Antisymmetric multi-partite quantum states and their applications

I. Jex[1]), G. Alber[2]), S. M. Barnett[3]) and A. Delgado[4])

[1]) Department of Physics, FNSPE, CTU Prague, Břehová 7, 115 19 Prague, Czech Republic
[2]) Institut für Angewandte Physik, Technische Universität Darmstadt, D-64289 Darmstadt,Germany
[3]) Department of Physics and Applied Physics, University of Strathclyde, Glasgow Q4 ONG, UK
[4]) Department of Physics and Astronomy, University of New Mexico, 87131 Albuquerque, USA

Abstract:
Entanglement is a powerful resource for processing quantum information. In this context pure, maximally entangled states have received considerable attention. In the case of bi-partite qubit-systems the four orthonormal Bell-states are of this type. One of these Bell states, the singlet Bell-state, has the additional property of being antisymmetric with respect to particle exchange. In this contribution we discuss possible generalizations of this anti-symmetric Bell-state to cases with more than two particles and with single-particle Hilbert spaces involving more than two dimensions. We review basic properties of these totally antisymmetric states. Among possible applications of this class of states we analyze a new quantum key sharing protocol and methods for comparing quantum states.

PACS: 03.67.-a, 03.65.Ta

1 Introduction

By now, quantum theory has become a well established part of modern physics. We have become accustomed to its results even if some of the concepts involved appear strange from the point of view of classical physics. However, as long as these peculiarities are restricted to the microscopic domain it is not so difficult for us to get used to them. During the last decade there have been various successful attempts to push characteristic quantum phenomena into the macroscopic domain and to exploit these very phenomena for practical purposes. These attempts may be viewed as first steps of a newly emerging quantum technology. Thus, it was possible to propose new, efficient quantum algorithms, to develop methods for the transfer of quantum states and of secret keys, and to invent new quantum error correction methods which suppress decoherence. Quite a number of these new effects rely on the use of states whose correlations are incompatible with local realistic theories. The singlet state of two distinguishable spin-1/2 particles is a prominent example which has been studied

extensively in the past. The main purpose of the subsequent contribution is to point out several possible applications of generalizations of this singlet state to cases which involve more than two distinguishable quantum systems of arbitrary but finite dimensions.

2 Definition and basic properties of totally antisymmetric quantum states

Totally antisymmetric quantum states are natural generalizations of the singlet state to many-particle quantum systems. In atomic and molecular physics, for example, they have already been playing an important role as Slater-determinant states. These are defined by the relation

$$|A_N\rangle = \frac{1}{\sqrt{N!}} \sum_{\pi} (-1)^{sgn(\pi)} |\pi_1\rangle ... |\pi_N\rangle \tag{1}$$

with $\{|i_1\rangle ... |i_N\rangle; i_1, ..., i_N = 0, ..., d-1\}$ denoting an orthonormal basis of the Hilbert space of N d-dimensional quantum systems. The sum appearing in Eq.(1) runs over all possible permutations π of the N elementary quantum systems considered. Due to basic properties of determinants this state exists only in cases in which the number of particles N equals the dimension of the one-particle Hilbert spaces d involved. Thus, in the simple case of three qutrits, for example, the totally antisymmetric quantum state is given by

$$|A_3\rangle = \frac{1}{\sqrt{6}} \left\{ |0\rangle|1\rangle|2\rangle + |1\rangle|2\rangle|0\rangle + |2\rangle|0\rangle|1\rangle - |0\rangle|2\rangle|1\rangle - |1\rangle|0\rangle|2\rangle - |2\rangle|1\rangle|0\rangle \right\}. \tag{2}$$

Let us summarize briefly some of the most important properties of these totally antisymmetric states:

1. They are invariant under local unitary transformations of the form $U \otimes U \otimes ... \otimes U$, i.e.
$$U \otimes U \otimes ... \otimes U |\psi\rangle\langle\psi| U^\dagger \otimes U^\dagger \otimes ... \otimes U^\dagger = |\psi\rangle\langle\psi|. \tag{3}$$

2. Simultaneous measurements of all particles in a commonly chosen measurement basis result in perfect correlations, i.e.
$$P(i_1, \ldots, i_N) \equiv | \langle\pi_1| ... \langle\pi_N|\psi\rangle |^2 \frac{1}{N!} |\varepsilon_{i_1,...,i_N}|^2 \tag{4}$$
with $\varepsilon_{i_1,...,i_N}$ denoting the totally antisymmetric tensor which is non-zero only if all its indices are different.

