Finding a state among a complete set of orthogonal states

Niko Donath and Karl Svozil*
Institut für Theoretische Physik, University of Technology Vienna, Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria
(Received 11 May 2001; revised manuscript received 17 October 2001; published 21 March 2002)

We consider the problem to single out a particular state among 2^n orthogonal pure states. As it turns out, in general the optimal strategy is not to measure the particles separately, but to consider joint properties of the n-particle system. The required number of propositions is n. There exist $2^n!$ equivalent operational procedures to do so. We enumerate some configurations for three particles, in particular the Greenberger-Horne-Zeilinger (GHZ) and W states, which are specific cases of a unitary transformation. For the GHZ case, an explicit physical meaning of the projection operators is discussed.

DOI: 10.1103/PhysRevA.65.044302 PACS number(s): 03.67.−a, 03.65.Ta, 03.65.Fd

Suppose "Bob" is told that "Alice" has prepared n two-state systems in a particular pure state among $N=2^n$ pure states. Assume further that these pure states correspond to a complete orthonormal basis of some N-dimensional Hilbert space. Both Bob and Alice know beforehand which basis is used. Bob's task is to find out which particular single one of the 2^n states Alice has chosen to communicate to him.

The difference to a classical weighting problem (e.g., [1,2]) associated with finding the correct number among 2^n ones encoded by n coins of two coin types is the entanglement of the quantum objects. That is, the information may be distributed over the objects in such a way as to make impossible its recovery by just looking at the individual objects. Thus the classical performance will not be improved but *extended* by the quantum case.

As can be expected, there exist efficient and expensive search strategies for such a task. The "worst" strategy (besides mere repetition) would be to check the proposition corresponding to each individual pure state, asking, "is the system in state i?" for $i=1,\ldots,2^n$. Yet, by exploiting the *joint properties* of the n systems, we may expect to reduce the complexity of Bob's task.

In what follows we shall thus deal with the following questions aimed at a systematic understanding of the state determination problem. (i) What is the minimal set of propositions (i.e., operationalizable yes-no statements) which singles out a particular pure state of n entangled two-state systems from other orthogonal pure states? (ii) How many different but equivalent sets of propositions can be defined? (iii) What is the explicit form and physical interpretation of the propositions associated with an arbitrary basis?

As it turns out, the number of propositions required for solving the problem can be reduced to n, which is an exponential gain with respect to the worst strategy just mentioned. This result is in agreement with Zeilinger's foundational principle stating that n elementary two-state systems carry n classical bits; i.e., the answer to at most n questions concerning their physical properties [3]. In classical information theory a proposition is the yes-no statement settling a question with two possible answers. In standard quantum logic [4–7], quantum propositions are identified with projection operators. The eigenvalues 0 and 1 of these projection operators are identified with the two possible yes-no answers, respectively.

Conversely, by assuming Zeilinger's principle, it should be possible to define n-particle quantum states by the set of eigenvalues associated with quantum-mechanical propositions. When choosing the "optimal" strategy, n propositions should suffice. However, one could also take an arbitrary number of consistent propositions. If these are not "optimal" in a well-defined sense, then this results in nonpure quantum states.

Consider a $2^n=N$-dimensional Hilbert space of n particles in two states (labeled by "1," "2," or "up," "down," or "+," "−," or whatever). The standard orthonormal basis is given by (superscript "T" indicates transposition)

$$\{|e_1\rangle=|+++\cdots+\rangle\equiv(1,0,0,\ldots,0)^T,$$
$$\vdots$$
$$|e_N\rangle=|---\cdots-\rangle\equiv(0,0,0,\ldots,1)^T\}. \qquad (1)$$

Let us first concentrate on an enumeration of all propositions which uniquely distinguish the N vectors that form an orthogonal basis of an N-dimensional vector space. This task corresponds to the construction of projection operators—which have some operational interpretation(s) in terms of (quantum-mechanical) measurements—whose combined effect is the separation of each individual base state from all the other ones. In that respect, the measurement apparatus and the associated propositions act as filters which effectively generate a *partitioning* of some orthonormal basis into partitions which contain only single elements of that basis (i.e., one basis element per partition element). Formally, the projections induce an equivalence relation on the set of base states.

