7-2-2004

# Mutually Unbiased Bases and Trinary Operator Sets for N Qutrits

Jay Lawrence
*Dartmouth College*

# Mutually unbiased bases and trinary operator sets for *N* qutrits

Jay Lawrence
*Department of Physics and Astronomy, Dartmouth College, Hanover, New Hampshire 03755, USA*
(Received 13 March 2004; published 2 July 2004)

A compete orthonormal basis of *N*-qutrit unitary operators drawn from the Pauli group consists of the identity and $9^N-1$ traceless operators. The traceless ones partition into $3^N+1$ maximally commuting subsets (MCS's) of $3^N-1$ operators each, whose joint eigenbases are mutually unbiased. We prove that Pauli factor groups of order $3^N$ are isomorphic to all MCS's and show how this result applies in specific cases. For two qutrits, the 80 traceless operators partition into 10 MCS's. We prove that 4 of the corresponding basis sets *must* be separable, while 6 must be totally entangled (and Bell-like). For three qutrits, 728 operators partition into 28 MCS's with less rigid structure, allowing for the coexistence of separable, partially entangled, and totally entangled (GHZ-like) bases. However a *minimum* of 16 GHZ-like bases must occur. Every basis state is described by an *N*-digit trinary number consisting of the eigenvalues of *N* observables constructed from the corresponding MCS.

DOI: 10.1103/PhysRevA.70.012302 PACS number(s): 03.67.−a, 03.65.Ud, 03.65.Wj

## I. INTRODUCTION

Systems of three-state particles (qutrits) have been much under discussion recently because they expand the potential for quantum information processing and they have been realized and controlled experimentally. Specific realizations for use in quantum communication protocols include biphotons [1,2], time-bin entangled photons [3], and photons with orbital angular momentum [4]. Qutrit quantum computation with trapped ions has been described theoretically [5], while one-qutrit gates have been demonstrated experimentally with deuterons [6]. Specific advantages of qutrits over qubits include more secure key distributions [7–9], the solution of the Byzantine agreement problem [10], and quantum coin flipping [11].

In this paper we describe the general framework for quantum tomography of *N*-qutrit states provided by mutually unbiased basis sets [12] and the special operators (or measurements) associated with them. As *N* increases, these operators retain their fundamental trinary character (having three distinct eigenvalues), unlike the more familiar operators of compound angular momentum, for example. This means that the quantum numbers specifying the *N*-qutrit basis states are *N*-digit trinary numbers: For separable states, each digit corresponds to a statement about a single qutrit. For totally entangled states in which the entanglement is shared among all qutrits, every statement refers to a joint property of two or more (perhaps all) qutrits; no statement refers to a single qutrit. Such descriptions parallel those introduced recently for *N*-qubit systems [13,14]. In this case, the descriptions rely on the existence of *N* commuting trinary operators. If these are Hermitian, they comprise a "complete set of commuting observables" in the familiar sense [15] that they define a basis in the Hilbert space of pure states, whose dimension is $3^N$.

But the density matrix $\rho$ describing mixed states resides in a vector space of dimension $9^N$, together with all other operators on the state space. This *operator* space is spanned by a complete and orthonormal set of operators [orthonormal in the sense $\mathrm{Tr}(O_i^\dagger O_j)\sim\delta_{ij}$]. Appropriate trinary operator "basis sets" are easily constructed as tensor products of unitary one-qutrit operators [16,17]. This set of $9^N$ operators partitions into $3^N+1$ maximally commuting subsets (MCS's) of $3^N-1$ operators each [17], expending all operators in the basis apart from the identity. Each of these MCS's contains a smaller subset of *N* operators that provide the trinary labels for the corresponding basis states. The $3^N+1$ distinct basis sets thus defined are *mutually unbiased* [17]; i.e., the inner product between any two states belonging to *different* ones has the common magnitude, $3^{-N/2}$. Since measurements within each basis set provide $3^N-1$ independent probabilities, the $3^N+1$ basis sets together provide $9^N-1$. This number is just sufficient to determine the density matrix (with $\mathrm{Tr}\rho=1$).

The partitioning structure described above is guaranteed because 3 is a prime number: Reference [12] proved that if the dimension ($d$) of a Hilbert space is equal to a power of a prime number (like $3^N$), then a full complement of $d+1$ mutually unbiased basis sets (MUB's) exists. The number $d+1$ is necessary and sufficient to determine a mixed state $\rho$ with maximum efficiency [12]. Reference [17] proved that $d+1$ MUB's exist if and only if a partitioning, complete, and orthonormal operator set exists and showed how to construct such operator sets from Pauli operators. These operators identify the measurements associated with each MUB. It is worth mentioning that while MUB's are desirable for quantum tomography generally, they have proven instrumental in certain proposed quantum key distributions [18] and in the solution of the mean king's problem for prime power dimensions [19]. The last example is a problem in quantum state determination in which both the choice of a measurement (the basis set), and its outcome (the state within the basis), are to be determined.

It should be noted in this connection that the partitioning property of an operator set is not guaranteed by completeness and orthonormality. A good counterexample in the one-qutrit case is the conventional set of generators of SU(3), $\lambda_1,\ldots,\lambda_8$ [20]. This set *is* orthonormal ($\mathrm{Tr}\lambda_i\lambda_j=2\delta_{ij}$) and complete (with the inclusion of the identity), but it does *not* partition into four subsets of two commuting operators each.

 

So the $\lambda_j$ operators provide a basis for quantum tomography [21], but not one associated with mutually unbiased basis sets. In Sec. II we shall construct Hermitian operator basis sets that have two desirable properties: They partition so as to define MUB's, and they generate SU(3) [or SU($3^N$) in the general case].

We are interested here in the discrete group properties of the unitary basis operators themselves. The $N$ operators that define basis states also generate, by multiplication, all remaining operators in the MCS, plus the identity, thus forming a group of order $3^N$. The full operator basis consisting of all MCS's plus the identity (one copy), totaling $9^N$ operators, does *not* form a group, but only because multiplication between operators from different MCS's generates one of the three phase factors, $\exp(2n\pi i/3)$. Thus, a group of order $3\times 9^N$ (which we shall call the Pauli group of $N$ qutrits) consists of the operator basis *in triplicate*—i.e., each operator multiplied by each phase factor [16]. Its factor groups relate closely to the partitioning structure. Those of order $3^N$ are most useful because they are isomorphic to all of the MCS groups.

In the next three sections we discuss the one-, two-, and three-qutrit cases to illustrate the general principles outlined above and also to highlight special properties that emerge in each case. The one-qutrit section describes the Pauli group and illustrates its connection with the (unique) partitioning of the eight-operator basis set. The two-qutrit section describes the mutually unbiased bases sets, separable and totally entangled, and the corresponding operator sets. While many partitions exist, we prove that their *structure* is unique. The three-qutrit section describes three types of mutually unbiased basis sets. We derive the allowed partitioning structures and the coexistence conditions for the three types. The concluding section summarizes the results and interprets the trinary descriptions of separable and entangled states in terms of complementarity between individual and joint properties of many-particle systems. Two brief appendixes supply background material for reference as desired while reading the text. Appendix A reviews the connection between mutually unbiased bases and the partitioning of an operator set. Appendix B proves a theorem that describes the general relationship between such operator partitionings and Pauli factor groups.

