Bell states, mutually unbiased bases and the Mean King’s problem.

Thomas Durt\(^1\)

PACS number: 03.65.Ud, 03.67.Dd, 89.70.+c

Abstract: We show that, when the dimension \(N\) of the Hilbert space is a prime power, mutually unbiased bases are naturally related to the symmetry group that leaves (generalized) Bell states invariant. We show how the mutually unbiased bases can be expressed in terms of the (multiplication of the) associated finite field of \(N\) elements, and derive a new solution for the mean king’s problem.

Introduction

We showed recently \(^1\), in the framework of quantum cloning, that in dimension \(N = 4\) different classes of Bell states can be defined, that are associated to different groups of permutations of the \(N\) basis states. These Bell states were shown to be in one to one correspondence with a commutative group (generalised addition) of \(N\) elements. When the dimension is a prime power, it is known that it is possible to define a multiplication that, together with the addition forms a field structure. Beside, it is known \(^3\) \(^4\) that for such dimensions there exists a maximal set of mutually unbiased \(^5\) bases (two orthonormal bases of a \(N\) dimensional Hilbert space are said to be mutually unbiased if whenever we choose one state in the first basis, and a second state in the second basis, the modulus squared of their in-product is equal to \(1/N\)). We show in this paper how to (re)derive in a straightforward manner an expression for the states of these bases. They appear to be defined intrinsically in terms of the field operations. We show that these bases diagonalize a finite group of \(N + 1\) unitary transformations under which (generalized) Bell states are invariant. The (straightforward) connection with techniques developed in the framework of quantum information (tomography \(^6\), error operators \(^7\) \(^8\) \(^9\), the Mean King’s problem \(^10\) \(^11\) \(^12\)) is discussed.

\(^1\)TENA-TONA Free University of Brussels, Pleinlaan 2, B-1050 Brussels, Belgium. email: thomdurt@vub.ac.be
Construction of \( N+1 \) mutually unbiased bases. A crucial element of the construction is the existence of a finite commutative division ring or field of \( N \) elements. A field is a set with a multiplication and an addition operation which satisfy the usual rules, associativity and commutativity of both operations, the distributive law, existence of an additive identity 0 and a multiplicative identity 1, additive inverses, and multiplicative inverses for every element, 0 excepted. As it is well known, finite fields with \( N \) elements exist if and only if the dimension \( N \) is a prime or a power of a prime. Note that the derivation of a set of mutually unbiased bases is already known in such cases \([3, 4]\), but we found an easy and nearly self-consistent derivation, in terms of the field operations only via the properties of Bell states. In what follows we shall assume that the dimension is a prime power \( N = p^m \), so that there exists a field \( G \) with \( N \) elements, and two operations \( \odot_G \) and \( \oplus_G \). Moreover, we choose an expression (this is always possible) of this field in terms of integer numbers (0,1,...,\( N-1 \)) such that \( \gamma_i \odot_G \gamma_j = \gamma_i \oplus_G \gamma_j \) where \( \gamma_G = e^{i \frac{2\pi}{p^m}} \) is a \( p \)th root of unity. The following identity is then fulfilled:

\[
\sum_{q=0}^{N-1} \gamma_G (p \odot_G q) = N \delta_{q,0}
\]

Let us define the \((N^2)\) \( U \) operators as follows:

\[
U_i^{k \odot_G l} = \sum_{q=0}^{N-1} |e_0^{0,k}\rangle \langle e_0^0|; l : 0...N - 1, k : 1...N
\]

where \( \gamma_G = e^{i \frac{2\pi}{p^m}} \) and the states \( |e_0^{0,k}\rangle \) are defined as follows:

\[
|e_0^{0,k}\rangle = (\gamma_G^{(k-1) \odot_G q} \gamma_G^q)^{\frac{1}{2}} |e_0^q\rangle q : 0...N - 1
\]