We shall impose the following requirements upon the propositions. (i) All propositions are comeasurable (i.e., the associated projections commute). (ii) Any single proposition separates half of the elements of the orthogonal base vectors from the other half; i.e., any proposition F_i generates a 50:50 partition f_i with $|f_i|=2$ and the kth element $f_{i,k}\in f_i$ of the partition f_i (note that $|f_{i,k}|=N/2$ and "$|x|$" stands for the

*Electronic address: svozil@tuwien.ac.at; http://tph.tuwien.ac.at/~svozil

number of elements of a finite set x). (iii) For any two propositions F_i, F_j, $i \neq j$, the intersection of elements of the associated partitions f_i, f_j of some orthogonal basis reduce the size of the elements of the partitions by a factor of two.

We shall introduce an optimal algorithm implementing these requirements which uses exactly n propositions to decompose every orthonormal basis of the N-dimensional vector space. It implements a binary search strategy which can be enumerated as follows: separate the first $N/2$ vectors from the second $N/2$. Then, within every such block, separate the first $N/4$ vectors from the second $N/4$. Iterate these procedures by reducing the block size by a factor of two in each step until blocks of size one are reached. This ''state sieve'' is an optimal search strategy in the sense that in general no shorter proposition system exists which separates each individual state of the standard orthonormal basis [15].

The explicit form of the operators are (''diag'' stands for a diagonal matrix)

$$O_1 = \text{diag}\left(\underbrace{1,\ldots,1}_{N/2},\underbrace{0,\ldots,0}_{N/2}\right), \tag{2}$$

$$O_2 = \text{diag}\left(\underbrace{1,\ldots,1}_{N/4},\underbrace{0,\ldots,0}_{N/4},\underbrace{1,\ldots,1}_{N/4},\underbrace{0,\ldots,0}_{N/4}\right), \tag{3}$$

$$\vdots$$

$$O_n = \text{diag}\left(\underbrace{1,0,1,0,\ldots,1,0}_{N}\right), \tag{4}$$

and the orthogonal operators $O_i' = 1 - O_i$. All these projections commute with one another. They are listed by the reverse lexicographic order of their diagonal elements. Their associated propositions can be stated as follows:

$O_1 \equiv$ ''The first particle is in state $+$.''

$O_2 \equiv$ ''The second particle is in state $+$.''

$\vdots$

$O_n \equiv$ ''The nth particle is in state $+$.''

It is easy to verify that these operators are projection operators and that they mutually commute; i.e., $O_i O_i = O_i$, $[O_i, O_j] = 0$, for all $i,j \in \{1,\ldots,N\}$. Physically, this scheme amounts to a nondestructive successive and conditional measurement of the propositions $O_1,\ldots,O_n$, relating to, say, electron spins in external magnetic fields (cf. Fig. 1 for $n=3$). Bob needs just one copy of the state of N particles to find out Alice's selection.

Having now dealt with the question (i) of the minimal set of propositions for the problem and having partly discussed a particular case of question (iii), let us now turn to the question of how many equivalent systems of operators and propositions exist. Notice that only diagonal matrices containing

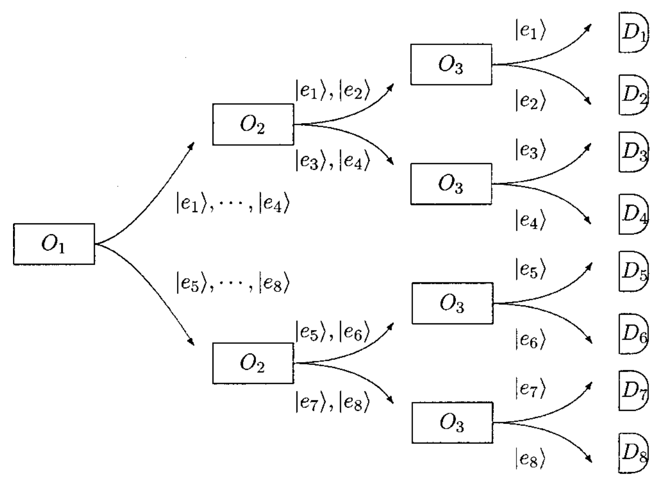

FIG. 1. State sieve resulting from binary search. Successive measurements of propositions O_1, O_2, O_3 serve as filters to single out the input state. $D_1,\ldots,D_8$ indicate the final detectors; in the lossless case, exactly one of them clicks.