## II. ONE QUTRIT

For comparison, recall briefly the Pauli operators for a single *qubit*, written in outer product notation [22] as

$$Z = |n\rangle(-1)^n\langle n|,$$

$$X = |n+1\rangle\langle n|,$$

$$Y \equiv XZ = |n+1\rangle\langle(-1)^n\langle n|, \tag{1}$$

where summation is implied over the values $n=0$, 1 (for spin up and down along $z$), and addition is modulo 2 so that the second equation, for example, reads $X=|1\rangle\langle 0|+|0\rangle\langle 1|$. The four operators $I$, $X$, $Y$, and $Z$ form a complete orthonormal set of operators on the one-qubit Hilbert space. The eigenbases of $X$, $Y$, and $Z$ are mutually unbiased: An eigenstate of $Z$ has equal probabilities of being found in any eigenstate of $X$ or $Y$. The eight operators $\pm Z$, $\pm X$, $\pm Y$, and $\pm I$ form the Pauli group [16] of a qubit. A larger Pauli group is sometimes defined as well [23], one which includes the Hermitian counterpart $iY$ ($Z$ and $X$ being Hermitian as they stand). This group consists of 16 elements $(\pm Z, \pm iZ, \ldots)$. The more exclusive former definition conforms to the general one that applies to qutrits.

While the operators defined above are all square roots of the identity $I$ $(2\times 2)$, the corresponding operators for the qutrit case are all cube roots of $I$ $(3\times 3)$, We may write the complete orthonormal set as $I$, $V$, $X$, $Y$, $Z$, $V^2$, $X^2$, $Y^2$, and $Z^2$, since each element has a square, which is also its inverse. We may define in analogy with the above, following Refs. [16,17,22],

$$Z = |n\rangle\omega^n\langle n|,$$

$$X = |n+1\rangle\langle n|,$$

$$Y \equiv XZ = |n+1\rangle\omega^n\langle n|,$$

$$V \equiv XZ^2 = |n+1\rangle\omega^{2n}\langle n|, \tag{2}$$

where summation is implied over the values $n=0$, 1, 2 (corresponding to spin projections 0, +1, −1 respectively), addition is modulo 3, and

$$\omega = \exp(2\pi i/3). \tag{3}$$

Each of the four operators in Eq. (2) defines, as its eigenbasis, one of the four required mutually unbiased basis sets [24], and each operator, together with its square, forms a MCS.

To facilitate writing the multiplication rules among these operators, we introduce a concise notation reflecting their actions upon the eigenstates of $Z$ (the standard basis): "diagonal" $(I, Z, Z^2)$, "right cyclic"$(X, Y, V)$, and "left cyclic" $(X^2, Y^2, V^2)$. Then, letting the index $l=0$, 1, 2 denote the operator within each grouping,

$$E_l = Z^l = |n\rangle\omega^{nl}\langle n|,$$

$$R_l = XZ^l = |n+1\rangle\omega^{nl}\langle n|,$$

$$L_l = R_l^\dagger = |n\rangle\omega^{-nl}\langle n+1|. \tag{4}$$

One can also think loosely of $R_l$ as "raising" and $L_l$ as "lowering" operators with respect to the standard basis, but the "cyclic" designations are more descriptive [25]: $R_l$ and $L_l$ are norm preserving, whereas the usual angular momentum raising and lowering operators annihilate the uppermost and lowermost rungs of the ladder, respectively. The multiplication rules may be constructed immediately. For conciseness, nine expressions are condensed into six by writing the last six in the form of commutators:

$$E_l E_m = E_{l+m},$$

$$R_l R_m = \omega^{m-l} L_{-l-m},$$

$$L_l L_m = \omega^{m-l} R_{-l-m},$$

$$[R_l, E_m] = (1-\omega^m) R_{l+m},$$

$$[L_l, E_m] = (\omega^m - 1) L_{l-m},$$

$$[R_l, L_m] = (\omega^{m-l} - 1) E_{l-m}. \tag{5}$$

It is apparent from this multiplication table that every one of the eight operators, $Z, \ldots, V^2$, commutes only with itself, its square, and the identity. Consider for example $R_l$: It commutes with $R_m$ only if $m=l$, with $L_m$ only if $m=l$ (since $L_m$ is then its square), and with $E_m$ only if $m=0$. It is also apparent that the *lack* of commutativity resides entirely in the phase factors.

These phase factors spoil the property of closure under multiplication and prevent these nine operators, by themselves, from forming a group. But, as mentioned, a group of order 27 (the Pauli group of a qutrit) *is* formed by taking the nine basis operators *in triplicate*—i.e., each operator multiplied by 1, $\omega$, and $\omega^2$.

This Pauli group has a trivial factor group of order 9, whose elements consist of the triples $\mathcal{I}=(I, \omega I, \omega^2 I)$, $\mathcal{Z}=(Z, \omega Z, \omega^2 Z), \ldots$, $\mathcal{V}^2=(V^2, \omega V^2, \omega^2 V^2)$. The multiplication $\mathcal{Z}\mathcal{X}=\mathcal{Y}$ means that the product of any element of $\mathcal{Z}$ with any element of $\mathcal{X}$ is equal to some element of $\mathcal{Y}$. This group is Abelian because no factors of $\omega^n$ appear in its multiplication table.

Factor groups of order 3 are more interesting. One example is apparent from Eqs. (5). The factor group elements, each consisting of nine Pauli group elements, may be denoted by

$$\mathcal{E} = \omega^n E_l = (\mathcal{I}, \mathcal{Z}, \mathcal{Z}^2),$$

$$\mathcal{R} = \omega^n R_l = (\mathcal{X}, \mathcal{Y}, \mathcal{V}),$$

$$\mathcal{L} = \omega^n L_l = (\mathcal{X}^2, \mathcal{Y}^2, \mathcal{V}^2), \tag{6}$$

where $n=0$, 1, 2 and $l=0$, 1, 2. The multiplication table consists of

$$\mathcal{R}^2 = \mathcal{L}, \quad \mathcal{L}^2 = \mathcal{R}, \quad \mathcal{R}\mathcal{L} = \mathcal{L}\mathcal{R} = \mathcal{E}, \tag{7}$$

and obvious equalities involving $\mathcal{E}$. This group is, of course, isomorphic to the group $(1, \omega, \omega^2)$. Equations (6) provide a useful summary of the relationship between the 27 Pauli group elements, the factor group of order 9, and the factor group of order 3.