Note that in this hybrid expression certain operations (the powers for instance) are expressed in terms of the usual operations (the corresponding field is the set of complex numbers, and \( \gamma_G \) is a complex phasor). In virtue of the identities \( \gamma_i \gamma_j = \gamma_i \odot_G \gamma_j \), and \( \sum_{p=0}^{N-1} \gamma_G (p \odot_G q) = N \delta_{q,0} \), the \((N^2 - N)\) \( U \) operators are diagonal in the \( N \) dual bases defined as follows (this expression is a generalisation of an expression already derived by Wootters and Fields \([3]\)):

\[
|e_i^k\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \gamma_G^{(k-1) \odot_G q} \gamma_G^q |e_0^q\rangle
\]

\[
= \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} \gamma_G^{q \odot_G q} \gamma_G^{(k-1) \odot_G q} \gamma_G^{q \odot_G q} |e_0^q\rangle
\]

One can check by direct computation that the following identity is valid:

\[
U_i^{(i \odot_G l)} = \sum_k \gamma_G^{k \odot_G l} |e_k^i\rangle \langle e_k^i|
\]
Let us now check that the $N$ bases obtained so are mutually unbiased.

$$
\langle e^k_i | e^l_j \rangle = \frac{1}{N} \sum_{q=0}^{N-1} \gamma_G^{\otimes q \oplus (i \oplus q)(j \oplus q)} \left( \gamma_G^{\otimes ((l-1) \oplus (k-1)) \oplus q \oplus q} \right)^{1/2} 
$$

$$
\langle e^k_i | e^l_j \rangle, \langle e^l_j | e^k_i \rangle = \frac{1}{N^2} \left( \sum_{q=0}^{N-1} \gamma_G^{\otimes q \oplus (i \oplus q)(j \oplus q)} \left( \gamma_G^{\otimes ((l-1) \oplus (k-1)) \oplus q \oplus q} \right)^{1/2} \right) \left( \sum_{q'=0}^{N-1} \gamma_G^{\otimes q' \oplus (i \oplus q')(j \oplus q')} \left( \gamma_G^{\otimes ((l-1) \oplus (k-1)) \oplus q' \oplus q'} \right)^{1/2} \right)
$$

$$
= \frac{1}{N^2} \left( \sum_{q=0}^{N-1} \gamma_G^{\otimes q \oplus (i \oplus q)(j \oplus q)} \left( \gamma_G^{\otimes ((l-1) \oplus (k-1)) \oplus q \oplus q} \right)^{1/2} \right) \left( \sum_{q'=0}^{N-1} \gamma_G^{\otimes q' \oplus (i \oplus q')(j \oplus q')} \left( \gamma_G^{\otimes ((l-1) \oplus (k-1)) \oplus q' \oplus q'} \right)^{1/2} \right)
$$

$$
= \frac{1}{N^2} \left( \sum_{q=0}^{N-1} \gamma_G^{\otimes q \oplus (i \oplus q)(j \oplus q)} \left( \gamma_G^{\otimes ((l-1) \oplus (k-1)) \oplus q \oplus q} \right)^{1/2} \right) \left( \sum_{t=0}^{N-1} \gamma_G^{\otimes t \oplus (j \oplus t)(k \oplus t)} \left( \gamma_G^{\otimes ((l-1) \oplus (k-1)) \oplus t \oplus t} \right)^{1/2} \right)
$$

$$
= \frac{1}{N} \sum_{t=0}^{N-1} \delta_{(k-1) \oplus (l-1),0} \delta_{i,j} \left( 1 - \delta_{(k-1) \oplus (l-1),0} \right) \frac{1}{N} \sum_{t=0}^{N-1} \delta_{t,0} \gamma_G^{\otimes t \oplus (j \oplus t)(k \oplus t)} \left( \gamma_G^{\otimes ((k-1) \oplus (l-1)) \oplus t \oplus t} \right)^{1/2}
$$

$$
= \delta_{k,j} \delta_{i,j} + \left( 1 - \delta_{(k-1) \oplus (l-1),0} \right) \frac{1}{N} \sum_{t=0}^{N-1} \delta_{t,0} \gamma_G^{\otimes t \oplus (j \oplus t)(k \oplus t)} \left( \gamma_G^{\otimes ((k-1) \oplus (l-1)) \oplus t \oplus t} \right)^{1/2}
$$

$$
= \delta_{k,j} \delta_{i,j} + (1/N)(1 - \delta_{k,j})
$$

We made use of the fact that there is no divider of 0 excepted 0 itself (the multiplication $\otimes_G$ forms a division ring). For $i = 0$, we define the operators $U$ as follows: $U_i^{(0 \oplus q)} = U_i^0 = V_i^0 = \sum_{k=0}^{N-1} \gamma_G^{(k \oplus q)} | e^0_k \rangle \langle e^0_k |$, in agreement with the relation $\mathbb{H}_i$. These operators are diagonal in the computational basis which, obviously, is mutually unbiased relatively to the $N$ other bases.

