# Multiparty $d$-Dimensional Quantum Information Splitting

A. Grudka* and A. Wójcik

Faculty of Physics, Adam Mickiewicz University
Umultowska 85, 61-614 Poznań, Poland

*(Received June 17, 2002; in final form September 12, 2002)*

Generalization of quantum information splitting protocol from qubits to qudits (quantum $d$-dimensional systems) is presented.

PACS numbers: 03.67.–a, 89.70.+c

## 1. Introduction

Recently Karlsson and Bourennane [1] and Hillery et al. [2] have presented a scheme for quantum information splitting, which allows encoding of a state of a given particle (qubit) into $N$-particle state in such a way that all $N$ particles are necessary for perfect reconstruction of the original state. In their scheme it is the phase information which is absent in the state of any single particle, and moreover, in the state of any subset of $M$ particles except $M = N$. On the other, in the last few years there has been growing interest in generalization of quantum information protocols from two-dimensional systems (qubits) to $d$-dimensional systems (qudits). For example generalization of teleportation was presented in [3–6], of quantum state purification in [7], of quantum cloning in [8]. Generalization of quantum key distribution protocols was proposed in [9, 10] and it was proven that the security of quantum cryptography increases with the dimension of the system used [11, 12]. It is the aim of our paper to present the $d$-dimensional generalization of the quantum information splitting protocol.

## 2. Outline of the scheme and discussion

Let us first briefly outline the scheme of Karlsson and Bourennane [1]. Alice is supposed to possess one qubit in a pure state $|\Psi\rangle_0 = a|0\rangle_0 + b|1\rangle_0$. She

*corresponding author; e-mail: agie@amu.edu.pl

wants to teleport it to two parties $\mathrm{Bob}_1$ and $\mathrm{Bob}_2$ in such a way that none of them can reconstruct the original state by himself. However, when they cooperate the reconstruction is possible even if we allow only local operations and classical communication between them. This task can be easily performed when all three parties have the Greenberger–Horne–Zeilinger state (GHZ-state), i.e. maximally entangled three-particle state of the form $|\mathrm{SO}(3)\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2|0\rangle_3 + |1\rangle_1|1\rangle_2|1\rangle_3)$, so the state of the whole system is

$$|\Psi\rangle_0|\mathrm{SO}(3)\rangle = \frac{a}{\sqrt{2}}(|0\rangle_0|0\rangle_1|0\rangle_2|0\rangle_3 + |0\rangle_0|1\rangle_1|1\rangle_2|1\rangle_3) + \frac{b}{\sqrt{2}}(|1\rangle_0|0\rangle_1|0\rangle_2|0\rangle_3 + |1\rangle_0|1\rangle_1|1\rangle_2|1\rangle_3), \tag{1}$$

where particles 0 and 3 belong to Alice and particles 1 and 2 belong to $\mathrm{Bob}_1$ and $\mathrm{Bob}_2$, respectively. In the first step of this protocol Alice performs the measurement of her particles (the qubit to be teleported and the qubit from GHZ-state) in the Bell basis, which consists of the following four states:

$$(|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2}, \qquad (|0\rangle|0\rangle - |1\rangle|1\rangle)/\sqrt{2},$$
$$(|0\rangle|1\rangle + |1\rangle|0\rangle)/\sqrt{2}, \qquad (|0\rangle|1\rangle - |1\rangle|0\rangle)/\sqrt{2}. \tag{2}$$

Depending on the result of the measurement, the two remaining particles are in one of the four states

$$a|0\rangle_1|0\rangle_2 + b|1\rangle_1|1\rangle_2, \tag{3}$$

$$a|0\rangle_1|0\rangle_2 - b|1\rangle_1|1\rangle_2, \tag{4}$$

$$a|1\rangle_1|1\rangle_2 + b|0\rangle_1|0\rangle_2, \tag{5}$$

$$a|1\rangle_1|1\rangle_2 - b|0\rangle_1|0\rangle_2. \tag{6}$$

The last three states can be transformed to the first one by the use of local unitary operations, so we consider only this state. To recover the original state, $\mathrm{Bob}_2$ applies the Hadamard transform $H$ defined as

$$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, \qquad H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}, \tag{7}$$

to his qubit and makes a measurement in computational basis. The resulting state after the measurement is

$$(a|0\rangle_1 + b|1\rangle_1)|0\rangle_2 \tag{8}$$

or

$$(a|0\rangle_1 - b|1\rangle_1)|1\rangle_2. \tag{9}$$

Thus, if $\mathrm{Bob}_2$ sends the result of his measurement to $\mathrm{Bob}_1$, then $\mathrm{Bob}_1$ can recover the original state.