There is a useful relationship between the last factor group and the partitioning structure. Any of the four MCS's may be combined with the identity to form a subgroup of the Pauli group. In Table I, we pick $(I, Z, Z^2)$. We define this, in triplicate, as the identity element $\mathcal{E}=(\mathcal{I}, \mathcal{Z}, \mathcal{Z}^2)$ of the factor group. The columns below (in triplicate) form the elements $\mathcal{R}$ and $\mathcal{L}$.

The first entry in each column generates all remaining entries by multiplication with elements of $\mathcal{E}$—i.e., $X\mathcal{E}=\mathcal{R}$ and $X^2\mathcal{E}=\mathcal{L}$. There are four such factorizations corresponding to the four choices of $\mathcal{E}$. A second example is

TABLE I. The partitioning of 8 one-qutrit operators into 4 maximally commuting subsets. If all entries are multiplied by 1, $\omega$, and $\omega^2$, then the top line, including $I$, forms the identity element $\mathcal{E}$ of the factor group [Eq. (6)], while the first and second columns (below the line) form the $\mathcal{R}$ and $\mathcal{L}$ elements, respectively.

| $I$ | $Z$ | $Z^2$ |
|---|---|---|
| | $X$ | $X^2$ |
| | $Y$ | $Y^2$ |
| | $V$ | $V^2$ |
| $\mathcal{E}$ | $\mathcal{R}$ | $\mathcal{L}$ |

$$\mathcal{E} = (\mathcal{I}, \mathcal{X}, \mathcal{X}^2),$$

$$\mathcal{R} = (\mathcal{V}, \mathcal{Y}^2, \mathcal{Z}^2),$$

$$\mathcal{L} = (\mathcal{V}^2, \mathcal{Y}, \mathcal{Z}). \tag{8}$$

Table I and its four variations illustrate that (i) these factor groups are isomorphic to all of the subgroups formed by the MCS's and (ii) every factor group element (apart from the identity) contains one and only one operator from every remaining MCS. We prove these two points in Appendix B for the general case of $N$ qutrits and apply them in later sections.

It is instructive to compare the order-3 qutrit factor groups with their qubit counterparts, which are of order 2. The identity element in the qubit case could be $\mathcal{E}=(\pm I, \pm Z)$, with the other element (the "flip" element, say) being $\mathcal{F}=(\pm X, \pm Y)$. Permutations of $X$, $Y$, and $Z$ produce the other factor groups of order 2.

Let us turn finally to the observables. Since the eight unitary operators $U=Z, \ldots, V$ and $U^\dagger=Z^2, \ldots, V^2$ form (together with the identity) a complete orthonormal set, we can immediately construct an alternative Hermitian basis through the transformation

$$H = (U - U^\dagger)/i\sqrt{3}, \tag{9}$$

$$\overline{H} = (U + U^\dagger)/\sqrt{3}. \tag{10}$$

The four operators of type $H$ have the trinary spectrum $(0, \pm 1)$, and the four others $\overline{H}$ have the spectrum $(2, -1, -1)/\sqrt{3}$. The relationship between each $H$ and its compatible partner $\overline{H}$ is

$$\overline{H} = (2I - 3H^2)/\sqrt{3}. \tag{11}$$

The orthonormality relation among all eight is

$$\mathrm{Tr}(H_i H_j) = 2\delta_{ij}, \tag{12}$$

where indices run from 1,…8, with (say) odd values corresponding to $H$ and even to $\overline{H}$. The properties of orthonormality and tracelessness in fact require that compatible *Hermitian* partners have different spectra. One can then see that the standard generators $\lambda_i$ of SU(3) fail to partition, because seven have the spectrum $(\pm 1, 0)$ and one has $(1, 1, -2)/\sqrt{3}$. The $H_i$ operators defined here divide equally among these

TABLE II. A partitioning of 80 two-qutrit operators into 10 maximally commuting subsets, each consisting of 8 elements. Factor group elements are identified at the bottom: The identity element consists of operators in the top row (each "in triplicate"), and remaining elements correspond to the columns directly above them (in triplicate).

| $II$ | $IZ$ | $IZ^2$ | $ZI$ | $ZZ$ | $ZZ^2$ | $Z^2I$ | $Z^2Z$ | $Z^2Z^2$ |
|---|---|---|---|---|---|---|---|---|
| | $IX$ | $IX^2$ | $XI$ | $XX$ | $XX^2$ | $X^2I$ | $X^2X$ | $X^2X^2$ |
| | $IY$ | $IY^2$ | $YI$ | $YY$ | $YY^2$ | $Y^2I$ | $Y^2Y$ | $Y^2Y^2$ |
| | $IV$ | $IV^2$ | $VI$ | $VV$ | $VV^2$ | $V^2I$ | $V^2V$ | $V^2V^2$ |
| | $ZX$ | $Z^2X^2$ | $VZ$ | $XY$ | $YV^2$ | $V^2Z^2$ | $Y^2V$ | $X^2Y^2$ |
| | $ZY$ | $Z^2Y^2$ | $XZ$ | $YV$ | $VX^2$ | $X^2Z^2$ | $V^2X$ | $Y^2V^2$ |
| | $ZV$ | $Z^2V^2$ | $YZ$ | $VX$ | $XY^2$ | $Y^2Z^2$ | $X^2Y$ | $V^2X^2$ |
| | $Z^2X$ | $ZX^2$ | $YZ^2$ | $XV$ | $VY^2$ | $Y^2Z$ | $V^2Y$ | $X^2V^2$ |
| | $Z^2Y$ | $ZY^2$ | $VZ^2$ | $YX$ | $XV^2$ | $V^2Z$ | $X^2V$ | $Y^2X^2$ |
| | $Z^2V$ | $ZV^2$ | $XZ^2$ | $VY$ | $YX^2$ | $X^2Z$ | $Y^2X$ | $V^2Y^2$ |
| $\mathcal{EE}$ | $\mathcal{ER}$ | $\mathcal{EL}$ | $\mathcal{RE}$ | $\mathcal{RR}$ | $\mathcal{RL}$ | $\mathcal{LE}$ | $\mathcal{LR}$ | $\mathcal{LL}$ |

two spectra, and it will be clear that the equal division generalizes to $N$ qutrits. The $9^N-1$ partitioning Hermitian operators provide an optimally symmetrical set of generators of SU($3^N$).

In the one-qutrit case, the four *trinary H* operators play a special role: They define the four mutually unbiased basis sets completely, they generate their partners $\overline{H}$ through Eq. (11), and they generate all eight unitary operators through

$$U=\exp(2\pi iH/3),\quad U^\dagger=\exp(-2\pi iH/3). \tag{13}$$

To verify that Eqs. (13) are equivalent to Eqs. (9) and (10), we expand the exponential noting that all odd powers of $H$ are equal to $H$ itself and all even powers are equal to $H^2$:

$$U=I+\frac{i\sqrt{3}}{2}H-\frac{3}{2}H^2. \tag{14}$$

Equation (11) then shows that $U$ and $U^\dagger$ are equal to $(\overline{H}\pm iH)\sqrt{3}/2$, which is the inverse of Eqs. (9) and (10).

