Blind encoding into qudits

J. S. Shaari[a], M. R. B. Wahiddin[a,b], and S. Mancini[c]

[a]*Faculty of Science, International Islamic University of Malaysia (IIUM), Jalan Gombak, 53100 Kuala Lumpur, Malaysia*
[b]*Cyberspace Security Laboratory, MIMOS Berhad,*
Technology Park Malaysia, 57000 Kuala Lumpur, Malaysia
[c]*Dipartimento di Fisica, Università di Camerino, 62032 Camerino, Italy*
(Dated: January 10, 2007)

We consider the problem of encoding classical information into unknown qudit states belonging to *any* basis, of a maximal set of mutually unbiased bases, by one party and then decoding by another party who has perfect knowledge of the basis. Working with qudits of prime dimensions, we point out a no-go theorem that forbids shift operations on arbitrary unknown states. We then provide the necessary conditions for reliable encoding/decoding.

PACS numbers: 03.67.-a, 89.70.+c

I. INTRODUCTION

The idea of encoding and decoding classical information onto an unknown quantum state is essentially related to transformations and measurements of vectors state in a Hilbert space.

Suppose that Bob picks a qudit state from a given set (a subset of a d-dimensional Hilbert space $\mathcal{H}_d$) and sends it to Alice who is oblivious about the state. Alice is then expected to encode classical information (one out of d symbols) by virtue of unitary transformations before sending it back to Bob who should decode by gaining full information. This task can be reliably accomplished once the initial set of states forms a basis of $\mathcal{H}_d$. In fact, in such a case, Alice has simply to shift the incoming state into another of the basis by an amount determined by the symbol she wants to encode, while Bob has to measure in (project onto) the basis to retrieve Alice operation-symbol.

What happen if the initial set of states comprises more than one basis, specifically a number of mutually unbiased bases (MUB) [1, 2]?

This problem is of fundamental interest in quantum cryptography. For instance, blind encoding of classical information into states belonging to MUB is used in two-way deterministic quantum key distribution [3, 4, 5, 6, 7]. A crucial point to note in these protocols is that security results from the ambiguity of bases introduced by MUB. The endeavor for a more secure protocol thus entails the problem of maximizing the number of MUB over which encoding operations perform equally and decoding may be done reliably.

The maximum cardinality of any set of MUB in $\mathcal{H}_d$ is exactly known to be $d+1$ only when d is a prime power [1, 2]. If, moreover, it is simply prime, a straightforward construction of bases states exist [1, 2]. We henceforth restrict our attention to qudits of prime dimensions.

Unfortunately, a nontrivial scenario already emerges for qubits ($d = 2$), where the non existence of the universal-NOT [8, 9] forbids the ability to shift (flip) arbitrary unknown qubit states while the unitary Pauli operators shift qubits in only two out of three MUB.

This entails two main problems that we shall deal with in this paper: *i)* Can Alice blindly encode onto an unknown state of *any* basis of a maximal set of MUB? *ii)* Can Bob efficiently decode the full information? We discuss the first in terms of the generalization of a No-Go Theorem [7] which forbids the shifting of one arbitrary pure state into another in Sec.II, and we address the second problem in Sec.III by devising a specific protocol. In order to quantify the figure of merit of this protocol we consider, in Sec.IV, its efficiency within a communication framework [10]. We then apply the protocol to some examples. We reserve Sec.V for conclusions.