Beside, the $N^2$ $U$ operators are equal, up to a phase, to the $V$ operators which are defined by the relation $V_i^j = \sum_{k=0}^{N-1} \gamma_G^{((k \oplus i)(l \oplus j)) \oplus k} | e^0_k \rangle \langle e^0_k |$. The phase relation is the following:

$$
U_i^{(i \oplus q)} = \left( \gamma_G^{\otimes (i-1) \oplus q \oplus q} \right)^{1/2} V_i^{(i-1) \oplus q}
$$

These operators $V$ satisfy the following composition relation:

$$
V_i^j V_i^k = \gamma_G^{\otimes (i \oplus k)} V_i^{j \oplus k}
$$
Up to phases, this is a group composition law. Actually, the commutator of such operators is known as the Weyl commutation rule, and was already derived before in the study of mutually unbiased bases in prime dimensions [13, 11]. The novelty is that we realized that this pseudo-groupal law corresponds to a symmetry group as we shall now show.

**Transformation law for the Bell states.**

We can reexpress in terms of the field operations the definition of Bell states introduced in [14] and [1], and define a family of $N^2$ generalized Bell states as follows:

$$|B_{m^*,n}\rangle = N^{-1/2} \sum_{k=0}^{N-1} \gamma^{(k \oplus G_j)} |k^*\rangle |k \oplus G m\rangle$$  (9)

Note that in this definition, we introduced the basis $|k^*\rangle$ which is the complex conjugate basis of the direct basis $|k\rangle$ [14]. This does not make any difference when $|k\rangle$ is the reference (computational) basis but it does when the Bell states are defined relatively to a basis that possesses states with complex amplitudes when they are expanded in the computational basis. For instance, in the $k$th basis, we find the following Bell states:

$$|B^k_{m^*,n}\rangle = N^{-1/2} \sum_{l=0}^{N-1} \gamma_G^{(l \oplus G_n)} |e^k_l\rangle |e^{k \oplus G m}_l\rangle$$  (10)

We get the following transformation law for the Bell states, when we pass from the computational basis $|e^0_p\rangle$ to one of the mutually unbiased bases defined in Eqn. 8

$$|B^0_{m^*,n}\rangle = \gamma_G^{(m^* \oplus G^n \oplus G j)} |B^0_{m^*,n}\rangle (11)$$

This is a bijective relation between the Bell states (up to global phases), because there is no divider of 0 excepted 0 itself. Most of all, the following identity is fulfilled:

$$V^i_j |B^0_{m^*,n}\rangle = \gamma_G^{(m^* \oplus G^n \oplus G j)} |B^0_{m^*,n}\rangle$$  (12)

Remember that $V^i_j |B^0_{Am^*,Bn}\rangle$ is like $((V^i_j)^* V^i_j |B^0_{Am^*,Bn}\rangle$, so that the problem of global phases in the definition of the $V$ operators is solved. This shows that, (up to irrelevant, global phases) the mutually unbiased bases are eigen bases of a finite symmetry group: a set of transformations that preserves the Bell states. As we shall
briefly show, the recognition of this fundamental invariant associated to the maximal sets of mutually unbiased bases allows us to shed a new light on old problems and techniques that were developed in the framework of quantum information.

**Applications in quantum information.**

We shall now briefly discuss three direct applications of these ideas in the framework of quantum information: error operators, quantum tomography, and the Mean King’s problem.