## III. TWO QUTRITS

A complete orthonormal set of operators on the two-qutrit Hilbert space is provided by the 81 tensor products of the form $(I,Z,\ldots,V^2)_1\otimes(I,Z,\ldots,V^2)_2$. Henceforth, in most expressions we shall drop both the $\otimes$ symbol and the subscripts referring to the individual qutrits, so that expressions like $ZX$ or $Y^2V$ or $IZ$ will be understood as tensor products. These operators have the following properties in common with their one-qutrit factors: Each generates a cyclic subgroup of order 3—namely, $(II,PQ,(PQ)^2)$, with $(PQ)^3=II$—and each has the trinary spectrum $(1,\omega,\omega^2)$. The product of any two operators is equal to a single operator multiplied by $\omega^n$, so that the Pauli group of two qutrits has order $81\times3=243$. Each of these properties follows from the fact that operators on one qutrit commute with operators on the other.

Clearly there is a factor group of order 81, each of whose elements consists of a basis operator in triplicate. But there are more interesting factor groups of order 9—for example, $(\mathcal{E},\mathcal{R},\mathcal{L})\otimes(\mathcal{E},\mathcal{R},\mathcal{L})$—which relate to the partitioning of the basis operators.

The basis operators partition into ten MCS's of eight operators each. One such partitioning and the associated MUB's were presented in Ref. [19]. We show another (similar) partitioning in Table II together with a related factor group. The factor group is defined by choosing its identity element $\mathcal{EE}$ to be the first row in triplicate—i.e., $\mathcal{E}=(\mathcal{I},\mathcal{Z},\mathcal{Z}^2)$ for both qutrits. All other elements are identified in the bottom row, and these consist of the nine entries in the columns directly above, all in triplicate. Each such element is generated by a multiplication such as $\mathcal{ER}=IX\times\mathcal{EE}$. While the factor group is determined uniquely once its $\mathcal{EE}$ element is specified, there are several ways in which the elements can be arranged within each column so that every *row* is a maximally commuting subset, and consequently, all eigenbases are mutually unbiased. However, these special arrangements are not likely to occur automatically, because only 12 out of the $(9!)^7$ possible arrangements within this particular factorization result in commuting subsets. The theorem of Ref. [17] proves that a partition exists, and our Appendix B proves that it conforms to the structure of a factor group as illustrated in Table II. This structure is useful in determining all possible partitions, of which there are 48. Before embarking on this task, however, it will be useful to discuss and classify the basis sets resulting from Table II.

### A. Mutually unbiased basis sets

A "complete set of commuting" operators consists of any two operators in a given row that are not squares of one another. We shall refer to such operator pairs as *generators* because, in addition to providing the two independent quantum numbers needed to specify the nine basis states, they generate the group consisting of the remaining operators in their row and the identity.

We may choose the first and third entries in each row as the generators. Then, because those of the top four rows are all one-qutrit operators, the corresponding bases must be separable. The first-row basis states are written $|n,m\rangle_{zz}$, the

indices $(n,m)$ being two-digit trinary numbers that specify the eigenvalues $(\omega^n,\omega^m)$ of the one-qutrit factors in the subscript, $Z_1$ and $Z_2$. Second-row states are written $|n,m\rangle_{xx}$, denoting products of eigenstates of $X_1$ and $X_2$, and similarly in rows 3 and 4. The full basis *sets* are denoted by $S(Z,Z)$, $S(X,X)$, and so forth ("S" for separable).

Generators in all remaining rows (5–10) are characterized by the failure of commutativity between their individual one-qutrit factors. As in the case of two *qubits* [14], the joint eigenstates of such operator pairs must be totally entangled. Focusing on the fifth row, we look for joint eigenstates of $ZX$ and $VZ$. Let us first write the most general form of eigenstates of $ZX$ as expansions in separable states $|n,m\rangle_{zx}$ belonging to $S(Z,X)$:

$$|\Psi_0\rangle = (a|0,0\rangle + b|1,2\rangle + c|2,1\rangle)_{zx},$$

$$|\Psi_1\rangle = (d|1,0\rangle + e|2,2\rangle + f|0,1\rangle)_{zx},$$

$$|\Psi_2\rangle = (g|2,0\rangle + h|0,2\rangle + k|1,1\rangle)_{zx}, \tag{15}$$

where the subscripts of $\Psi$ denote the eigenvalues of $ZX$ (namely, 1, $\omega$, and $\omega^2$, respectively) and the coefficients $a,\ldots,k$ are arbitrary. The coefficients are then fixed by requiring that the general states above also be eigenstates of $VZ$. There are three choices of coefficients in each expression, corresponding to the three eigenvalues of $VZ$. The salient feature is that the coefficients have equal amplitudes, their relative phases being integral powers of $\omega$. The physical interpretation of this is that while $ZX$ takes a definite value, its factors $Z$ and $X$ are maximally random. That is, the sum of the two indices (the subscript of $\Psi_n$) is fixed, while each index by itself takes all three of its possible values with equal probabilities. With this in mind, we can write all nine row-5 basis states in the form

$$|n,m\rangle_{\mathrm{B}(zx,vz)} = \frac{1}{\sqrt{3}}\sum_{k=0}^{2} C_{nmk}|k,n-k\rangle_{zx}, \tag{16}$$

where $C^3_{nmk}=1$. The subscript on the left side, $B(ZX,VZ)$, refers to the entangled basis *set* ("B" for Bell like). The individual states within this set are denoted by the two-digit trinary number $(n,m)$ specifying the two eigenvalues $(\omega^n,\omega^m)$ of the operators $(ZX,VZ)$, respectively. The indices $(n,m)$ themselves are just the eigenvalues of the *trinary Hermitian* counterparts defined by Eq. (9); for example,

$$H(ZX) = (ZX - Z^2X^2)/i\sqrt{3}. \tag{17}$$

So, restating the physical interpretation in terms of observables, the eigenvalue $(n)$ of $H(ZX)$ is the sum, modulo 3, of the eigenvalues of $H(Z_1)$ and $H(X_2)$ ($k$ and $n-k$, respectively), the sum being definite while the summands are random.

The randomness applies not just to the one-qutrit factors in the two generators as shown above, but to *all* one-qutrit operators. This follows most dramatically from the stunning appearance of all 16 one-qutrit factors in every maximally commuting subset in rows 5–10. So *any* one-qutrit factor may appear in a generator and the above arguments apply. A concise general proof will be given in the following subsection.