II. THE NO-GO THEOREM

We start by considering a d-dimensional quantum system, i.e., a qudit. In its Hilbert space $\mathcal{H}_d$ we choose a basis (computational basis) $\{|j\rangle\}$ labeled by elements $j \in \mathbb{Z}_d$. Moving from the $d = 2$ case (qubit), we can introduce generalized Pauli operators X and Z such that

$$X|j\rangle = |j + 1\rangle, \tag{1}$$
$$Z|j\rangle = \omega^j |j\rangle, \tag{2}$$

with

$$\omega := \exp\left(i\frac{2\pi}{d}\right). \tag{3}$$

Generalized Pauli operators are unitary and satisfy the anticommutation relation

$$ZX = \omega XZ. \tag{4}$$

It is well known [1, 2] that in $\mathcal{H}_d$, with d prime number, there are $d+1$ MUB and their states can be constructed as eigenstates of operators

$$XZ^0,\ XZ^1,\ XZ^2,\ \ldots,\ XZ^{d-1},\ Z. \tag{5}$$

Now suppose that Bob picks one of these states, say $|\psi_t^k\rangle$ where $t = 0, 1, \ldots, d-1$ denotes the element within a basis and $k = 0, 1, \ldots, d$ denotes the basis. Bob sends the state to Alice who is oblivious about it and she wants to encode one of the symbols belonging to the alphabet $\mathcal{A} \equiv \{0, 1, \ldots, d-1\}$. She therefore requires a unitary shift operator U such that

$$|\psi_t^k\rangle \xrightarrow{U^r} |\psi_{t\oplus r}^k\rangle, \tag{6}$$

where $\oplus$ stands for the sum mod d.

However, in considering a unitary operation that may shift qudit states in any MUB, we arrive at the following theorem (generalizing the one for qutrit [7] and extending the arguments for the nonexistence of Universal-NOT [8, 9]).

Theorem 1 *There is no unitary transformation that may shift between pure orthogonal states of any MUB of prime dimension.*

Proof. We prove the theorem by *reductio ad absurdum*. Let us first consider the eigenvectors of operators XZ^k, $k = 0, 1 \ldots, d-1$ denoting d different MUB, thus excluding the computational basis. They can be written as

$$\left|\psi_t^k\right\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{t(d-j)-ks_j} |j\rangle, \tag{7}$$

where $s_j = j + \ldots + d - 1$. We then write the unitary transformation U acting on the computational basis as

$$U\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\} \to \{a_{k,0}|1\rangle, a_{k,1}|2\rangle, \ldots, a_{k,d-1}|0\rangle\}, \tag{8}$$

with $a_{k,i} \in \mathbb{C}$ and $i = 0, 1 \ldots, d-1$. Without loss of generality, we may single out a state $\left|\psi_T^k\right\rangle$ with index T for any k (basis) and consider the operator U acting on it

$$U\left|\psi_T^k\right\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-2} a_{k,j}\omega^{T(d-j)-ks_j} |j+1\rangle + \frac{1}{\sqrt{d}} a_{k,d-1}\omega^{T-k(d-1)} |0\rangle. \tag{9}$$

Then, for any k, the resulting vector should correspond to one of the other vectors of the basis (orthogonal to the initial state) and we may write

$$\frac{1}{\sqrt{d}} \sum_{j=0}^{d-2} a_{k,j}\omega^{T(d-j)-ks_j} |j+1\rangle + \frac{1}{\sqrt{d}} a_{k,d-1}\omega^{T-k(d-1)} |0\rangle$$
$$= \frac{1}{\sqrt{d}} C_k \sum_{j=0}^{d-1} \omega^{t(d-j)-ks_j} |j\rangle, \tag{10}$$

with $t \neq T$ (as necessary shift requirement) and $C_k \in \mathbb{C}$ a global phase factor. By equating the coefficients of the same states at both sides of Eq.(10), we get

$$a_{k,j} = C_k\omega^{t(d-j-1)-T(d-j)+kj}. \tag{11}$$

Taking two indexes j and j' differing by an integer i, we have

$$\frac{a_{k,j}}{a_{k,j'}} = \omega^{-t+ki+Ti}, \tag{12}$$

and for $i = 1$

$$\frac{a_{k,j}}{a_{k,j+1}} = \omega^{-t+k+T}, \tag{13}$$

which must be invariant with respect to k, i.e.

