Mutually unbiased binary observable sets on *N* qubits

Jay Lawrence,[1] Časlav Brukner,[2] and Anton Zeilinger[2]
[1]*Department of Physics, Dartmouth College, Hanover, New Hampshire 03755*
[2]*Institute for Experimentalphysics, University of Vienna, Boltzmanngasse 5, A–1090 Vienna, Austria*
(Received 17 October 2001; published 27 February 2002)

The Pauli operators (tensor products of Pauli matrices) provide a complete basis of operators on the Hilbert space of N qubits. We prove that the set of 4^N-1 Pauli operators may be partitioned into 2^N+1 distinct subsets, each consisting of 2^N-1 internally commuting observables. Furthermore, each such partitioning defines a unique choice of 2^N+1 mutually *unbiased* basis sets in the N-qubit Hilbert space. Examples for 2 and 3 qubit systems are discussed with emphasis on the nature and amount of entanglement that occurs within these basis sets.

DOI: 10.1103/PhysRevA.65.032320 PACS number(s): 03.67.−a, 03.65.Ta, 03.65.Ud

I. INTRODUCTION

A pure quantum state of an N-qubit system is specified by the eigenvalues of N independent commuting binary observables (''N qubits carry N bits of information'' [1,2]). In fact, a complete set of 2^N such states are so specified, each being associated with a binary number consisting of the N eigenvalues. Of the many alternative choices of observable sets that define N-qubit basis sets, we are interested in those that are maximally incompatible in the sense that a state producing precise measurement results in one set produces maximally random results in the other.

The Pauli operators [3] provide an explicit realization of points raised above. First, they illustrate that although a greater number 2^N-1 of observables simultaneously take definite values, only N of these are required to define a pure state, and in fact these N generate all of the remaining compatible observables through multiplication. On the other hand, all 4^N-1 Pauli operators are required in order to determine an arbitrary mixed state. In this connection, we shall show that the full set of these operators is exhausted in forming 2^N+1 distinct subsets, each consisting of 2^N-1 internally commuting observables, and each defining its own unique eigenbasis. Both the observable sets and the corresponding basis sets are called mutually unbiased [4] (and in previous works the observable sets have also been called mutually complementary [2]) because of the following physical property: If an N qubit system is prepared in a joint eigenstate of one such observable set, then it has a uniform probability distribution over the joint eigenstates of any of the other sets. It follows that all $2^N(2^N-1)$ observables outside the original (maximal) set of 2^N-1 compatible observables will produce measurement results that are uniformly distributed over all possibilities. Since the Pauli operators have binary spectra, it also follows that their dispersion is maximized.

The equivalence of unbiasedness of basis sets and operator sets may be understood from the formal definition as applied to basis sets, which may be summarized in general terms as follows: Let us denote basis sets by $A=1,2,\ldots,$ and states within a basis by $|A,\alpha\rangle$, with $\alpha=1,2,\ldots,d$ (for the moment, we consider a Hilbert space with general dimension d, although our interest here is in $d=2^N$). Two bases A and B are said to be mutually unbiased [4,5] if a system prepared in any element of A (such as $|A,\alpha\rangle$) has a uniform probability distribution of being found in any element of B,

$$|\langle A,\alpha|B,\beta\rangle|^2=d^{-1},\quad (A\neq B), \tag{1}$$

where individual bases are understood to be orthonormal,

$$\langle A,\alpha|A,\beta\rangle=\delta_{\alpha\beta}. \tag{2}$$

Certainty of measurement outcomes for the operator set defining the $|A,\alpha\rangle$'s implies a uniform probability distribution over states $|B,\beta\rangle$, and this in turn implies a uniform probability distribution over all eigenvalue sets (and distinct measurement outcomes) of operators defining the $|B,\beta\rangle$'s.

A particular motivation for considering unbiased basis sets is that they provide for the most efficient determination, using measurements alone, of a general (pure or impure) quantum state [6]. In a d-dimensional Hilbert space, one needs d^2-1 real parameters to specify a general density matrix ρ, which must be Hermitean and have $\mathrm{Tr}(\rho)=1$. Since measurements within a particular basis set can yield only $d-1$ independent probabilities, one needs $d+1$ distinct basis sets to provide the required total number of d^2-1 independent probabilities. Ivanović [5] showed that the required number $d+1$ of unbiased basis sets indeed exists if d is a prime number, and Wootters and Fields [6] showed that it exists if d is any *power* of a prime number. Our proof is based upon this theorem of Wootters and Fields.