1. Error operators: According to a standard procedure in quantum cryptography, let us assume that Alice and Bob share the maximally entangled state $|B_{0^*0}\rangle_{AB} = N^{-1/2} \sum_{k=0}^{N-1} |k^*\rangle_A |k\rangle_B$ and that Alice measures the state $|k^*\rangle_A$, so that Bob gets the collapsed state $|k\rangle_B$. This is a way for Alice to transmit quNits to Bob. Let us assume now that an eavesdropper Eve controls the source and replaces $|B_{0^*0}\rangle_{AB}$ by $|B_{n^*,m}\rangle_{AB}$. When Alice projects her quNit onto $|k^*\rangle_A$, then Bob receives, instead of $|k\rangle_B$, $V_n^m |k\rangle_B$ (up to a global, irrelevant, phase). This explains why we can interpret the operator $V$ as an error operator. According to the transformation law $11$, if Alice and Bob want to transmit the key in another, mutually unbiased basis, as in the BB84 protocol $15$, the change of basis maps the Bell state $|B_{n^*,m}\rangle$ onto $|B_{-m+n(k-1)^*,n}\rangle$ (up to a phase). Accordingly, the error operators $V$ are bijectively intertwined when one passes from the computational basis to any of the $N$ other bases that diagonalize these operators; for instance, $V_n^m$ is mapped onto $V_{(k-1),n-m}^n$, up to a phase. This mapping is bijective only in prime dimensions. This explains the special role played by prime dimensions (or more generally by the existence of a field): it is only for such dimensions that the $N+1$ bases are treated on the same footing.

2. Quantum tomography:

Measuring the probabilities of transition towards the states of the mutual unbiased bases allow us to make a complete tomography of an arbitrary quantum state. For instance, it is easy to show that the following equivalence is fulfilled:

$$|e_{i\oplus j}^0\rangle\langle e_i^0| = (1/N) \sum_{k,l} V_l^k Tr.( (V_l^k)^+ |e_{i\oplus j}^0\rangle\langle e_i^0|)$$  \hfill (13)

Formally, if we express the density matrix as a $N^2$ dimensional state, the previous identity is equivalent to the fact that the Bell states form an orthonormal basis. By linearity, we obtain a similar development for any linear operator $L$: $L = (1/N) \sum_{k,l} V_l^k Tr.( (V_l^k)^+ L)$. The same is true for what concerns the $U$ operators, which are (for prime dimensions only) in one to one correspondence with the.
V operators. As they are equal to the V operators up to a phase, they also allow us to perform tomography: 

\[ L = (1/N) \sum_{k,l} U^k_l Tr.((U^k_l)^* \cdot L). \]

In particular, when \( L \) represents an arbitrary density matrix, we can obtain a complete knowledge about it by measuring the \( N^2 - 1 \) operators \( V^k_l k, l \neq 0 \), or because they are in one to one correspondence by measuring in the \( N + 1 \) bases that diagonalize the V operators the \( (N - 1)(N + 1) \) average values \( \langle e^k_i | L | e^k_i \rangle \), \( k : 0...N + 1, j \neq 0 \) (the remaining values \( \langle e^k_0 | L | e^k_0 \rangle \), \( j : 0...N + 1 \) being obtained by normalisation).

3. The Mean King’s problem:

We shall firstly give an overview of the treatment in the simplest case (qubits) \[10\]. We shall then consider the general case for which solutions already exist (in prime \[11\] and power prime dimensions \[12\]) and derive a solution thanks to the tools that were introduced in this paper. The problem to solve is, roughly speaking, the following: Alice must, in order to save her head, be able to distinguish the 6 product states \( |e^k_i|^\text{King} \otimes |e^k_i|^\text{Alice}, i = 0...N = 2, k = 0, N - 1 = 1 \). According to our previous conventions, the indices \( i = 0,1 \) and 2 correspond to the \( Z \), \( X \) and \( Y \) bases respectively. According to the solution derived by B-G Englert (\[11\]), Alice can solve the problem by measuring such states in the 4-dimensional basis that is defined as follows:

\[
|\Psi\rangle^Z_1 = \frac{1}{4} (|B^Z_{0,0}\rangle_{K,A} + |B^Z_{0,1}\rangle_{K,A} + |B^Z_{1,0}\rangle_{K,A} + i|B^Z_{1,1}\rangle_{K,A})
\]

\[
|\Psi\rangle^Z_2 = \frac{1}{4} (|B^Z_{0,0}\rangle_{K,A} + |B^Z_{0,1}\rangle_{K,A} - |B^Z_{1,0}\rangle_{K,A} - i|B^Z_{1,1}\rangle_{K,A})
\]

\[
|\Psi\rangle^Z_3 = \frac{1}{4} (|B^Z_{0,0}\rangle_{K,A} - |B^Z_{0,1}\rangle_{K,A} + |B^Z_{1,0}\rangle_{K,A} - i|B^Z_{1,1}\rangle_{K,A})
\]

\[
|\Psi\rangle^Z_4 = \frac{1}{4} (|B^Z_{0,0}\rangle_{K,A} - |B^Z_{0,1}\rangle_{K,A} - |B^Z_{1,0}\rangle_{K,A} + i|B^Z_{1,1}\rangle_{K,A})
\]