$$\frac{a_{k,j}}{a_{k,j+1}} = \frac{a_{k',j}}{a_{k',j+1}}, \quad \forall\, k, k',\ k' \neq k. \tag{14}$$

Notice however that t may be different for differing ks. Hence, we write

$$\omega^{-t_k+k+T} = \omega^{-t_{k'}+k'+T}. \tag{15}$$

For every term $x \equiv k - t_k$, we may find a particular k' such that

$$k' = (x + T)\,\mathrm{mod}(d-1), \tag{16}$$

thus

$$\omega^{x+T} = \omega^{-t_{k'}+(x+T)\,\mathrm{mod}(d-1)+T}, \tag{17}$$

$$1 = \omega^{-t_{k'}+T}, \tag{18}$$

$$T = t_{k'}. \tag{19}$$

The last equality contradicts the shift requirement $T \neq t_k,\ \forall k$. This completes the proof. ∎

III.   REQUIREMENTS FOR RELIABLE ENCODING/ DECODING

Given the result of theorem 1 together with the fact that a unitary operator of the form XZ^l may shift eigenvectors of XZ^k when $k \neq l$ (that is states in a number of d MUB) [2], we also have the following corollary.

Corollary 2 *A unitary operation may shift a qudit state to an orthogonal one in at most d MUB.*

This results in the impossibility for Alice to reliably encode on $d + 1$ MUB. An obvious example would see Bob sending a state which is the eigenvector of XZ^k and Alice cannot encode a shift unless she knows the basis Bob used, that is k (then she may use XZ^l, $k \neq l$). Bob on the other hand could not perfectly decode, since in the event he measured a shifted state he could not discern between the d different kinds of transformations that would have resulted in the same evolution. However, Bob may be able to lessen his uncertainty by sending more qudits of differing bases and in the case that Bob may deduce perfectly Alice's unitary transformation, the problems of both encoding and decoding are solved. We therefore propose the following lemma.

Lemma 3 *A reliably blind encoding with $d + 1$ MUB needs to use strings of d qudits from d differing MUB.*

Proof. Let us denote the unitary transformation to shift a state in any basis except kth as $U_{\overline{k}}$. The number of unitaries available to shift a qudit state (including identity) would be $d + 2$ [those of Eq.(5) plus identity operation]. Bob's initial uncertainty about unitary transformation U amounts to

$$H(U) = \log(d+2). \tag{20}$$

where H stands for the Shannon entropy. Thus, the maximum information I_{max} that Bob may gain is exactly given by Eq.(20).

Suppose that Bob prepares a qudit state and that it undergoes Alice's unitary U_i. All U_i, $i = 1, \ldots, d+2$, are equally probable, thus

$$\Pr(U_i) = \frac{1}{d+2}. \tag{21}$$

Bob's subsequent measurement reveals whether the shift has taken place or not. The latter happens when the unitary is either identity or $U_{\overline{k}}$. Thus, we have the following probabilities

$$\Pr(s = 0) = \frac{2}{d+2}, \tag{22}$$

$$\Pr(s = 1) = \frac{d}{d+2}, \tag{23}$$

with S is a binary random variable taking values to denote shift of the state ($s = 0$ no shift, $s = 1$ shift). Moreover,

$$\Pr\left(U = U_i \mid s = 0\right) = \frac{1}{2}, \tag{24}$$

$$\Pr\left(U = U_i \mid s = 1\right) = \frac{1}{d}. \tag{25}$$

Then, Bob's uncertainty (about U) subsequent to his measurement may be calculated by using

$$H\left(U_i \mid S = s\right) = -\sum_i \Pr\left(U_i \mid S = s\right)\log\left[\Pr\left(U_i \mid S = s\right)\right], \tag{26}$$

so that Bob's a posteriori uncertainty results

$$
\begin{aligned}
H_{post}\left(U\right) &= \sum_s \Pr\left(S = s\right) H\left(U_i \mid S = s\right) \\
&= \frac{d}{d+2}\left[-\log\frac{1}{d}\right] + \frac{2}{d+2}\left[-\log\left(\frac{1}{2}\right)\right].
\end{aligned} \tag{27}
$$