The question of the existence and construction of unbiased basis sets is interesting not only from a fundamental point of view (e.g., in the formulation of ''quantum mechanics without probability amplitudes'' [4], and in the information-theoretic formulation of quantum mechanics [2]), but also as an important ingredient in quantum-information protocols (e.g., in the solution of ''the mean king's problem'' [7] and in quantum cryptography [8]). In particular, it was found recently that key distributions based on higher-dimensional quantum systems with larger numbers of unbiased basis sets can have certain advantages over those based on qubits [9].

The present paper illustrates how the study of operator relationships can provide a useful approach to the construc-

tion of unbiased basis sets of entangled as well as product character. The N-qubit Hilbert space has dimension $d=2^N$, and operators on this space (which include the density matrix) live in their own vector space of dimension 4^N. The complete basis consisting of the Pauli operators [3] may be written as follows: Starting with the usual 2×2 Pauli matrices and the identity I that act on the spaces of individual qubits,

$$\sigma_\mu=(\sigma_x,\sigma_y,\sigma_z,I), \quad \mu=(1,2,3,4), \tag{3}$$

we write the 4^N tensor products (the Pauli operators and identity $\mathcal{I}$) that act on the N-qubit Hilbert space as

$$O_i=\sigma^1_{\mu(1,i)}\sigma^2_{\mu(2,i)}\cdots\sigma^N_{\mu(N,i)}=\prod_{k=1}^{N}\sigma^k_{\mu(k,i)}, \tag{4}$$

where k is the particle label and i distinguishes among the 4^N choices of the N subscripts $\mu(k,i)$. This basis is *orthonormal* [10]; the inner product of two operators is defined as the trace of their product,

$$\mathrm{Tr}(O_iO_j)=\prod_{k=1}^{N}\mathrm{Tr}(\sigma^k_{\mu(k,i)}\sigma^k_{\mu(k,j)})=\prod_{k=1}^{N}2\,\delta_{\mu(k,i)\mu(k,j)}$$
$$=2^N\delta_{ij}, \tag{5}$$

where $i=j$ means that $\mu(k,i)=\mu(k,j)$ for every particle k. Like the individual Pauli matrices, each tensor product is self-inverse, $O_i^2=\mathcal{I}$, and apart from the identity (for which we reserve $i=4^N$ so that $O_{4^N}=I^1I^2\ldots I^N\equiv\mathcal{I}$) they are all traceless and have eigenvalues ± 1.

The binary spectrum for each observable O_i permits its expression as a binary proposition: The two eigenvalues ± 1 of the observable O_i correspond to the values ''true'' or ''false'' of the proposition ''The product of the spin projections $\sigma^1_{\mu(1,i)}\sigma^2_{\mu(2,i)}\cdots\sigma^N_{\mu(N,i)}$ is $+1$.'' (If a particular σ^k_μ happens to be the identity, then no statement is made about the kth qubit.)

II. GENERAL RESULTS FOR N QUBITS

We may now proceed to demonstrate the main formal points of the paper: First, that the set of 4^N-1 Pauli operators (excluding the identity) may be partitioned into 2^N+1 subsets, each consisting of 2^N-1 internally commuting members, and second, that every such partitioning defines a unique choice of unbiased basis sets (i.e., there is a one-to-one mapping from partitionings to choices of unbiased basis sets).