If we replace the three-particle maximally entangled state in the protocol of teleportation by $(N+1)$-particle maximally entangled state, then the above

protocol can be easily generalized to split the information among $N$ parties ($\mathrm{Bob}_1$, $\mathrm{Bob}_2$, ..., $\mathrm{Bob}_N$). At the end of the splitting protocol $N$ parties share the state given by

$$a|0\rangle_1|0\rangle_2 \ldots |0\rangle_N + b|1\rangle_1|1\rangle_2 \ldots |1\rangle_N. \tag{10}$$

To recover the information $\mathrm{Bob}_2$, $\mathrm{Bob}_3$, ..., $\mathrm{Bob}_N$ perform Hadamard transformation and a measurement on their qubits. Knowing the results of all measurements, $\mathrm{Bob}_1$ can transform his qubit to the state

$$a|0\rangle_1 + b|1\rangle_1. \tag{11}$$

Now we will generalize this protocol for qudits. We will need the following unitary operations. The first one is quantum Fourier transform $\mathrm{QFT}_\mu$ which acts only on the $\mu$-th qudit

$$\mathrm{QFT}_\mu|j\rangle_\mu = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \exp\left(\frac{\mathrm{i}2\pi jk}{d}\right) |k\rangle_\mu. \tag{12}$$

For the case of qubits ($d = 2$) this is simply the Hadamard transform. The next one is a $d$-dimensional generalization of XOR (performed on the $\mu$-th and $\nu$-th qudit), given by the following definition:

$$\mathrm{XOR}_{\mu\nu}|j\rangle_\mu|k\rangle_\nu = |j\rangle_\mu|k + j \mathrm{mod} d\rangle_\nu. \tag{13}$$

Let $N + 1$ parties share initially the state of the form

$$|\mathrm{SO}(N+1)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_1|j\rangle_2 \ldots |j\rangle_{N+1}, \tag{14}$$

which is maximally entangled state of $N + 1$ qudits. Alice also has a qudit in the state

$$|\Psi\rangle_0 = \sum_{j=0}^{d-1} \alpha_j |j\rangle_0. \tag{15}$$

Thus, the state of the whole system is

$$|\Psi\rangle_0|\mathrm{SO}(N+1)\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \sum_{j=0}^{d-1} \alpha_k |k\rangle_0|j\rangle_1|j\rangle_2 \ldots |j\rangle_{N+1}. \tag{16}$$

In order to teleport the state $|\Psi\rangle$, Alice and $\mathrm{Bob}_1$, $\mathrm{Bob}_2$, ..., $\mathrm{Bob}_N$ have to perform the following operations:

(Step 1.) Alice applies $\mathrm{XOR}_{0N+1}$ and then $\mathrm{QFT}_0$. The resulting state is

$$\frac{1}{d} \sum_{k=0}^{d-1} \sum_{j=0}^{d-1} \sum_{l=0}^{d-1} \alpha_k \exp\left(\frac{\mathrm{i}2\pi kl}{d}\right) |l\rangle_0|j\rangle_1|j\rangle_2 \ldots |j + k \mathrm{mod} d\rangle_{N+1}. \tag{17}$$

With the use of the substitution $k + j \mathrm{mod} d = m$, Eq. (17) takes the form

$$\frac{1}{d}\sum_{k=0}^{d-1}\sum_{m=0}^{d-1}\sum_{l=0}^{d-1}\alpha_k \exp\left(\frac{\mathrm{i}2\pi kl}{d}\right)|l\rangle_0|m-k\mathrm{mod}d\rangle_1|m-k\mathrm{mod}d\rangle_2\ldots$$
$$\times|m-k\mathrm{mod}d\rangle_N|m\rangle_{N+1}. \tag{18}$$

(Step 2.) Alice measures her qudits (in computational basis). If the result of this measurement is $|l\rangle_0|m\rangle_{N+1}$, then the remaining $N$ qudits are in the state

$$\sum_{k=0}^{d-1}\alpha_k \exp\left(\frac{\mathrm{i}2\pi kl}{d}\right)|m-k\mathrm{mod}d\rangle_1|m-k\mathrm{mod}d\rangle_2\ldots|m-k\mathrm{mod}d\rangle_N. \tag{19}$$

Steps 1 and 2 are equivalent to the measurement in the generalized Bell basis.

(Step 3.) Alice sends the results of her measurement $l$ and $m$ to $\mathrm{Bob}_1$ and $m$ to $\mathrm{Bob}_2$, $\mathrm{Bob}_3$, ..., $\mathrm{Bob}_N$.

(Step 4.) $\mathrm{Bob}_1$ performs unitary operation

$$|m-k\mathrm{mod}d\rangle_1 \to \exp\left(\frac{-\mathrm{i}2\pi kl}{d}\right)|k\rangle_1. \tag{20}$$

$\mathrm{Bob}_2$, $\mathrm{Bob}_3$, ..., $\mathrm{Bob}_N$ perform unitary operations

$$|m-k\mathrm{mod}d\rangle_\mu \to |k\rangle_\mu \quad (\mu=2,\ldots,N). \tag{21}$$

The final state shared by $\mathrm{Bob}_1$, $\mathrm{Bob}_2$, ..., $\mathrm{Bob}_N$ is

$$|\mathrm{QSS}(N)\rangle = \sum_{k=0}^{d-1}\alpha_k|k\rangle_1\ldots|k\rangle_N. \tag{22}$$

Each party now possesses a qudit, which can be described by the following reduced diagonal density operator:

$$\rho_\mathrm{R} = \sum_{k=0}^{d-1}|\alpha_k|^2|k\rangle\langle k|, \tag{23}$$

which means that each party alone does not have the information on phases between the states $|k\rangle$.