By using Eqs.(20) and (27) we get

$$H\left(U\right) - H_{post}\left(U\right) < I_{max}. \tag{28}$$

If Bob had used two qudits of differing basis, with the encoding operation acting on both of them, we have to distinguish among four values of s with probabilities

$$\Pr\left(s = 00\right) = \frac{1}{d+2}, \tag{29}$$

$$\Pr\left(s = 01\right) = \frac{1}{d+2}, \tag{30}$$

$$\Pr\left(s = 10\right) = \frac{1}{d+2}, \tag{31}$$

$$\Pr\left(s = 11\right) = \frac{d-1}{d+2}. \tag{32}$$

Moreover,

$$\Pr\left(U = U_i \mid s = 00\right) = 1, \tag{33}$$
$$\Pr\left(U = U_i \mid s = 01\right) = 1, \tag{34}$$
$$\Pr\left(U = U_i \mid s = 10\right) = 1, \tag{35}$$
$$\Pr\left(U = U_i \mid s = 11\right) = \frac{1}{d-1}, \tag{36}$$

then Bob's a posteriori uncertainty becomes

$$H_{post}\left(U\right) = \frac{d-1}{d+2}\log\left(d-1\right). \tag{37}$$

Equation (37) can straightforwardly be generalized to strings of $n+1$ qudits (with $n+3$ possible s values) as

$$H_{post}\left(U\right) = \frac{d-n}{d+2}\log\left(d-n\right). \tag{38}$$

It is easy to see that the uncertainty becomes 0, when $d - n = 1$, or when $n = d - 1$. Hence in order for Bob to have complete information on the unitary transformation used, the number of qudits sent must be at least equal to d.

It is worth noting that the problem of encoding is consequently solved as well. ∎

IV. EFFICIENCY OF THE PROTOCOL

Despite the fact that Alice and Bob may communicate reliably as described above, the protocol is far from being efficient. Let us consider the definition of efficiency for blind encoding in the framework of communication. This definition closely follows the work of Ref.[10]. It is well known that given a quantum system the maximally attainable classical information I (in independent measurements) is bounded by the Holevo bound [11]

$$I \leq S(\rho) - \sum_i p_i S(\rho_i). \tag{39}$$

Since each qudit sent and received by Bob may perfectly be distinguished by Bob (as the states represent pure orthogonal states), he saturates the Holevo bound thus achieving, with d qudits, the maximal information $d \log_2 d$ bits. However, given a protocol, the actual amount of information that may be shared between Alice and Bob may differ from this maximal value. If we consider the shared information between Alice and Bob in the previous section, an ideal channel would have allowed its classical capacity [11] to be

$$C := \max I\left(A : B\right) = -\log\left(\frac{1}{d+2}\right). \tag{40}$$

Defining efficiency to be the ratio of the perfect channel capacity to the maximal information of d qudits, we get

$$\frac{\log_2\left(d+2\right)}{d \log_2 d} \leq 1, \tag{41}$$

with equality only in the case for qubits ($d = 2$). The ratio decreases by increasing d. In order to achieve unitary efficiency we must force the numerator to be $d \log_2 d$ or we must allow Alice to use d^d unitary operations. Intuitively this may be understood as follows: since d qudits are sent back and forth between Bob and Alice, the exhaustive number of codewords that may be shared between them would be d^d. Therefore, Alice must be able to execute d^d unitary operations for encoding while Bob must perfectly decode them. This means that Alice must construct unique operations that the composite system of d qudits (of differing MUB) could actually discern.