The first part makes use of the proven existence of 2^N+1 unbiased basis sets [6]. The projectors onto the unbiased basis states,

$$P^A_\alpha=|A,\alpha\rangle\langle A,\alpha|, \tag{6}$$

may be used to re-express the unbiasedness of bases $A\neq B$ [Eq. (1)] as

$$\mathrm{Tr}(P^A_\alpha P^B_\beta)=2^{-N}, \tag{7}$$

and to define a set of operators O^A_a by their spectral decompositions

$$O^A_a=\sum_{\alpha=1}^{2^N}\varepsilon_{a\alpha}P^A_\alpha. \tag{8}$$

We *define* $\varepsilon_{a\alpha}$ as a $2^N\times 2^N$ matrix consisting of orthogonal row vectors, one of whose entries are all $+1$'s, and the remaining of whose entries are equal numbers of $+1$'s and -1's. There are exactly 2^N such orthogonal vectors, the components of each vector a being the eigenvalues of O^A_a. One of these operators (say the $a=2^N$th) is proportional to the identity, $O^A_{2^N}=\mathcal{I}$. We include this to make Eq. (8) invertible, which will be useful later. The columns α label the joint eigenstates of the O^A_a ($a=1,2,\ldots,2^N-1$), and comprise the truth tables associated with the 2^N-1 corresponding propositions. This labeling is redundant; clearly an appropriate subset of just N rows may be used to construct N-component column vectors that define all 2^N joint eigenstates unambiguously as binary numbers. This reflects a property of the Pauli operators mentioned earlier.

The above definition provides 2^N+1 distinct sets (indexed by A), each set containing 2^N-1 operators (fixed A and running index $a=1,\ldots,2^N-1$), after discarding the identity. Each of these operators has the spectrum ± 1 and is traceless, by construction. To show that they are unitarily equivalent to the Pauli operators, we need only demonstrate that they form an orthonormal set. For the case $A\neq B$,

$$\mathrm{Tr}(O^A_aO^B_b)=\sum_{\alpha,\beta}\varepsilon_{a\alpha}\varepsilon_{b\beta}\,\mathrm{Tr}(P^A_\alpha P^B_\beta)=0, \tag{9}$$

where Eq. (7) and the property $\Sigma_\alpha\varepsilon_{a\alpha}=0$ were used; then for the case $A=B$, using Eqs. (6) and (2),

$$\mathrm{Tr}(O^A_aO^A_b)=\sum_{\alpha,\beta}\varepsilon_{a\alpha}\varepsilon_{b\beta}\,\mathrm{Tr}(P^A_\alpha P^A_\beta)=\sum_{\alpha}\varepsilon_{a\alpha}\varepsilon_{b\alpha}=2^N\delta_{ab}. \tag{10}$$

Finally, this orthonormal set of 4^N-1 traceless operators is completed by adding the identity, so indeed they have a representation in the form given by Eq. (4). This shows that the Pauli operators may be partitioned accordingly.

We now show the second part, namely, that *any* such partitioning of Pauli operators defines a unique choice of unbiased basis sets. Assuming such a partitioning, each subset (A) of Pauli operators $\{O^A_1,O^A_2,\ldots,O^A_{2^N-1}\}$ defines a unique basis of 2^N joint eigenstates $|A,\alpha\rangle$, $\alpha=1,\ldots 2^N$. Thus, each O^A_a operator may be expanded as in Eq. (8), with $\varepsilon_{a\alpha}$ now defined as the eigenvalue of O^A_a on the state $|A,\alpha\rangle$, the lower index taking the values $a=1,\ldots,2^N-1$. The known spectrum of the O^A_a's dictates that each row of the $\varepsilon_{a\alpha}$ matrix must consist of an equal number of $+1$'s and -1's, and the identity $\mathrm{Tr}\,O^A_aO^A_b=2^N\delta_{ab}$ shows (note Eq. 10) that any two rows a and b are orthogonal. Thus, by appending an additional row ($a=2^N$) to the $\varepsilon_{a\alpha}$ matrix, we recover its previ-

ous form. The scaled matrix $\varepsilon_{a\alpha}/\sqrt{2^N}$ is orthogonal, and, therefore, we may invert Eq. (8) to yield the projection operators

$$P_\alpha^A = 2^{-N}\sum_a \varepsilon_{\alpha a} O_a^A = 2^{-N}\left(\mathcal{I} + \sum_a{}' \varepsilon_{\alpha a} O_a^A\right). \qquad (11)$$

In the second equality we write the identity contribution explicitly and delete the $a=2^N$ term from the sum, as denoted by the prime.