Rows 8–10 of Table II define states that differ subtly from those of rows 5–7. Consider the generators $Z^2X$ and $YZ^2$ of row 8. The Hermitian counterpart of either of these, for example,

$$H(Z^2X) = (Z^2X - ZX^2)/i\sqrt{3}, \tag{18}$$

refers to differences, not sums of individual qutrit indices: If joint eigenstates of $Z^2X$ and $YZ^2$ are expanded in the same product basis $S(Z,X)$ used for Eq. (16), the result takes the form

$$|n,m\rangle_{\mathrm{B}(z^2x,yz^2)} = \frac{1}{\sqrt{3}}\sum_{k=-1}^{1} D_{nmk}|k,n+k\rangle_{zx}, \tag{19}$$

showing that the eigenvalue $(n)$ of $H(Z^2X)$ is the difference between eigenvalues of $H(X_2)$ and $H(Z_1)$. Of course one may choose different operators to label the states, and in row 8 there is one choice, $XV$, which refers to sums, while the other three independent choices refer to differences. Rows 8–10 share the preference for differences, while rows 5–7 share the preference for sums. These balanced asymmetries can be interchanged but not removed by renaming the operators, and they appear to be inevitable.

In all the above examples, basis states have been written in "minimal" form—i.e., three-term expansions for entangled states and single terms (by definition) for separable states. This requires a special choice of "quantization axes" for both qutrits, a choice that is unique for S states although not for B states. It is interesting to note that if one instead expands all MUB states in the standard basis, $S(Z,Z)$, then all those outside of $S(Z,Z)$ have nine-term expansions, of necessity. A full complement of MUB's was written out explicitly in this manner for solving the mean king's problem in nine dimensions [19].

### B. 4S-6B theorem

We now address the problem of enumerating all partitions of the operator set and of proving that all have the same structure, producing exactly four separable and six totally entangled basis sets. We begin by proving that there must be exactly four separable bases. Consider any operator having an identity factor—say, $PI$. The most general MCS to which it may belong is generated by itself and any operator that commutes with it, apart from a power of itself. Such an operator must take the form $IQ$, leading to the MCS $(II,PI,P^2I)\otimes(II,IQ,IQ^2)-II$, where $Q$ may be any of $V$, $X$, $Y$, or $Z$, squares being redundant. This subset, or its two generators, defines the separable basis set $S(PQ)$. Since there are four operators of type $PI$ to begin with and since each must belong to a MCS containing a distinct $IQ$ operator, we conclude (1) that there are 4 MCS's of this type and (2) there are 24 distinct choices of these 4 subsets. Correspondingly, there are 4 separable, mutually unbiased basis sets and 24 distinct choices for this quartet. The distinction is simply one of renaming the basis states of one qutrit while keeping those of the other qutrit fixed. We may therefore conclude from the

specific example shown in Table II that the remaining six basis sets are totally entangled. It is instructive, however, to prove this result in more general terms.

Since the required separable bases exhaust all operators containing an identity factor, it suffices to show that any MCS lacking such operators must produce a totally entangled basis set. We make use of Eq. (A7) of Appendix A, which expresses the projection operator $P_\alpha^A$ of any state $\alpha$ belonging to the basis $A$ in terms of all the corresponding operators $U_1^A,\ldots,U_{d-1}^A$ and the identity $I=U_d^A$. The coefficients $\varepsilon_{a\alpha}^*$ all have unit amplitude and, in particular, $\varepsilon_{d\alpha}=1$. The overall factor of $d^{-1}=1/9$ guarantees that $\mathrm{Tr}\,P_\alpha^A=1$. The reduced density matrix of either qutrit is the partial trace of $P_\alpha^A$ over the states of the other. The partial trace vanishes for all operators with $a=1,\ldots,d-1$ because no identity factors appear, leaving only $a=d$:

$$\rho_1=\mathrm{Tr}_2 P_\alpha^A=\frac{1}{9}\mathrm{Tr}_2 I=\frac{1}{3}I_1, \tag{20}$$

where $I_1$ is the identity operator on qutrit 1. Similarly, $\rho_2=I_2/3$, showing that the pure state $P_\alpha^A$ is totally entangled. This proves that all six remaining MCS's give rise to totally entangled basis sets.

It is interesting to note that the absence of identity factors in a MCS implies two other points encountered earlier: (1) *All one-qutrit operators must appear as factors*. To prove this, assume that they do not. Then at least one such factor would have to appear twice, producing a pair such as $PQ$ and $PR$. But these are distinct and commute only if $R=Q^2$, in which case their product $(P^2I)$ contains a single identity factor, producing a contradiction. (2) *No two generators of such a MCS may have compatible one-qutrit factors*. This follows from point (1), noting that $PQ$ and $P^2Q^2$ appear in the same MCS but cannot be generators.

### C. Final count: 48 partitions

Having counted 24 choices for the four separable basis sets, we ask finally how many choices remain for partitioning the complete operator set. It suffices to begin with the specific choices of rows 1–4 as written in Table II, since all others correspond to relabeling the operators on the second qutrit. To count the remaining options for partitioning the operators in rows 5–10, we count the ways to rearrange operators in the third column, keeping those of the first column fixed, in such a way that these pairs generate compatible rows that do not overlap with any other rows. (This simplification rests on the factor group theorem of Appendix B.) Consider $ZX$ from the first column. It commutes with $VZ$, $XZ$, and $YZ$ and no others from the third column. The first and third choices are viable, while the second must be ruled out because it generates $YY$, which already appears in the third row. Given either viable choice, there remains only one choice for partners of $ZY$ and $ZV$ that does not reproduce an operator already existing in some row above. Moving to the last three rows, $Z^2X$ commutes with $YZ^2$, $VZ^2$, and $XZ^2$ and no others from the third column. Given our choice for the fifth row, only the first choice is viable: $VZ^2$ is ruled out because it generates $YV$, which already appears in the sixth row, and $XZ^2$ is ruled out because it generates $VV$, which is found in the fourth row. Therefore, in total, only two choices exist for the last six rows given the first four rows. The choice not shown here appears in Table V of Ref. [19]. With 24 options available for the first four rows, there are 48 distinct partitions of the full operator set. Only the last choice, involving just the totally entangled basis sets, does not correspond to a simple relabeling of one-qutrit states.

TABLE III. These 13 three-qutrit operators and their squares form a maximally commuting subset whose eigenbasis consists of totally entangled three-qutrit GHZ states.

| | | | |
|---|---|---|---|
| $XXX$ | $YYY$ | $VVV$ | |
| $XYV$ | $YVX$ | $VXY$ | |
| $XVY$ | $YXV$ | $VYX$ | |
| $Z^2ZI$ | $Z^2IZ$ | $IZ^2Z$ | $ZZZ$ |

## IV. THREE QUTRITS

There are $9^3=729$ tensor product operators such as $VZX^2$, $Y^2IX$, $ZII$, etc., that comprise a complete orthonormal set. As before, each generates a cyclic subgroup of order 3 and has the trinary spectrum. The product of any two is a single operator times $\omega^n$, so that the Pauli group has order $3\times 9^3=2187$. The more interesting factor groups are of order 27—for example, $(\mathcal{E},\mathcal{R},\mathcal{L})^{\otimes 3}$; these relate to the partitioning of the basis operator set into $3^3+1=28$ maximally commuting subsets of $3^3-1=26$ operators each. The new aspect that emerges with $N=3$ is that different partitioning *structures* are possible. For example, if the number of separable basis sets is maximized at 4, then all remaining 24 basis sets are totally entangled. However, one may choose fewer than 4 separable bases, requiring that some others have partial entanglement. Let us begin by illustrating the three types of basis sets and corresponding MCS's that can occur. We shall then determine the partitioning structures that are possible, without attempting to count the actual number of each type.