In say the first basis the four Bell states are defined as follows:

\[
|B^Z_{m,n}\rangle_{1,2} = \frac{1}{\sqrt{2}} \sum_{k=0}^{1} (-)^{k,n} |k\rangle^Z_1 |k + m\rangle^Z_2
\]
where $m, n \in \{0, 1\}$. Note that in the two first bases, which are real, we omit the conjugation marks. Consequently:

$$|B^Z_{0,0}\rangle_{1,2} = \frac{1}{\sqrt{2}}\{|0\rangle_1^Z|0\rangle_2^Z + |1\rangle_1^Z|1\rangle_2^Z\}, \quad |B^Z_{0,1}\rangle = \frac{1}{\sqrt{2}}\{|0\rangle_1^Z|0\rangle_2^Z - |1\rangle_1^Z|1\rangle_2^Z\}$$

$$|B^Z_{1,0}\rangle = \frac{1}{\sqrt{2}}\{|0\rangle_1^Z|1\rangle_2^Z + |1\rangle_1^Z|0\rangle_2^Z\}, \quad |B^Z_{1,1}\rangle = \frac{1}{\sqrt{2}}\{|0\rangle_1^Z|1\rangle_2^Z - |1\rangle_1^Z|0\rangle_2^Z\}$$

It is easy to check that the two last $\Psi^Z$ states are orthogonal to the product state $|e^0_{0King}\rangle \otimes |e^0_{0Alice}\rangle$, and the first ones to $|e^1_{1King}\rangle \otimes |e^1_{1Alice}\rangle$. For instance $\langle \Psi^Z_{e^0_{0King}e^0_{0Alice}} | \Psi^Z_{e^0_{1King}e^0_{1Alice}} \rangle = 0$. Therefore, if Alice observes one of the two last (first) states and that afterwards the King reveals that he prepared a state in the $Z$ basis she can infer unambiguously that the Mean King prepared the state $|e^1_{1King}\rangle \otimes |e^1_{1Alice}\rangle$ (up to unobservable phase changes!). Therefore Alice can infer without error the values of the spins along three orthogonal directions (a rather counterintuitive result!) and consequently save her head. Once again the solution of this problem was already known in the past \[11\,12\]. Nevertheless the use of Bell states provides a direct way to attack the problem: if the Mean King’s problem is formulated in terms of $i$ (not necessary mutually unbiased) bases, the first candidate for the solution will be a combination of Bell states that is invariant in these bases. If we expand this state in terms of Bell states, the amplitudes of its development must obey linear constraints (of the order of $i.N^2$ constraints) that express that the state is eigenstate (for the eigenvalue 1) under the $i$ changes of basis. For instance, it can be checked that the two first columns of the matrix of amplitudes in the expression \[14\] are mapped onto themselves (up to permutations of the lines) if we intervert the two central columns. This constraint is the expression of the invariance of the $\Psi^Z$ states when we pass from the $Z$ to the $X$ basis. In principle, imposing strict covariance we ought also recover the same matrix after multiplying the last column by -1, but this does not matter, because the Mean King will never prepare combinations
We iterated the operations to emphasize that we are in a field with instead of (problem Alice’s problem). So the passage to a Hilbert space of dimension (larger than 9.8 percent \[16\]) (by the way, it would be more appropriate to call this problem Alice’s problem). So the passage to a Hilbert space of dimension \((p^m)^2\) is crucial. It is also worth noting that the matrix \[17\] with \(i\) replaced by 1, which is strictly covariant in the \(X\) basis is the double Hadamard matrix, which exhibits remarkable duality properties in dimension 4 \[1\]. This matrix can be expressed \[17\] in terms of the multiplication of a field with 4 elements \((2^2)\). Therefore, it is natural to look for a solution which is expressed in terms of the operations of a field of \((p^m)^2\) elements. We can express such elements as follows: \((i_1, i_2) = i_1 \odot i_2\). We iterated the operations to emphasize that we are in a field with \(N^2\) elements instead of \(N\). \(\lambda\) corresponds, roughly, to \(p^m\), but we wrote it this way in order not to confuse with other (Latin) indices. Now, as these operations form a field, we get: \((i_1, i_2) \odot (j_1, j_2) = i_1 \odot j_1 \oplus (i_1 \odot j_1 \odot j_2) \odot \lambda\). We can express \(\lambda \odot \lambda\) as \(\text{Res.}(\lambda \odot \lambda) \odot \text{Im.} (\lambda \odot \lambda) \odot \lambda = (R_1, I_2)\), and \(R_1 \neq 0\).