We may now show that all of the basis sets are mutually unbiased: Substituting Eq. (11) into Eq. (7) yields

$$\mathrm{Tr}(P_\alpha^A P_\beta^B) = 2^{-N} + 4^{-N}\sum_a{}' \sum_b{}' \varepsilon_{\alpha a}\varepsilon_{\beta b}\,\mathrm{Tr}(O_a^A O_b^B), \qquad (12)$$

since terms linear in O_a^A have vanishing trace. It follows immediately that if A and B refer to different basis sets, then Eq. (7) is satisfied. If $A=B$, then only the $a=b$ term in the sum survives and

$$\mathrm{Tr}(P_\alpha^A P_\beta^A) = 2^{-N}\left(1 + \sum_a{}' \varepsilon_{\alpha a}\varepsilon_{\beta a}\right) = 2^{-N}\sum_a \varepsilon_{\alpha a}\varepsilon_{\beta a} = \delta_{\alpha\beta}, \qquad (13)$$

where the orthogonality of $\varepsilon_{a\alpha}/\sqrt{2^N}$ was used. This establishes that the 2^N-1 basis sets generated (uniquely) by the commuting subsets of Pauli operators are in fact unbiased. So there is a one-to-one correspondence between partitionings of Pauli operators and choices of unbiased basis sets.

III. EXAMPLES FOR TWO AND THREE QUBITS

We now illustrate this correspondence for systems of two and three qubits. To develop notation, the operator subsets for the *one* qubit case consist of single elements, σ_x, σ_y, and σ_z. Corresponding basis sets are denoted by (x), (y), and (z), where each basis set consists of the two states "up" and "down" along the indicated axis. The individual basis states are denoted by $|n_x\rangle$, $|n_y\rangle$, and $|n_z\rangle$, where $n_x=1$ or 0 for spin "up" and "down," respectively. The inner products between any two states appearing in these basis sets obey Eqs. (1) and (2). Obviously, measurements by any of the above operators on an eigenstate of any other will produce perfectly random results (i.e., an average spin projection of zero).

1	$(zz)_\pi$	σ_z^1	σ_z^2	$\sigma_z^1\sigma_z^2$
2	$(xy)_\pi$	σ_x^1	σ_y^2	$\sigma_x^1\sigma_y^2$
3	$(yx)_\pi$	σ_y^1	σ_x^2	$\sigma_y^1\sigma_x^2$
4	$(zx)_B$	$\sigma_y^1\sigma_y^2$	$\sigma_z^1\sigma_x^2$	$\sigma_x^1\sigma_z^2$
5	$(yz)_{Bi}$	$\sigma_x^1\sigma_x^2$	$\sigma_y^1\sigma_z^2$	$\sigma_z^1\sigma_y^2$

FIG. 1. Five unbiased bases sets and corresponding Pauli operator sets. Each operator set consists of three commuting members, any two of which determine the corresponding basis set as their joint eigenbasis.

In the case of two qubits, the dimension of the Hilbert space is $d=4$, so that five unbiased basis sets exist. Fig. 1 shows these together with the five corresponding operator sets, each consisting of three compatible operators. Subscripts indicate three product bases, $(zz)_\pi$, $(xy)_\pi$, and $(yx)_\pi$, whose individual states are denoted in the $(\mathrm{zz})_\pi$ case, for example, by $|n_z^1, n_z^2\rangle$. There are two Bell bases, $(zx)_B$ and $(yz)_{Bi}$, and the states belonging to each of these may be written, respectively, as

$$|n_z^1, n_x^2; \pm\rangle = \frac{1}{\sqrt{2}}(|n_z^1, n_x^2\rangle \pm |\overline{n_z^1}, \overline{n_x^2}\rangle), \qquad (14)$$

$$|n_y^1, n_z^2; \pm i\rangle = \frac{1}{\sqrt{2}}(|n_y^1, n_z^2\rangle \pm i|\overline{n_y^1}, \overline{n_z^2}\rangle), \qquad (15)$$

where bars denote spin flips; ie, if $n_x=1$ or 0, then $\overline{n_x}=0$ or 1, respectively. Thus, the four individual basis states are explicitly enumerated [in Eq. (15), for example] by $|1_y, 1_z; \pm i\rangle$ and $|1_y, 0_z; \pm i\rangle$. The factor of i [as denoted by the subscript in the basis label $(yz)_{Bi}$] is not arbitrary; its presence is dictated by the operators that define the basis, or equivalently by the requirement that the two Bell bases be mutually unbiased. It is a property of Bell bases that they can