Product bases may be denoted by $\mathrm{S}(PQR)$, where $P$ is any of $V$, $X$, $Y$, or $Z$, etc. These are eigenbases of the one-qutrit operators $PII$, $IQI$, and $IIR$, which generate the maximally commuting subsets $(I,P,P^2)\otimes(I,Q,Q^2)\otimes(I,R,R^2)$. As with two qutrits, there are only four (nonredundant) choices for $P$ and therefore at most four such subsets, with four corresponding product bases. As before, of course, there are many choices for these quartets.

Totally entangled basis sets in which the entanglement is shared equally among all three qutrits (analogous to three-qubit GHZ basis sets [14]) arise from MCS's similar to the example shown in Table III. ("Similar" means "same number of $I$ factors.") We show half of the operators which, together with their squares, comprise the full MCS of 26. Each row, together with its squares, forms a subgroup when combined with $ZZZ$, its square, and the identity. The three generators of the full MCS may be any three operators that do not belong to the same subgroup. The operators in the last row are notable because they (and their squares) are diagonal in the *separable* basis $\mathrm{S}(ZZZ)$. The first three operators specify dif-

ferences between two one-qutrit indices, and the fourth operator specifies the sum of all three. A simultaneous eigenstate (with the sum and all differences equal to zero, for example) is

$$|\Psi\rangle = (a|000\rangle + b|111\rangle + c|222\rangle)_{zzz}, \tag{21}$$

where the subscript indicates separable states, and the coefficients $a$, $b$, and $c$ are arbitrary. There are nine expressions of the form of Eq. (21) which are simultaneous eigenstates of fourth-row operators, each being a superposition ($k=0,1,2$) of separable states $|k,n+k,l+k\rangle_{zzz}$ with arbitrary coefficients. The fourth-row operators (or, more precisely, their Hermitian counterparts $H$) have eigenvalues $n$, $l$, $(l-n)$, and $(l+n)$, respectively, which reflects the fact that only two of them are independent. In order to fix the coefficients in the 9 expressions and extract the 27 simultaneous eigenstates of all operators in Table III, we require that these expressions be eigenstates of a third independent operator—say, $XXX$. We may write the 27 basis states in analogy with Eq. (16) as

$$|n,l,m\rangle_{\mathrm{G}} = \frac{1}{\sqrt{3}}\sum_{k=0}^{2} C_{nlmk}|k,n+k,l+k\rangle_{zzz}, \tag{22}$$

where $|C_{nlmk}|=1$, the subscript G identifies the entangled basis *set* $\mathrm{G}(Z^2ZI, Z^2IZ, XXX)$, and $n$, $l$, and $m$ are the eigenvalues of (the Hermitian counterparts of) the three operators listed, respectively. For example, $H(XXX)=[XXX-(XXX)^{\dagger}]/i\sqrt{3}\rightarrow m$.

The presence of the operator $XXX$ in this list might suggest the alternative separable basis set $\mathrm{S}(XXX)$ for the expansion of the $|n,l,m\rangle_{\mathrm{G}}$ states. However, such expansions would require sums of nine terms, not three. The basis $\mathrm{S}(ZZZ)$ is special in reducing the expansion to its "simplest" form. This situation is analogous to that of three-qubit GHZ states, where the "simplest" form consists of two-term expansions in separable states. There too the simplification depends on a special choice of quantization axes for the individual qubits, other choices requiring four- or eight-term expansions.

The "three-qutrit GHZ" states, like their three-qubit counterparts, share the property that all one-particle reduced density matrices are proportional to the identity. The proof of this fact again follows directly from the operators themselves: We expand the projection operator $P_{\alpha}^{A}$ of any such basis state in terms of the MCS operators using Eq. (A7) of Appendix A. Since no operator in the expansion has more than a single identity factor (apart from the $III/27$ term), the partial trace of $P_{\alpha}^{A}$ over any two qutrits is proportional to the identity on the other—for example,

$$\rho_1 = \mathrm{Tr}_{2,3}P_{\alpha}^{A} = \frac{1}{27}\mathrm{Tr}_{2,3}I = \frac{1}{3}I_1. \tag{23}$$

There are subtle differences among three-qutrit G bases analogous to those occurring in two-qutrit B bases, in which the expansion of Eq. (22) takes slightly different forms. For example, suppose that all operators on the third qutrit are interchanged with their squares in Table III. Then sums and differences are interchanged wherever the third qutrit is involved, and the expansion in the same separable basis $\mathrm{S}(ZZZ)$ takes the form

$$|n,l,m\rangle_{G'} = \frac{1}{\sqrt{3}}\sum_{k=0}^{2} D_{nlmk}|k,n+k,-l-k\rangle_{zzz}, \tag{24}$$

where G′ refers to $\mathrm{G}(Z^2ZI, Z^2IZ^2, XXX^2)$ and $m$ is the eigenvalue of $H(XXX^2)$, etc. Clearly there are four distinct expansions of the type seen in Eqs. (22) and (24), corresponding to the four ways of distributing $(-)$ signs among the $k$'s.

The Aharonov state $|\mathcal{A}\rangle$ that is used in the solution of the Byzantine agreement problem [10] is the (unique) spin singlet state of three qutrits. It is the superposition of all six permutations of 0, 1, and 2 among the three qutrits, with coefficients $(1/\sqrt{6})$ for even permutations and $(-1/\sqrt{6})$ for odd. Thus, it is the superposition of two states of the form of Eq. (22),

$$|\mathcal{A}\rangle = \frac{1}{\sqrt{2}}(|1,2,1\rangle_{\mathrm{G}} - |2,1,1\rangle_{\mathrm{G}}), \tag{25}$$

where the third entry in the kets is the eigenvalue of $XXX$, which is a cyclic permutation operator, and the first two entries distinguish even and odd permutations.