We consider the composed system state of d qudits

$$|\Psi\rangle \equiv \left|\psi_{t_1}^1 \psi_{t_2}^2 \ldots \psi_{t_d}^d\right\rangle \tag{42}$$

where the ψ^i belongs to d different MUB. Vectors like (42) span the space of d^d independent vectors. Then the encoding problem can be recast into the following form: can we find an encoding operation on $|\Psi\rangle$ such that $\left|\psi_{t_l}^l\right\rangle$ gets shifted to $\left|\psi_{t_l \oplus a}^l\right\rangle$ for any integers $t_l \in [1, d]$ and $a \in [0, d-1]$? The answer to this question is positive.

Let us first define the operation $U_{\overline{d+1}}$ as the operation that does not shift the state of the $(d+1)$th basis (which is not part of the composite system $|\Psi\rangle$) but would shift the states of all other qudits by 1. If we wish to encode a value a on a particular qudit i, we need to ensure that while qudit i gets shifted by a, the others would not be affected by the shift. Hence we could operate on the system $|\Psi\rangle$ the operations $U_{\overline{i}}^{d-a} U_{\overline{d+1}}^a$ which shifts the qudit i by a and the others by $(d - a + a) \bmod d = 0$. It is straightforward to see that we could execute a similar recipe to any other qudits in $|\Psi\rangle$. Hence, a general encoding may be written as

$$\left(U_{\overline{1}}^{d-a} U_{\overline{d+1}}^a\right) \left(U_{\overline{2}}^{d-b} U_{\overline{d+1}}^b\right) \ldots \left(U_{\overline{d}}^{d-k} U_{\overline{d+1}}^k\right) \left|\psi_{t_1}^1 \psi_{t_2}^2 \ldots \psi_{t_d}^d\right\rangle, \tag{43}$$

where $a, b, \ldots, k$ are different values to encode onto the relevant qudits. Simple observation tells us that we may encode in such a way all the d^d codewords.

The remaining question is whether such a combination is unique; i.e. despite the possible combinations for a string (subject to the condition that no two qudits in the string share a basis), one set of operations results in only one unique evolution of a string of states. This is vital as a set of operations must be recognizable by such strings of qudits. Let us write Eq.(43) as $A|\Psi\rangle \rightarrow |\Phi\rangle$ and suppose that another operation B gives $B|\Psi\rangle \rightarrow |\Phi\rangle$ then it obviously follows $A = B$. It goes without saying that other strings do not yield the same result as that of $|\Psi\rangle$. As long as Alice and Bob agrees to codewords to be designated to each set of operations, they may then have a faithful encoding/decoding procedure which is of unit efficiency. This is important since the above construction of encoding operations is done in states of known bases, while Alice needs to use these operations on unknown strings of qudits.

A. The Qubit Case

Consider Bob preparing two qubits states $\left|\psi_{t_1}^1 \otimes \psi_{t_2}^2\right\rangle$ with $\left|\psi_{t_1}^1\right\rangle$, $\left|\psi_{t_2}^2\right\rangle$ eigenstates of Pauli operator X and $Y \equiv XZ$ respectively. In constructing an operation which may flip the states of both qubits, Alice makes use of Eq.(43)

$$\left(U_{\overline{x}}^{2-a} U_{\overline{z}}^a U_{\overline{y}}^{2-b} U_{\overline{z}}^b\right)^{\otimes 2} \left|\psi_{t_1}^1 \otimes \psi_{t_2}^2\right\rangle \rightarrow \left|\psi_{t_1 \oplus a}^1 \otimes \psi_{t_2 \oplus b}^2\right\rangle, \tag{44}$$

with $a, b \in [0,1]$.