1	$(xyz)_\pi$	σ_x^1	σ_y^2	σ_z^3	$\sigma_x^1\sigma_y^2\sigma_z^3$	$\sigma_x^1\sigma_y^2$	$\sigma_x^1\sigma_z^3$	$\sigma_y^2\sigma_z^3$
2	$(yzx)_\pi$	σ_y^1	σ_z^2	σ_x^3	$\sigma_y^1\sigma_z^2\sigma_x^3$	$\sigma_y^1\sigma_z^2$	$\sigma_y^1\sigma_x^3$	$\sigma_z^2\sigma_x^3$
3	$(zxy)_\pi$	σ_z^1	σ_x^2	σ_y^3	$\sigma_z^1\sigma_x^2\sigma_y^3$	$\sigma_z^1\sigma_x^2$	$\sigma_z^1\sigma_y^3$	$\sigma_x^2\sigma_y^3$
4	$(xxx)_{Gi}$	$\sigma_y^1\sigma_z^2\sigma_z^3$	$\sigma_z^1\sigma_y^2\sigma_z^3$	$\sigma_z^1\sigma_z^2\sigma_y^3$	$\sigma_y^1\sigma_y^2\sigma_y^3$	$\sigma_x^1\sigma_x^2$	$\sigma_x^1\sigma_x^3$	$\sigma_x^2\sigma_x^3$
5	$(yyy)_G$	$\sigma_z^1\sigma_x^2\sigma_x^3$	$\sigma_x^1\sigma_z^2\sigma_x^3$	$\sigma_x^1\sigma_x^2\sigma_z^3$	$\sigma_z^1\sigma_z^2\sigma_z^3$	$\sigma_y^1\sigma_y^2$	$\sigma_y^1\sigma_y^3$	$\sigma_y^2\sigma_y^3$
6	$(zzz)_G$	$\sigma_x^1\sigma_y^2\sigma_y^3$	$\sigma_y^1\sigma_x^2\sigma_y^3$	$\sigma_y^1\sigma_y^2\sigma_x^3$	$\sigma_x^1\sigma_x^2\sigma_x^3$	$\sigma_z^1\sigma_z^2$	$\sigma_z^1\sigma_z^3$	$\sigma_z^2\sigma_z^3$
7	$(xzy)_G$	$\sigma_z^1\sigma_x^2\sigma_z^3$	$\sigma_y^1\sigma_x^2\sigma_x^3$	$\sigma_y^1\sigma_y^2\sigma_z^3$	$\sigma_z^1\sigma_y^2\sigma_x^3$	$\sigma_x^1\sigma_z^2$	$\sigma_x^1\sigma_y^3$	$\sigma_z^2\sigma_y^3$
8	$(yxz)_G$	$\sigma_x^1\sigma_y^2\sigma_x^3$	$\sigma_z^1\sigma_y^2\sigma_y^3$	$\sigma_z^1\sigma_z^2\sigma_x^3$	$\sigma_x^1\sigma_z^2\sigma_y^3$	$\sigma_y^1\sigma_x^2$	$\sigma_y^1\sigma_z^3$	$\sigma_x^2\sigma_z^3$
9	$(zyx)_G$	$\sigma_y^1\sigma_z^2\sigma_y^3$	$\sigma_x^1\sigma_z^2\sigma_z^3$	$\sigma_x^1\sigma_x^2\sigma_y^3$	$\sigma_y^1\sigma_x^2\sigma_z^3$	$\sigma_z^1\sigma_y^2$	$\sigma_z^1\sigma_x^3$	$\sigma_y^2\sigma_x^3$

FIG. 2. Listing of nine unbiased basis sets and corresponding operator sets, each consisting of 7 commuting members. Particular subsets of three determine the corresponding basis sets completely.