As \(\gamma_G = e^{\frac{i\pi}{p^n}}\) is a 2nd root of unity, only the lowest power of \(p\) (0) is relevant and we also have \(\gamma_G^{(i_1, i_2) \odot (j_1, j_2)} = \gamma^{(i_1 \odot j_1) \oplus (i_2 \odot j_2 \odot \text{Res.} (\lambda \odot \lambda))} = \gamma^{(i_1 \odot j_1) \oplus (i_2 \odot j_2 \odot R_1)}\). Intuitively, \(\text{Res}\) corresponds to the rest after division by \(p^m\).

Let us consider the \(N^2\) states defined as follows:

\[
|\Psi\rangle^{0}_{(i_1, i_2)} = \frac{1}{N^2} \sum_{m, n=0}^{N-1} \gamma_G^{(i_1, i_2) \odot (m, n)} (\gamma_G^{(m \odot n)})^{\frac{1}{2}} |B\rangle^{0}_{m, n})_{K, A}
\]

(19)

This basis is dual to the Bell basis (up to phases!) in a \(N^2\) dimensional Hilbert space \[17\]. It is easy to check its orthonormality, in virtue of the identity \(\sum_{i_1, i_2=0}^{N-1} \gamma^{(i_1, i_2) \odot (m, n)} = N^2\delta_{m, 0}\delta_{n, 0}\). If the King prepares a product of states of the computational basis \(|\epsilon_t^{0*}\rangle_{\text{King}} \otimes |\epsilon_t^{0}\rangle_{\text{Alice}}, i = 0...N - 1 = 1\), it is easy to check that \(\langle \Psi^{0}_{(i_1, i_2)} | \epsilon_t^{0*}_{\text{King}} \epsilon_t^{0}_{\text{Alice}} \rangle = \frac{1}{N^2} \sum_{i_1, i_2=0}^{N-1} \delta_{m, 0} \gamma^{(i_1 \odot i_2)} \gamma^{(i_2 \odot n \odot R_1)} \langle B\rangle^{0}_{m, n} \langle \epsilon_t^{0}_{\text{King}} \epsilon_t^{0}_{\text{Alice}} \rangle = \frac{1}{N} \delta_{i_2, R_1 / \odot R_1}\). This shows that, up to components of negligible weight, the basis \(\Psi^{0}_{(i_1, i_2)}\) is equivalent to the King’s basis. In order to be able to infer the value of the King’s preparation in any mutually unbiased basis, we must have a similar relation when we reexpress the King’s states and the \(\Psi^{0}_{(i_1, i_2)}\) state in the \(k\)th basis. In virtue of the identity \[11\] the
transformation law for the $|\Psi\rangle$ states is the following:

$$
|\Psi\rangle^k_{(i_1,i_2)} = \frac{1}{N^2} \sum_{m',n'=0}^{N-1} \gamma_G^{(i_1,i_2)\otimes(m'n')} (\gamma_G^{(m'\otimes n)})\frac{1}{2} \gamma_G^{(n\otimes Gn)} (\gamma_G^{(G(k-1)\otimes Gn\otimes Gn)})\frac{1}{2} |B_{m'n',n}\rangle, (k-1) = 0 \ldots N - 1(20)
$$

where $(\otimes_G m \oplus_G (k-1) \oplus_G n) = n'$, and $m' = n$. We are interested in the states of non negligible weight, which imposes that $m = 0$. Thus $(k-1) \oplus_G n = n'$, and $m' = n$.