Let us finally illustrate MCS types that produce basis sets of mixed entanglement, in which one particle is unentangled while the other two are maximally entangled in the Bell-like states of the previous section. One such subset that singles out the first particle is generated by $ZII$, $IZX$, and $IYZ$. The corresponding basis set can be denoted by $\mathrm{SB}[Z_1;(ZX,YZ)_{2,3}]$, which indicates products of $Z$ states for particle 1 with Bell states for particles 2 and 3. States within this basis set can be expanded using the coefficients defined in Eq. (16):

$$|n,l,m\rangle_{\mathrm{SB}} = \frac{1}{\sqrt{3}}\sum_{k=0}^{2} C_{lmk}|n,k,l-k\rangle_{zzx}, \tag{26}$$

where the subscript SB is short for $\mathrm{SB}[Z_1;(ZX,YZ)_{2,3}]$. Here the first index does not vary in the sum; in other basis sets such as $\mathrm{SB}[Z_2;(ZX,YZ)_{1,3}]$ the second would be held constant. A maximum of 12 such basis sets can be mutually unbiased: Any qutrit can be singled out to be unentangled, and in each case four basis sets are possible ($V$, $X$, $Y$, or $Z$). In a partition where this maximum is realized, the remaining 16 basis sets must all be of the GHZ (G) type.

To understand the range of partitioning structures, we classify the 728 operators as one-body (two identity factors), two-body (one identity factor), and three-body (no identity factors). The total number of each type is given in Table IV and compared with the numbers that occur within each type of MCS. This table shows that there can never be more than 4 mutually unbiased separable bases, since this would require more than the existing 24 one-body operators. Similarly, there can never by more than 12 partially entangled bases. More generally, the numbers of each type that may coexist within any partitioning structure must satisfy the relations

TABLE IV. The distribution of operators within the three types of maximally commuting subsets: separable (S), partially entangled (SB), and totally entangled (G). These profiles determine which partitioning structures are possible.

| Operators | One-body | Two-body | Three-body |
|---|---|---|---|
| Total numbers | 24 | 192 | 512 |
| One S basis | 6 | 12 | 8 |
| One SB basis | 2 | 8 | 16 |
| One G basis | 0 | 6 | 20 |

$$N(\mathrm{G}) = 16 + 2N(\mathrm{S}),$$

$$N(\mathrm{SB}) = 12 - 3N(\mathrm{S}), \tag{27}$$

where $N(\mathrm{S}) = 0, 1, \ldots, 4$ is the number of separable bases. The number of partially entangled (SB) bases may be 0–12 in steps of 3, and the number of GHZ bases may range from 16 to 24 in steps of 2. Equations (27) require that no other MCS types exist, and one can easily verify that this is indeed the case [26]. Similar coexistence conditions exist for the three-*qubit* case, where analogous types of mutually unbiased basis sets occur. However, the new and surprising aspect of the present results is the existence of a *minimum* number of GHZ bases.

## V. CONCLUDING SUMMARY

The foregoing three sections illustrate how factorizations of the Pauli group relate to operator partitions and hence to mutually unbiased basis sets. The factor groups of order $3^N$—for example, $(\mathcal{E}, \mathcal{R}, \mathcal{L}))^{\otimes N}$—are isomorphic to every MCS in the partition. Every MCS has $N$ generators, which provide the necessary quantum numbers to label the associated basis states by $N$-digit trinary numbers. The Hermitian counterparts of these generators form the "complete sets of commuting observables." The $3^N+1$ distinct sets are mutually unbiased: Any state for which one set takes definite values produces perfectly random outcomes for all other sets. This statement applies equally well to the full MCS's.

New aspects emerge as one proceeds to larger numbers of qutrits. In the case of a single qutrit there is a unique partitioning of the eight operators into four MCS's.

In the case of two qutrits, there are 48 distinct partitionings, but they all have the same structure, producing four separable bases and six totally entangled (Bell-like) bases. Each of the 10 MCS's has two generators, so that all quantum numbers are two-digit trinary numbers. Those associated with the Bell-like basis states refer exclusively to sums or differences of particular one-qutrit attributes, and in doing so they impose perfect randomness on *all* one-qutrit attributes.

The three-qutrit case exhibits distinct partitioning structures, allowing for the coexistence of three different types of basis sets according to Eqs. (27): The GHZ-like states are defined by three-digit trinary numbers, each digit referring to sums or differences of two or three one-qutrit attributes. At least one digit must refer to all three qutrits, as is seen from the generators. All one-qutrit attributes are perfectly random in the GHZ-like states.

The latter two cases illustrate a sort of complementarity between individual and joint properties of a system of particles. This complementarity is expressed through operator sets rather than individual operators, and in general all $N$ generators are required: With $N=3$, suppose we choose two generators $Z^2ZI$ and $Z^2IZ$ from Table III. A third choice $XXX$ produces a GHZ basis, while the alternative choice $ZII$ produces a separable basis. In the latter case, $XXX$ is random while in the former, $ZII$ is random (since *every* operator outside the MCS of the generators is random). In this sense the concept of unbiasedness of operator sets incorporates aspects of both complementarity and contextuality. The compatibility of two operators does not rest on their commutativity alone, but on the choice of other operators to be measured.

## ACKNOWLEDGMENTS

I would like to thank Jagdish and Suranjana Luthra for many stimulating discussions about the subject of this work.

## APPENDIX A

In this appendix we review a general theorem proved in Ref. [17]: A full complement of mutually unbiased basis sets exists if and only if a partitioning, complete, and orthonormal set of operators exists. We follow the notation of a similar proof given specifically for $N$-qubit systems in Ref. [14].

First, suppose that a full complement of $d+1$ mutually unbiased basis sets exists in a Hilbert space of dimension $d$. In terms of projection operators $P^A_\alpha = |A,\alpha\rangle\langle A,\alpha|$, where $A = 1, \ldots, d+1$ denotes the basis and $\alpha = 1, \ldots, d$ the state within it, the orthonormality of each basis is expressed by

$$\mathrm{Tr}(P^A_\alpha P^A_\beta) = \delta_{\alpha\beta} \tag{A1}$$

and the unbiasedness of different bases $(A \neq B)$ by

$$\mathrm{Tr}(P^A_\alpha P^B_\beta) = d^{-1}. \tag{A2}$$

Corresponding to each basis set, we may *define* a maximally commuting set of unitary operators, $U^A_a$, where $a = 1, \ldots, d$, including the identity, $I \equiv U^A_d$, by their spectral representations

$$U^A_a = \sum_{\alpha=1}^{d} \varepsilon_{a\alpha} P^A_\alpha. \tag{A3}$$

Unitarity of $U^A_a$ requires that $|\varepsilon_{a\alpha}| = 1$, and $U^A_d = I$ requires $\varepsilon_{d\alpha} = 1$. We further stipulate that the rows of the "$\varepsilon$ matrix" be orthogonal,

$$\sum_{\alpha=1}^{d} \varepsilon^*_{a\alpha}\varepsilon_{b\alpha} \equiv (\varepsilon_a, \varepsilon_b) = d\,\delta_{ab}, \tag{A4}$$

i.e., that the scaled matrix $\varepsilon/\sqrt{d}$ be unitary:

$$d^{-1}\varepsilon^\dagger\varepsilon = I. \tag{A5}$$

In consequence, the $U^A_a$ operators form an orthonormal set (with the exception of the redundant identities $U^A_d$), that is,

$$\mathrm{Tr}(U_a^{A\dagger}U_b^B)=\sum_{\alpha,\beta}\varepsilon_{a\alpha}^*\varepsilon_{b\beta}\mathrm{Tr}(P_\alpha^A P_\beta^B)=d\delta_{AB}\delta_{ab}, \quad \text{(A6)}$$

where Eqs. (A1) and (A4) are used if $A=B$ and Eq. (A2) and $\Sigma\varepsilon_{a\alpha}=0$ (for $a\neq d$) are used otherwise. Equation (A6) shows that the $d^2-1$ traceless $U_a^A$ operators, together with the identity, form a complete and orthonormal set. The partitioning property is guaranteed by Eq. (A3), which implies commutativity within subsets ($A$).