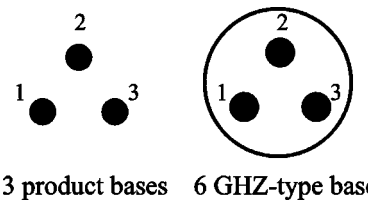

FIG. 3. Schematic of unbiased basis sets listed in Fig. 2—three product and six GHZ bases. The three particles in the circle are maximally entangled (in a GHZ state).

appear equally simple if other quantization axes are chosen in appropriate combinations. For example, the Bell bases 4 and 5 in Fig. 1 may be written as $(yy)_B$ and $(xx)_B$, respectively. While these are simply different ways of writing the same basis sets, truely different alternatives involving all five-basis sets exist for two qubits (see Refs. [11] and [12]). These alternatives also consist of three product bases and two Bell bases.

The three-qubit Hilbert space has $d=8$, and thus nine unbiased basis sets. One choice contains three product bases, $(xyz)_\pi$, $(yzx)_\pi$, and $(zxy)_\pi$; and six bases consisting of maximally entangled states, $(xxx)_{Gi}$, $(yyy)_G$, $(zzz)_G$, $(xzy)_G$, $(yxz)_G$, and $(zyx)_G$. The nine basis sets are listed in Fig. 2 and represented graphically in Fig. 3. The entangled basis sets are labeled by coordinate axes in which the states reduce to the familiar Greenberger-Horne-Zeilinger [13] (GHZ) form. For example, all of the states belonging to the basis set $(zyx)_G$ may be written as

$$|n_z^1,n_y^2,n_x^3;\pm\rangle=\frac{1}{\sqrt{2}}(|n_z^1,n_y^2,n_x^3\rangle\pm|\overline{n_z^1},\overline{n_y^2},\overline{n_x^3}\rangle); \quad (16)$$

these would require more complicated expressions if referred to other coordinate axes. Fig. 2 lists the seven-member operator sets that correspond uniquely to each basis set. As in the two-qubit case, the operators involving only a single Pauli matrix are exhausted within the product basis sets.

It is striking that in the progression from one to two to three qubits, the number of totally entangled bases can grow from none to two to six, while the number of product bases remains fixed at three. It is easy to convince onesself that the maximum number of product bases remains fixed at three for all numbers N of qubits.

To show that the structure is more flexible with three qubits than with two, we describe now a different choice of unbiased basis sets for three qubits, one that cannot be obtained from the previous choice by local unitary transformations. In this choice (Fig. 4), there are no product states, and no states with three-particle entanglement. Every basis consists of states that are products of one-particle states with Bell states; one particle is unentangled while the other two are totally entangled, as depicted in Fig. 5. The basis sets form groupings of three: $(x^1)(yz)_{Bi}$, $(y^1)(zx)_B$, $(z^1)(xy)_B$, then $(x^2)(xy)_B$, $(y^2)(yz)_{Bi}$, $(z^2)(zx)_B$, and finally $(x^3)(zx)_B$, $(y^3)(xy)_B$, $(z^3)(yz)_{Bi}$, in which a different particle is factored out within each group. Coordinate axes are permuted within each group, but not from group to group. Factors of i appear once within each group.

Note that within each grouping, we find *three* unbiased Bell-type bases—a feature that was not seen in the two-qubit system. Indeed, if one were to begin with three unbiased Bell bases in a two-qubit system, one could then *not* find two additional basis sets. This can be understood in terms of the operator decomposition: The nine operators exhausted by three Bell bases do not leave six operators that are decomposable into two commuting subsets.

We also note that the choices of unbiased basis sets given for the three qubit case are not obtained from the algorithmic construction given in Ref. [6]. Wootters has pointed out [14] that this construction produces another choice which consists of two product, four GHZ, and three ''product-Bell'' bases. In the case of two qubits, not surprisingly, the same construction produces three product and two Bell bases [14].