$1s$ and $0s$ in the principal diagonal can be eigenmatrices of the standard orthonormal basis (1). For this particular basis, the only possible variations are obtained as follows. First, the diagonals of $O_1, O_2,\ldots,O_n$ are written below each other. If one considers the columns of this listing, each one of the N columns of length n represents a unique number $N = a_1 > a_2 > \cdots > a_{N-1} > a_N = 0$ in binary notation and in strictly decreasing order. Other valid state sieves are obtained by exchanging two arbitrary columns. This amounts to the permutation of N different n-ary columns. The total number of such entities and thus of all equivalent systems of n propositions is $N! = 2^n!$.

Let us demonstrate the construction by considering the case $n=3$, $N=8$ (e.g., three spin 1/2 particles). The operators can be written in a diagonal form

$$O_1 = \text{diag}(1,1,1,1,0,0,0,0), \tag{5}$$

$$O_2 = \text{diag}(1,1,0,0,1,1,0,0), \tag{6}$$

$$O_3 = \text{diag}(1,0,1,0,1,0,1,0). \tag{7}$$

Some of the permutations yielding $8! = 40\,320$ equivalent systems of three propositions are enumerated in Table I. The cascade of filters representable by projection operators (5)–(7) and interpretable as elementary yes-no propositions are depicted in Fig. 1. Any permutation of these measurements yields the same partitioning of states.

TABLE I. Enumeration of the $8!$ equivalent variations of propositions for $n=3$, $N=2^3=8$.

11110000		11110000		00001111
11001100	$\leftrightarrow$	11001100	$\leftrightarrow\cdots\leftrightarrow$	00110011
10101010		01101010		01010101

An arbitrary orthonormal basis of an N-dimensional vector space can be defined as the isometric transforms of the standard orthonormal basis (1). If the vector space is complex (i.e., C^N), these isometries are the unitary transforms. Furthermore, any basis change in C^N from one orthonormal basis into another one can be represented by some unitary matrix U; i.e., $|b_i\rangle = U|e_i\rangle$. The group of unitary transformations $U(N)$ in N-dimensional Hilbert space has N^2 parameters. In the following we shall study this entire group rather than the transformations resulting from the combined effect of $[U(2)]^n$, which are again unitary transformations (this would unnecessarily restrict the general case).

Thus the problem of finding the N propositions for the basis $|b_i\rangle$ can simply be solved by transforming the propositions for the vector space; i.e., $O_i^b = UO_i^e U^{-1}$. Here, $O = O^e$ for some $O^e \in \{O_1, \ldots, O_N\}$. These propositions have the same eigenvalues as the propositions, since if we identify $O^e|e_i\rangle = \lambda|e_i\rangle$, then $O^b|b_i\rangle = UO^eU^{-1}U|e_i\rangle = \lambda U|e_i\rangle = \lambda|b_i\rangle$.

In Ref. [3] Zeilinger poses the following question, "What are the three propositions which can be used to uniquely define the eight states of the three-particle case?" Consider the eight orthonormal Greenber-Horne-Zeilinger (GHZ)-basis states

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|+++\rangle + |---\rangle) \equiv (1,0,0,0,0,0,0,1)^T \equiv |111\rangle$$

$$\vdots$$

$$|\psi_8\rangle = \frac{1}{\sqrt{2}}(|-++\rangle - |+--\rangle) \equiv (0,0,0,1,-1,0,0,0)^T \equiv |000\rangle. \tag{8}$$

They can be interpreted as follows. The relative directions of the three spins are fixed but their respective values undetermined. Thus, one measurement on each one of the t hree particles will suffice to know the exact values of all spins. It is possible to characterize the states according to the truth value of the propositions below by $|111\rangle$ to $|000\rangle$. Just as before, let us define the vector components of the standard orthonormal basis states as $|+++\rangle \equiv (1,0,0,0,0,0,0,0)^T, \ldots, |---\rangle \equiv (0,0,0,0,0,0,0,1)^T$. Let U^{GHZ} be the unitary matrix which transforms this standard basis into the GHZ-basis. An explicit calculation shows that the matrices $O_i = O_i^{\mathrm{GHZ}} = U^{\mathrm{GHZ}} O_i^e (U^{\mathrm{GHZ}})^{-1}$, $i=1,2,3$, can be written as follows:

$$O_1 = \mathrm{diag}(1,1,0,0,0,0,1,1), \tag{9}$$

$$O_2 = \mathrm{diag}(1,0,1,0,0,1,0,1), \tag{10}$$

$$O_3 = \frac{1}{2}\begin{pmatrix} 1&0&0&0&0&0&0&1\\ 0&1&0&0&0&0&1&0\\ 0&0&1&0&0&1&0&0\\ 0&0&0&1&1&0&0&0\\ 0&0&0&1&1&0&0&0\\ 0&0&1&0&0&1&0&0\\ 0&1&0&0&0&0&1&0\\ 1&0&0&0&0&0&0&1 \end{pmatrix}. \tag{11}$$

O_1 distinguishes the first four states from the second four and thus induces a partition (we abbreviate $|\psi_j\rangle$ by j) $[\{1,2,3,4\},\{5,6,7,8\}]$ of the GHZ-basis states. O_2 distinguishes 1,2,5,6 from 3,4,7,8 and thus induces a partition $[\{1,2,5,6\},\{3,4,7,8\}]$ of the GHZ-basis states. O_3 identifies the relative phases and thus induces a partition $[\{1,3,5,7\},\{2,4,6,8\}]$ of the GHZ-basis states. The three matrices are mutually commutative. Their combined effect is an atomic partition of the set of base states $[\{1\},\{2\},\{3\},\{4\},\{5\},\{6\},\{7\},\{8\}]$ which is the formal analogue of the experimental sieve. It is obtained by a successive application of experiments, represented by the intersection of each partition element of O_i with all the other ones. Notice also that [16] $O_3 = \frac{1}{2}(1 + \sigma_{1x}\sigma_{2x}\sigma_{3x})$.

The propositions associated with these operators are as follows. O_1 corresponds to the statement that "the spin of the first and the spin of the second particle are the same in the z direction." O_2 corresponds to the statement that "the spin of the first and the spin of the third particle are the same in the z direction." O_3 corresponds to the statement that "an even number of spins is pointing down when measured in the x direction." This result can be generalized to the case of n particles in a straightforward manner. Thereby, $n-1$ propositions characterize the relative spins of the particles, and also the nth proposition is the same as above.

Another, equivalent but permutated set of propositions was proposed by Cereceda [8,9]: $T_1 = \frac{1}{2}(1 + \sigma_{1x}\sigma_{2y}\sigma_{3y})$, $T_2 = \frac{1}{2}(1 + \sigma_{1y}\sigma_{2x}\sigma_{3y})$, and $T_3 = \frac{1}{2}(1 + \sigma_{1y}\sigma_{2y}\sigma_{3x})$. Since the transformation matrix U^{GHZ} remains the same, the projection operators differ from the previous ones (9)–(11) by a permutation of the propositional system (5)–(7) yielding equivalent, though not identical propositions. This can be explicitly seen by taking row permutations of the operators (5)–(7)

$$O_1 = \mathrm{diag}(0,1,1,0,1,0,0,1), \tag{12}$$

$$O_2 = \mathrm{diag}(0,1,1,0,0,1,1,0), \tag{13}$$

$$O_3 = \mathrm{diag}(0,1,0,1,1,0,1,0), \tag{14}$$

such that $T_i = U^{\mathrm{GHZ}} O_i (U^{\mathrm{GHZ}})^{-1}$, $i=1,2,3$. The physical interpretations of T_i [cf. question (iii)] are as follows [8]. T_1 corresponds to the statement that "the product of the spin of particles 1, 2, and 3 along the axes x, y, and y, respectively, is equal to 1." T_2 corresponds to the statement that "the product of the spin of particles 1, 2, and 3 along the axes y, x, and *y*, respectively, is equal to 1.'' T_3 corresponds to the statement that ''the product of the spin of particles 1, 2, and 3 along the axes *y*, *y*, and *x*, respectively, is equal to 1.'' The associated GHZ-base state partitions are $[\{1,4,6,7\},\{2,3,5,8\}]$ for O_1, $[\{1,4,5,8\},\{2,3,6,7\}]$ for O_2, and $[\{1,3,6,8\},\{2,4,5,7\}]$ for O_3, respectively.