The converse of the above theorem may be demonstrated immediately. Assume that a complete and orthonormal set of operators $U_a^A$ exists with the partitioning property. Append the identity to each maximally commuting subset and apply the inverse of the transformation defined by Eq. (A3), exploiting Eq. (A5):

$$P_\alpha^A=d^{-1}\sum_{a=1}^{d}\varepsilon_{a\alpha}^*U_a^A. \quad \text{(A7)}$$

The required properties [Eqs. (A1) and (A2)] are easily verified. Equation (A7) is useful in Secs. III and IV.

As a final note, the operators $U_a^A$ need not be unitary. One can choose the matrix $\varepsilon$ to have real entries making $U_a^A$ Hermitian, for example. The matrix $\varepsilon/\sqrt{d}$ must then be orthogonal to ensure orthonormality of the set $\{U_a^A\}$.

## APPENDIX B

In this appendix we prove the relationship between partitionings of the operator set $\{U_a^A\}$ and factorizations of the Pauli group, $\{(1,\omega,\omega^2)\times U_a^A\}$. Simply stated, *any maximally commuting subset (say, A) in the partition corresponds to the identity element of a Pauli factor group. The other elements contain one and only one operator from every other MCS* ($B\neq A$). *The factor group is isomorphic to every MCS (plus the identity, and in triplicate).*

The following proof is given for $N$ qutrits (Hilbert space dimension $d=3^N$), although clearly the theorem is more general.

Consider the complete orthonormal set of unitary operators $\{U_a^A\}$ that partitions into maximally commuting subsets $A=1,\ldots,d+1$, where $a=1,\ldots,d-1$ denotes operators within each subset. The Pauli group consists of these operators, plus the identity, all *in triplicate* (i.e., multiplied by the three phase factors $\omega^n$) and is thus of order $3d^2=3\times 9^N$. A subgroup $\mathcal{F}$ consists of any maximally commuting subset (say, $A$), plus the identity, in triplicate:

$$\mathcal{F}=(1,\omega,\omega^2)\times(U_1^A,\ldots,U_d^A), \quad \text{(B1)}$$

where $U_d^A\equiv I$. The inclusion of the phase factors makes $\mathcal{F}$ an invariant subgroup which, consisting of $3d$ elements, defines a factor group of order $d$. All of the factor group elements are generated by the multiplication,

$$\mathcal{F}_b=U_b^B\mathcal{F}, \quad \text{(B2)}$$

with fixed $B\neq A$ and $b=1,\ldots,d$, the last entry reproducing the identity element $\mathcal{F}_d=\mathcal{F}$. The product rule of these $\mathcal{F}_b$ is identical to that of the $U_b^B$ themselves, modulo $W_n$,

$$\mathcal{F}_b\mathcal{F}_c=U_b^B\mathcal{F}U_c^B\mathcal{F}=U_b^BU_c^B\mathcal{F}, \quad \text{(B3)}$$

showing that indeed they form a factor group as advertised.

To prove the theorem stated above, notice that every $\mathcal{F}_b$ ($b\neq d$) contains a distinct operator in $B$, each in triplicate. But there are $d$ choices of $B$ ($B\neq A$), every one of which must generate the same factor group elements. Therefore every $\mathcal{F}_b$ ($b\neq d$) must contain a distinct operator from every maximally commuting subset other than $A$, each in triplicate. This accounts for the full constituency ($3d$) of each $\mathcal{F}_b$, so the theorem is proved.


[1] A.A. Zhukov, G.A. Maslennikov, and M.V. Chekhova, JETP Lett. **76**, 596 (2002); quant-ph/0305113.

[2] A.V. Burlakov *et al.*, Opt. Spectrosc. **94**, 684 (2003).

[3] R. Thew, A. Acin, H. Zbinden, and N. Gisin, Quantum Inf. Comput. **4**, 93 (2004).

[4] A. Vaziri, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **89**, 240401 (2002).

[5] A.B. Klimov, R. Guzmán, J.C. Retamal, and C. Saavedra, Phys. Rev. A **67**, 062313 (2003).

[6] R. Das, A. Mitra, V. Kumar, and A. Kumar, e-print quant-ph/0307240.

[7] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).

[8] D. Bruss and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).

[9] T. Durt, N.J. Cerf, N. Gisin, and M. Zukowski, Phys. Rev. A **67**, 012311 (2003).

[10] M. Fitzi, N. Gisin, and U. Maurer, Phys. Rev. Lett. **87**, 217901 (2001).

[11] A. Ambainis, e-print quant-ph/0204063.

[12] W.K. Wootters and B.D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989); in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, 1989), pp. 65–67.

[13] A. Zeilinger, Found. Phys. **29**, 631 (1999); Č. Brukner and A. Zeilinger, Phys. Rev. A **63**, 022113 (2001).

[14] J. Lawrence, Č. Brukner, and A. Zeilinger, Phys. Rev. A **65**, 032320 (2002).

[15] K. Gottfried, *Quantum Mechanics* (Benjamin, New York, 1966), p. 63.

[16] J. Preskill, Caltech, Lecture Notes, Physics 219, Chapter 7, pp. 90–91, available at http://www.theory.caltech.edu/~preskill/ph219

[17] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).

[18] N.J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[19] P.K. Aravind, Z. Naturforsch., A: Phys. Sci. **58**, 85 (2003).

[20] A.W. Joshi, *Elements of Group Theory for Physicists* (Wiley Eastern Limited, New Delhi, 1977), p. 139.
[21] R.T. Thew, K. Nemoto, A.G. White, and W.J. Munro, Phys. Rev. A **66**, 012303 (2002).
[22] J. Schwinger, in *Quantum Mechanics—Symbolism of Atomic Measurements*, edited by B.-G. Englert (Springer-Verlag, Berlin, 2001).
[23] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000), p. 454.
[24] I. Ivanovič, Phys. Lett. A **228**, 329 (1997).
[25] I thank Mark Byrd for suggesting these names.
[26] It is instructive to show that all possible generator sets lead to one of the three MCS types listed.