IV. CONCLUSIONS

The two- and three-qubit cases illustrate general points made at the beginning. First, with regard to state preparation, one can see that N observables suffice to define any of the listed basis states completely, representing these states as binary numbers. In the two-qubit case, any two of the three compatible observables within a subset may be chosen. In the three-qubit case, there are many choices of three observables that suffice [15]—for example, the first three listed

1	$(x^1)(yz)_{Bi}$	σ_x^1	$\sigma_x^2\sigma_x^3$	$\sigma_y^2\sigma_z^3$	$\sigma_z^2\sigma_y^3$	$\sigma_x^1\sigma_x^2\sigma_x^3$	$\sigma_x^1\sigma_y^2\sigma_z^3$	$\sigma_x^1\sigma_z^2\sigma_y^3$
2	$(y^1)(zx)_B$	σ_y^1	$\sigma_y^2\sigma_y^3$	$\sigma_z^2\sigma_x^3$	$\sigma_x^2\sigma_z^3$	$\sigma_y^1\sigma_y^2\sigma_y^3$	$\sigma_y^1\sigma_z^2\sigma_x^3$	$\sigma_y^1\sigma_x^2\sigma_z^3$
3	$(z^1)(xy)_B$	σ_z^1	$\sigma_z^2\sigma_z^3$	$\sigma_x^2\sigma_y^3$	$\sigma_y^2\sigma_x^3$	$\sigma_z^1\sigma_z^2\sigma_z^3$	$\sigma_z^1\sigma_x^2\sigma_y^3$	$\sigma_z^1\sigma_y^2\sigma_x^3$
4	$(x^2)(xy)_B$	σ_x^2	$\sigma_z^1\sigma_z^3$	$\sigma_x^1\sigma_y^3$	$\sigma_y^1\sigma_x^3$	$\sigma_z^1\sigma_x^2\sigma_z^3$	$\sigma_x^1\sigma_x^2\sigma_y^3$	$\sigma_y^1\sigma_x^2\sigma_x^3$
5	$(y^2)(yz)_{Bi}$	σ_y^2	$\sigma_x^1\sigma_x^3$	$\sigma_y^1\sigma_z^3$	$\sigma_z^1\sigma_y^3$	$\sigma_x^1\sigma_y^2\sigma_x^3$	$\sigma_y^1\sigma_y^2\sigma_z^3$	$\sigma_z^1\sigma_y^2\sigma_y^3$
6	$(z^2)(zx)_B$	σ_z^2	$\sigma_y^1\sigma_y^3$	$\sigma_z^1\sigma_x^3$	$\sigma_x^1\sigma_z^3$	$\sigma_y^1\sigma_z^2\sigma_y^3$	$\sigma_z^1\sigma_z^2\sigma_x^3$	$\sigma_x^1\sigma_z^2\sigma_z^3$
7	$(x^3)(zx)_B$	σ_x^3	$\sigma_y^1\sigma_y^2$	$\sigma_z^1\sigma_x^2$	$\sigma_x^1\sigma_z^2$	$\sigma_y^1\sigma_y^2\sigma_x^3$	$\sigma_z^1\sigma_x^2\sigma_x^3$	$\sigma_x^1\sigma_z^2\sigma_x^3$
8	$(y^3)(xy)_B$	σ_y^3	$\sigma_z^1\sigma_z^2$	$\sigma_x^1\sigma_y^2$	$\sigma_y^1\sigma_x^2$	$\sigma_z^1\sigma_z^2\sigma_y^3$	$\sigma_x^1\sigma_y^2\sigma_y^3$	$\sigma_y^1\sigma_x^2\sigma_y^3$
9	$(z^3)(yz)_{Bi}$	σ_z^3	$\sigma_x^1\sigma_x^2$	$\sigma_y^1\sigma_z^2$	$\sigma_z^1\sigma_y^2$	$\sigma_x^1\sigma_x^2\sigma_z^3$	$\sigma_y^1\sigma_z^2\sigma_z^3$	$\sigma_z^1\sigma_y^2\sigma_z^3$

FIG. 4. Same structure as in Fig. 3, but all bases are partially entangled. In each of three groups a different particle must be singled out as unentangled.

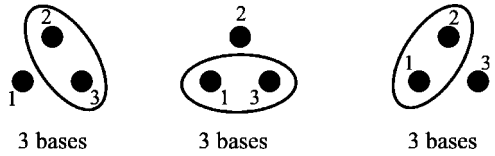

FIG. 5. Schematic of unbiased basis sets listed in Fig. 4, all partially entangled. One particle is unentangled with the other two, which are totally entangled in Bell states.

within each subset. In the N-qubit case, we introduced an $\varepsilon_{a\alpha}$ matrix in which an appropriate choice of N rows (representing N operators) describe all 2^N basis states as binary nunbers.