One of the parties (e.g. $\mathrm{Bob}_1$) can reconstruct the original state if all parties cooperate in the process of the subsequent transforms

$$|\mathrm{QSS}(N)\rangle \to |\mathrm{QSS}(N-1)\rangle \to \ldots \to |\mathrm{QSS}(1)\rangle = |\Psi\rangle_1. \tag{24}$$

Below, we present how the transform $|\mathrm{QSS}(K)\rangle \to |\mathrm{QSS}(K-1)\rangle$ $(K=2\ldots,N)$ can be performed with the use of local operations and classical communication.

(Step 1.) $\mathrm{Bob}_K$ applies quantum Fourier transform ($\mathrm{QFT}_K$) to his qudit

$$\mathrm{QFT}_K|\mathrm{QSS}(K)\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\sum_{k=0}^{d-1}\alpha_j \exp\left(\frac{\mathrm{i}2\pi jk}{d}\right)|j\rangle_1|j\rangle_2\ldots|k\rangle_K. \tag{25}$$

(Step 2.) $\mathrm{Bob}_K$ measures his qudit in the computational basis. If he obtains the result $k_K$, the state of the remaining qudits is

$$\overline{|\mathrm{QSS}(K-1)\rangle} = \sum_{j=0}^{d-1} \alpha_j \exp\left(\frac{\mathrm{i}2\pi j k_K}{d}\right) |j\rangle_1 |j\rangle_2 \ldots |j\rangle_{K-1}. \tag{26}$$

(Step 3.) $\mathrm{Bob}_K$ sends the result of his measurement to $\mathrm{Bob}_1$.

(Step 4.) $\mathrm{Bob}_1$ changes phase of his qudit in the following way:

$$|j\rangle_1 \to \exp\left(\frac{-\mathrm{i}2\pi j k_K}{d}\right) |j\rangle_1. \tag{27}$$

After these steps the first $K-1$ parties share the following state:

$$|\mathrm{QSS}(K-1)\rangle = \sum_{j=0}^{d-1} \alpha_j |j\rangle_1 |j\rangle_2 \ldots |j\rangle_{K-1}. \tag{28}$$

It is clear that if $\mathrm{Bob}_2$, $\mathrm{Bob}_3$, ..., $\mathrm{Bob}_N$ perform the above protocol (step 1 to step 4) then $\mathrm{Bob}_1$ will obtain the desired state of his qudit, i.e. $|\Psi\rangle_1 = |\mathrm{QSS}(1)\rangle = \sum_{j=0}^{d-1} \alpha_j |j\rangle_1$. It is worth noting that the transform $|\mathrm{QSS}(N)\rangle \to |\Psi\rangle_1$ although written as a recursive formula (Eq. (24)) can be performed in parallel. In this case, $\mathrm{Bob}_1$ can perform all necessary phase changes in one step (instead of $N-1$). The appropriate unitary transform is

$$|j\rangle_1 \to \exp\left[\frac{-\mathrm{i}2\pi j(k_2 + k_3 + \ldots + k_N)}{d}\right] |j\rangle_1. \tag{29}$$

In conclusion, we have presented a protocol allowing to split the information on the quantum state of a qudit among $N$ parties.

## Acknowledgment

We would like to thank the State Committee for Scientific Research for financial support under grant no. 0 T00A 003 23.

## References

[1] A. Karlsson, M. Bourennane, *Phys. Rev. A* **58,** 4394 (1998).

[2] M. Hillery, V. Buzek, A. Berthiaume, *Phys. Rev. A* **59,** 1829 (1999).

[3] S. Stenholm, P.J. Bardroff, *Phys. Rev. A* **58,** 4373 (1998).

[4] K. Banaszek, *Phys. Rev. A* **62,** 024301 (2000).

[5] S. Albeverio, S.-M. Fei, *Phys. Lett. A* **276,** 8 (2000).

[6] W. Son, J. Lee, M.S. Kim, Y.J. Park, *Phys. Rev. A* **64,** 064304 (2001).

[7] G. Alber, A. Delgado, N. Gisin, I. Jex, http://xxx.arXiv.org/quant-ph/0102035.

[8] P. Zanardi, *Phys. Rev. A* **58,** 3484 (1998).

[9] H. Bechmann-Pasquinucci, W. Tittel, *Phys. Rev. A* **61,** 062308 (2000).

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

[11] D. Bruß, C. Macchiavello, *Phys. Rev. Lett.* **88,** 127901 (2002).

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