We can readily convince ourselves of the above by noticing

$$\left(U_{\overline{x}}^{2-a} U_{\overline{z}}^a\right) \equiv X^{2-a} Z^a, \tag{45}$$

$$\left(U_{\overline{y}}^{2-b} U_{\overline{z}}^b\right) \equiv Y^{2-b} Z^b. \tag{46}$$

B. The Qutrit Case

Consider Bob preparing three qutrits states $\left|\psi_1 \otimes \psi_2 \otimes \psi_3\right\rangle$ with the integer indices denoting different MUB. In constructing operations which may flip the states of qutrits, Alice makes use of Eq.(43)

$$\left[\left(U_{\overline{1}}^{3-a} U_{\overline{4}}^a\right)\left(U_{\overline{2}}^{3-b} U_{\overline{4}}^b\right)\left(U_{\overline{3}}^{3-c} U_{\overline{4}}^c\right)\right]^{\otimes 3} \left|\psi_{t_1}^1 \otimes \psi_{t_2}^2 \otimes \psi_{t_3}^3\right\rangle$$
$$\rightarrow \left|\psi_{t_1 \oplus a}^1\right\rangle \left|\psi_{t_2 \oplus b}^2\right\rangle \left|\psi_{t_3 \oplus c}^3\right\rangle, \tag{47}$$

with $a, b, c \in [0, 1, 2]$.

The unitary operations $U_{\overline{i}}$ corresponds to the well known shift/error operators for qutrits [12] . A table for the explicit evolution of the various possible states Bob may prepare under Alice's transformation is referred to in [7].

V. CONCLUSION

We have considered the problem of blind encoding classical information into quantum states belonging to a maximal set of MUB for systems whose dimensions equal to a prime number d. We noted that trivial encoding is essentially forbidden due to the inability of reliably shifting an unknown arbitrary qudit by unitary operations. We proved this in a no-go theorem which is a generalisation of specific case treated in Ref.[7]. On the other hand, Bob cannot reliably decode the information content of a qudit unless he actually prepares and then measures a string of d qudits. We provided a simple information theoretic proof for this lemma.

We then noticed that while d is the minimum number of qudits that must be sent to Alice for reliable decoding, the available generalised Pauli operations do not provide an efficient encoding protocol. Unit efficiency may be achieved with the protocol we proposed for the relevant encoding and decoding procedure. Two examples of application of this protocol has been explicitly shown.

The developed theory paves the way for the study of two way quantum communication in generic dimension and may be useful for a number of cryptographic tasks.

---

[1] I. D. Ivanovic, Geometric description of quantal state determination, J. Phys. A **14**, 3241 (1981).
[2] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury and F. Vatan, A New Proof for the Existence of Mutually Unbiased Bases, Algorithmica **34**, 512 (2002).
[3] Q.-Y. Cai, and B. W. Li, Deterministic Secure Communication Without Entanglement, Chin. Phys. Lett. **21**, 601 (2004).

[4] F.-G. Deng, and G. L. Long, Bidirectional quantum key distribution protocol with practical faint laser pulses, Phys. Rev. A **70**, 012311 (2004).

[5] M. Lucamarini, and S. Mancini, Secure Deterministic Communication without Entanglement, Phys. Rev. Lett. **94**, 140501 (2005).

[6] J.S. Shaari, M. Lucamarini, M.R.B. Wahiddin, Deterministic six states protocol for quantum communication, Phys. Lett. A **358**, 85 (2006).

[7] J.S. Shaari, and M.R.B. Wahiddin, Nonentagled qutrits in two way deterministic QKD, Phys. Lett. A (to appear).

[8] N. Gisin, and S. Popescu, Spin Flips and Quantum Information for Antiparallel Spins, Phys. Rev. Lett. **83**, 432 (1999).

[9] V. Buzek, M. Hillery, and R.F. Werner, Optimal manipulations with qubits: Universal-NOT gate, Phys. Rev. A **60**, R2626 (1999).

[10] A. Cabello, Efficient Quantum Cryptography, Rec. Res. Dev. Phys. **2**, 249 (2001).

[11] M. Keyl, Fundamentals ofquantum information theory, Phys. Rep. **369**, 431 (2002).

[12] N.J. Cerf, T. Durt, and N. Gisin, Cloning a qutrit, J. Mod. Opt., **49**, 1355 (2002).