Second, with regard to the determination of a general, possibly mixed state, recall that 4^N-1 real parameters (15 for two qubits and 63 for three qubits) are required to specify the N-qubit density matrix completely [4,5]. And exactly this number is provided, either by the expectation values of the operators themselves, or by all the independent probabilities associated with the unbiased basis states. As we have proven for the general case, the 4^N-1 Pauli operators can be partitioned into 2^N+1 subsets, each consisting of 2^N-1 internally commuting observables. The set of all such partitionings has a one-to-one correspondence with choices of 2^N+1 unbiased basis sets in the N-qubit Hilbert space. There are many such choices, and for $N>2$ the entanglement may be distributed over basis sets in many different ways. The maximum number of product bases is fixed at three for any N.

The correspondence between basis sets and observables makes it possible to regard all Pauli operator subsets within a given partitioning as being mutually unbiased: If the system is prepared in a joint eigenstate of one observable set, then it has a uniform probability distribution over the joint eigenstates of any other observable set in the partitioning. As a result, all observables outside the original maximal commuting subset yield minimal information—measurement outcomes are uniformly distributed over all possibilities.

The concept of unbiasedness between observable sets extends the idea of complementarity of two individual observables that fail to commute. Clearly two such observables must always belong to different mutually unbiased subsets within any partitioning. However, as the two-and three-qubit examples show, two commuting observables may belong to the same or to different unbiased subsets. Their compatibility is dependent upon the partitioning.

Note added. After this work was completed, an e-print [12] appeared reporting work which is related to this work, but complementary in several respects. Ref. [12] obtained a general relationship between complete bases of unitary operators (belonging to the general Pauli group) and unbiased basis sets, for any power-of-prime dimension. In this paper, we considered the many-qubit case. We expanded upon the physical interpretation of the concept of complementarity. We showed that many alternative partionings are possible and, most importantly, entanglement is distributed among unbiased basis sets in a partition-dependent manner for $N>2$.

ACKNOWLEDGMENTS

We would like to thank W. K. Wootters for insightful and informative discussions. Č.B. has been supported by the Austrian Science Foundation (FWF), Project No. F1506, and by the QIPC Program of the European Union. J.L. thanks the Erwin Schrödinger Institute for its hospitality during the period when this work was carried out.

[1] A. Zeilinger, Found. Phys. **29**, 631 (1999).
[2] Č. Brukner and A. Zeilinger, Phys. Rev. Lett. **83**, 3354 (1999); Phys. Rev. A **63**, 022113 (2001).
[3] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press 2000), p. 454.
[4] W.K. Wootters, Found. Phys. **16**, 391 (1986).
[5] I. Ivanovič, J. Phys. A **14**, 3241 (1981).
[6] W.K. Wootters and B.D. Fields, Ann. Phys. **191**, 363 (1989); and in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic Publishers, Dordrecht, 1989), pp. 65–67.
[7] L. Vaidman, Y. Aharonov, and D.Z. Albert, Phys. Rev. Lett. **58**, 1385 (1987); Y. Aharonov and B.-G. Englert, Z. Naturforsch A **56**, 16 (2001); B-G. Englert and Y. Aharonov, Phys. Lett. A **284**, 1 (2001).
[8] C.H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore* (IEEE, New York, 1984) p. 175; A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[9] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000); H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000); M. Bourennane, A. Karlsson, and G. Björk, Phys. Rev. A **64**, 012306 (2001); D. Bruss and C. Macchiavello, J. Phys. A **34**, 6815 (2001).
[10] This is the usual definition of the orthonormality of operators except for the factor of 2^N in Eq. (5). This factor allows us to retain the usual definition of the Pauli operators.
[11] Č. Brukner and A. Zeilinger, J. Mod. Opt. **47**, 2233 (2000).
[12] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, and F. Vatan, e-print quant-ph/0103162.
[13] D.M. Greenberger, M. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
[14] W.K. Wootters (private communication).
[15] Any three of these operators that do not form a subgroup determine the basis set completely.