Fortnow, “One complexity theorist’s view of quantum computing,” *Theoretical Computer Science* **292**, 597–610 (2003).
- [11] Giuseppe Castagnoli, “Highlighting the mechanism of the quantum speedup by time-symmetric and relational quantum mechanics,” (2013), arXiv:1308.5077.
- [12] Karl Svozil, “Unscrambling the quantum omelette,” *International Journal of Theoretical Physics* **53**, 3648–3657 (2014), arXiv:1206.6024.
- [13] Paul R. Halmos, *Finite-dimensional Vector Spaces* (Springer, New York, Heidelberg, Berlin, 1974).
- [14] Alastair A. Abbott, Cristian S. Calude, and Karl Svozil, “A variant of the Kochen-Specker theorem localising value indefiniteness,” *Journal of Mathematical Physics* **56**, 102201 (2015), arXiv:1503.01985.
- [15] Karl Svozil, “Quantum information via state partitions and the context translation principle,” *Journal of Modern Optics* **51**, 811–819 (2004), arXiv:quant-ph/0308110.
- [16] Andrew M. Gleason, “Measures on the closed subspaces of a Hilbert space,” *Journal of Mathematics and Mechanics (now Indiana University Mathematics Journal)* **6**, 885–893 (1957).
- [17] Simon Kochen and Ernst P. Specker, “The problem of hidden variables in quantum mechanics,” *Journal of Mathematics and Mechanics (now Indiana University Mathematics Journal)* **17**, 59–87 (1967).
- [18] Itamar Pitowsky, “From George Boole to John Bell: The origin of Bell’s inequality,” in *Bell’s Theorem, Quantum Theory and the Conceptions of the Universe*, Fundamental Theories of Physics, Vol. 37, edited by Menas Kafatos (Springer (Kluwer), Dordrecht, 1989) pp. 37–49.
- [19] David N. Mermin, *Quantum Computer Science* (Cambridge University Press, Cambridge, 2007).
- [20] Anton Zeilinger, “Quantum teleportation and the non-locality of information,” *Philosophical Transactions of the Royal Society of London A* **355**, 2401–2404 (1997).
- [21] Anton Zeilinger, “A foundational principle for quantum mechanics,” *Foundations of Physics* **29**, 631–643 (1999).
- [22] A. Einstein, “Quanten-Mechanik und Wirklichkeit,” *Dialectica* **2**, 320324 (1948).
- [23] Julian Schwinger, “Unitary operators bases,” *Proceedings of the National Academy of Sciences (PNAS)* **46**, 570–579 (1960).
- [24] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” *Physical Review Letters* **70**, 1895–1899 (1993).
- [25] X. Y. Zou, L. J. Wang, and L. Mandel, “Induced coherence and indistinguishability in optical interference,” *Physical Review Letters* **67**, 318–321 (1991).
- [26] Asher Peres, “Can we undo quantum measurements?” *Physical Review D* **22**, 879–883 (1980).
- [27] Marlan O. Scully and Kai Drühl, “Quantum eraser: A proposed photon correlation experiment concerning observation and “delayed choice” in quantum mechanics,” *Physical Review A* **25**, 2208–2213 (1982).
- [28] Berthold-Georg Englert, Julian Schwinger, and Marlan O. Scully, “Is spin coherence like Humpty-Dumpty? I. Simplified treatment,” *Foundations of Physics* **18**, 1045–1056 (1988).
- [29] Hugh Everett III, “‘Relative State’ formulation of quantum mechanics,” *Reviews of Modern Physics* **29**, 454–462 (1957).
- [30] Eugene P. Wigner, “Remarks on the mind-body question,” in *The Scientist Speculates*, edited by I. J. Good (Heinemann and Basic Books, London and New York, 1961) pp. 284–302.

- [31] John S. Bell, “Against ‘measurement’,” *Physics World* **3**, 33–41 (1990).
- [32] Wayne C. Myrvold, “Statistical mechanics and thermodynamics: A Maxwellian view,” *Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics* **42**, 237–243 (2011).
- [33] Edwin Thompson Jaynes, “Clearing up mysteries - the original goal,” in *Maximum-Entropy and Bayesian Methods: : Proceedings of the 8th Maximum Entropy Workshop, held on August 1-5, 1988, in St. John’s College, Cambridge, England*, edited by John Skilling (Kluwer, Dordrecht, 1989) pp. 1–28.
- [34] Edwin Thompson Jaynes, “Probability in quantum theory,” in *Complexity, Entropy, and the Physics of Information: Proceedings of the 1988 Workshop on Complexity, Entropy, and the Physics of Information, held May - June, 1989, in Santa Fe, New Mexico*, edited by Wojciech Hubert Zurek (Addison-Wesley, Reading, MA, 1990) pp. 381–404.
- [35] Daniel F. Galouye, *Simulacron 3* (Bantam Books, New York, NY, 1964).
- [36] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser, “Limit on the speed of quantum computation in determining parity,” *Physical Review Letters* **81**, 5442–5444 (1998), [arXiv:quant-ph/9802045](#).
- [37] Edward F. Moore, “Gedanken-experiments on sequential machines,” in *Automata Studies*, edited by C. E. Shannon and J. McCarthy (Princeton University Press, Princeton, NJ, 1956) pp. 129–153.
- [38] Karl Svozil, “Logical equivalence between generalized urn models and finite automata,” *International Journal of Theoretical Physics* **44**, 745–754 (2005), [arXiv:quant-ph/0209136](#).
- [39] Niko Donath and Karl Svozil, “Finding a state among a complete set of orthogonal ones,” *Physical Review A* **65**, 044302 (2002), [arXiv:quant-ph/0105046](#).
- [40] Karl Svozil, “Quantum information in base n defined by state partitions,” *Physical Review A* **66**, 044306 (2002), [arXiv:quant-ph/0205031](#).
- [41] Karl Svozil and Josef Tkadlec, “On the solution of trivalent decision problems by quantum state identification,” *Natural Computing in print, in print* (2009).
- [42] Hans Havlicek, Private communication.
- [43] L. Schläfli, *Theorie der vielfachen Kontinuität* (Zürcher & Furrer, Zürich, 1901) pp. 134–139, ed. by J. H. Graf for the Denkschriften-Kommission der Schweizerischen Naturforschenden Gesellschaft. Separatabdruck aus den Denkschriften der Schweizerischen Naturforschenden Gesellschaft. Band XXXVIII. 1st half.
- [44] Dietrich Haase and Hellmuth Stachel, “Almost-orthonormal vector systems,” *Beitr. Algebra Geom.* **37**, 367–381 (1996).
- [45] Karl Svozil, “Quantum queries associated with equipartitioning of states and multipartite relational encoding across space-time,” (2015).