The method proposed here is quite general and can, for instance, be applied to another set of orthonormal base states of eight-dimensional Hilbert space which contains the *W* state introduced in [10] and discussed in [11]. Still another orthonormal basis contains all elements of the standard orthogonal basis equally weighted. For the above cases, projection operators $Q_j = U^{W} O_i^{e} U^{W\dagger}$, $j=1,2,3$, can be defined, whereby the operators O_1, O_2, O_3 produce parti- tions $[\{1,2,3,4\},\{5,6,7,8\}]$, $[\{1,2,5,6\},\{3,4,7,8\}]$, and $[\{1,3,5,7\},\{2,4,6,8\}]$ of the original basis, respectively. (Any vertical permutation thereof would be equally suitable.) As before, all Q_i can be given a direct physical interpretation in terms of ''clicks in a counter'' [12], but their meaning cannot be expressed in elementary statements.

In summary, we have shown that, given *n* quantized two-state systems, *n* propositions are enough to find and separate any individual pure state from others of an arbitrary orthogonal basis. There exist $2^n!$ equivalent sets of *n* propositions achieving this. They all differ by permutations from one another. By considering the simplest case of the standard orthogonal basis, we have been able to explicitly construct these sets of propositions and their corresponding projection operators. Any other orthogonal basis system and the corresponding more general projection operators can be obtained from this standard orthogonal one by unitary transformations. We have explicitly discussed two equivalent solutions of the state determination problem for the GHZ-base states and mentioned the *W* state and more general cases. We conclude that the optimal strategy to single out particular states is in general based on a measurement of the joint properties of the particles rather than the properties of the individual particles.

The authors would like to acknowledge stimulating discussions and suggestions by Časlav Brukner and Anton Zeilinger. We also would like to thank Daniel Greenberger for pointing out similarities to classical weighting cases.

[1] C.A.B. Smith, Mathematical Gazette **31**, 31 (1947).
[2] S.S. Cairns, Am. Math. Monthly **70**(5), 136 (1963).
[3] A. Zeilinger, Found. Phys. **29**(4), 631 (1999).
[4] G. Birkhoff and J. von Neumann, Ann. Math. **37**(4), 823 (1936).
[5] G.W. Mackey, Amer. Math. Monthly, Supplement **64**(8), 45 (1957).
[6] S. Kochen and E.P. Specker, J. Math. Mech. **17**(1), 59 (1967); see also [13], p. 235.
[7] K. Svozil, *Quantum Logic* (Springer, Singapore, 1998).
[8] J.L. Cereceda (private communication).
[9] N.D. Mermin, Phys. Today **43**(6), 9 (1990).
[10] A. Zeilinger, M.A. Horne, and D.M. Greenberger, in *NASA Conf. Publ. No. 3135* (National Aeronautics and Space Administration, Code NTT, Washington, DC, 1997).
[11] W. Dür, G. Vidal, and J.I. Cirac, Phys. Rev. A **62**, 062314 (2000).
[12] M. Reck, A. Zeilinger, H.J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994); see also [14].
[13] E. Specker, *Selecta* (Birkhäuser Verlag, Basel, 1990).
[14] F.D. Murnaghan, *The Unitary and Rotation Groups* (Spartan Books, Washington, DC, 1962).
[15] Optimality is a consequence of the classical binary search, given the premises.
[16] Recall that $\sigma_{1x} \equiv \sigma_x \otimes 1_4$, $\sigma_{2x} \equiv 1_2 \otimes \sigma_x \otimes 1_2$, $\sigma_{3x} \equiv 1_4 \otimes \sigma_x$. The tensor product $\otimes$ of two second degree tensors a,b representable by two $n\times n$ and $m\times m$ matrices whose components are a_{ij} and $b_{k,l}$ can be represented by an $nm\times nm$ matrix

$$(a\otimes b)_{s,t} = a_{\lceil s/m\rceil,\lceil t/m\rceil} b_{s-\lfloor (s-1)/m\rfloor m,\, t-\lfloor (t-1)/m\rfloor m}, \quad s,t=1,\ldots,nm,$$

where $\lceil x\rceil$ stands for the smallest integer greater than or equal to *x*, and $\lfloor x\rfloor$ stands for the greatest integer less than or equal to *x*, respectively.