$$
|\Psi\rangle^k_{(i_1,i_2)} = \frac{1}{N^2} \sum_{n=0}^{N-1} \gamma_G^{(i_1,i_2)\otimes(n,(k-1)\otimes Gn)} (\gamma_G^{(G(k-1)\otimes Gn\otimes Gn)})\frac{1}{2} \gamma_G^{(G(k-1)\otimes Gn\otimes Gn)} (\gamma_G^{(\oplus_G Gn\otimes Gn)} (\oplus_G Gn\otimes Gn)}\frac{1}{2} |B_{0,n'}\rangle
$$

$$
+\text{contributions of weight 0}
$$

$$
= \frac{1}{N^2} \sum_{n=0}^{N-1} \gamma_G^{(i_1\otimes Gn\otimes G(i_2\otimes G(k-1)\otimes Gn\otimes R1)} |B_{0,n'}\rangle
$$

$$
= \frac{1}{N} \sum_{n=0}^{N-1} \gamma_G^{(i_3\otimes Gn)} |B_{0,n'}\rangle
$$

The last expression is similar to the one obtained in the computational basis. This proves the invariance of the relevant components of the states $|\Psi\rangle$. Remark that it coincides exactly, in the qubit case, with the expression 14 computed from [11].

**Conclusion.**

We show in another paper [17] how the rather formal results relative to the construction of the mutually unbiased bases can be derived from very primitive concepts: addition, multiplication, and duality. The whole structure can be derived in a nearly self-consistent manner. Beside, it seems that our results are simpler than what can be found in the literature on the subject. We believe that our approach provides a gain of simplicity, and maybe of generality. In any case, the recognition of the Bell states as fundamental objects in this framework appeared to be useful in the resolution of the Mean King’s problem, god forgives him!

**Acknowledgment**

The author acknowledges a Postdoctoral Fellowship of the Fonds voor Wetenschappelijke Onderzoek, Vlaanderen and also support from the IUAP programme of the Belgian government, and the grant V-18. Many thanks to Prof. A. Rimini for his kind hospitality at the university of Pavia where this work was completed. Sincere thanks to Prof. M. D’Ariano and Dr. M. Sacchi for discussions and comments, and also to B-G Englert for fruitful explanations about the Mean King’s problem. This paper is dedicated to the 27th birthday of the founding paper of L. Vaidman, Y. Aharonov and D.Z. Albert.
References

[1] B. Nagler and T. Durt, Phys. Rev. A 66 042323 (2003).
[2] J. Schwinger, Proc. Nat. Acad.Sci. U.S.A., 46 570 (1960).
[3] W.K. Wootters, and B.D. Fields, Ann. Phys. 91, 363 (1989).
[4] J. Lawrence, C. Bruckner, and A. Zeilinger, Phys. Rev. A 65, 032320 (2002).
[5] J. Schwinger, Proc. Nat. Acad.Sci. U.S.A., 46 570 (1960).
[6] I.D. Ivanovic, J. Phys. A, 14, 3241 (1981).
[7] N. J. Cerf, Phys. Rev. Lett. 84, 4497 (2000), N. J. Cerf, Acta Phys. Slov. 48, 115 (1998); special issue on quantum information, N. J. Cerf, J. Mod. Opt. 47, 187 (2000); special issue on quantum information.
[8] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. 88, 127902 (2002); M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. J. Cerf, e-print quant-ph/0106049
[9] M.A. Nielsen, and I.L. Chuang, Quantum Computing and Quantum Information (Cambridge University Press, Cambridge, 2000).
[10] L. Vaidman, Y. Aharonov, and D.Z. Albert, Phys. Rev. Lett. 58 1385 (1987).
[11] Y. Aharonov and B.-G. Englert, Z. Naturforsch. 56, 16 (2001).
[12] P.K. Aravind, Z. Naturforsch. 58A 2212 (2003).
[13] H. Weyl, Z. Phys. 46 1 (1927), H. Weyl: Gruppenthorie und Quantemechanik (1928), english translation by H.P. Robertson, E.P. Dutton, N-Y (1932).
[14] T. Durt, D. Kaslikowski, J-L Chen, en L.C. Kwek, quant-ph 0302078, 1-15 (2003).
[15] C. H. Bennett, and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984) p. 175.
[16] O. Schulz, R. Steinhubl, M. Weber, B-G Englert, C. Kursiefer, and H. Weinfurter, Phys. Rev. Lett. 90, 177901 (2003).
[17] T. Durt, to be put on the arxives soon.