3. They can be generated in an iterative manner by a sequence of generalized XOR-gates and discrete Fourier transforms. The three-particle state $|A_3\rangle$, for example, can be prepared from the antisymmetric two-particle state $\frac{1}{\sqrt{2}}(|2\rangle_1|1\rangle_2 - |1\rangle_1|2\rangle_2)$ by
$$|A_3\rangle = GR_{31}\ GR_{32}\ F_3\ |0\rangle_3 \frac{1}{\sqrt{2}}(|2\rangle_1|1\rangle_2 - |1\rangle_1|2\rangle_2).$$
Thereby, F_3 denotes the discrete Fourier transformation applied to the third particle and GR_{ij} represents a generalized XOR-operation applied to particles i and j. Applied to the first and second particle, for example, this latter operation is defined by
$$GR_{12}\ |i\rangle_1|j\rangle_2 = |i\rangle_1|i \ominus j\ \rangle_2 \tag{5}$$

with $\ominus$ denoting subtraction $mod(d)$. This construction can be generalized in a straightforward way to more than three particles.

4. In the case of N particles the reduced density matrix $\hat{\rho}_i$ of subsystem i is given by

$$\hat{\rho}_i = \frac{1}{d} \sum_{j=0}^{d-1} |j\rangle\langle j|, \tag{6}$$

i.e., the single-particle reduced density matrix describes a completely depolarized state. Projection of one of the particles onto a particular state, say $|j\rangle\langle j|$, leaves the rest of the system in the pure antisymmetric state which involves all one-particle states except state $|j\rangle$, i.e.

$$|\overline{A}_{N-1}\rangle = \frac{1}{\sqrt{(N-1)!}} \sum_{\pi} (-1)^{sgn(\pi)} |\pi_1\rangle ... |\pi_{N-1}\rangle. \tag{7}$$

The index of correlation [1] between a particular particle and the remaining part of the system is given by

$$I_{i-r} = S_i + S_r - S = 2S_i = 2\log\ (\mathrm{d}). \tag{8}$$

with the von-Neumann entropy of particle i being given by $S_i = -Tr\hat{\rho}_i \ln \hat{\rho}_i$ and with S_{i-r} denoting the von-Neumann entropy of the remaining part. The entropy S of the whole system equals zero as it is in a pure state.

As exemplified in the subsequent sections totally antisymmetric quantum states can be used for many tasks which are of interest for quantum communication.

3 A quantum mechanical key sharing protocol

The secret distribution of a classical key is one of the main aims of quantum cryptography. Known secure protocols of bipartite key distribution are either based on non-orthogonal two dimensional quantum states [2] or on entangled states [3]. These protocols enable two parties to share a common, secret classical key. Recently, several more general situations have been discussed. One of them involves the distribution of a classical key between several parties in such a way that a subset of the parties has access to the key only if they share the information available. Various multi-partite key sharing protocols of this kind have been proposed which are either based on the use of GHZ-states [4] or on the use of pairs of singlet states [5].

Here we discuss an alternative multi-partite quantum key sharing protocol which is based on anti-symmetric states of qudit systems. (A qudit system is a d dimensional elementary quantum system.) This protocol enables one to generate, to split and to distribute a classical d-ary key securely. We demonstrate the basic principles of this protocol for quantum key sharing in the simplest nontrivial case of three three-dimensional quantum systems. In this case we base our quantum protocol on the totally antisymmetric state $|A_3\rangle$ defined by Eq. (2). For this key sharing protocol two basic properties of totally antisymmetric states are important. Firstly, all outcomes of simultaneous measurements performed by the participants in identical bases must be different and secondly, the unitary invariance of A-states guarantees that this is also true for any commonly chosen basis.

Let us consider three parties (Alice, Bob and Charlie). Each of them is endowed with a common set $\mathcal{U}$ of unitary transformations. The protocol runs as follows:

- Alice prepares three qutrits in the anti-symmetric state $|A_3\rangle$. She applies a unitary transformation ($\in \mathcal{U}$) on qutrit one, measures this qutrit and keeps her choice of the unitary transformation and the measurement result secret. This transformation with the subsequent measurement changes the correlations in the anti-symmetric state.
- Alice sends qutrit two to Bob and qutrit three to Charlie.
- In order to recover the original state and the correlations of the measurements, Bob (Charlie) also chooses a unitary transformation ($\in \mathcal{U}$) randomly and applies it onto his qutrit. Afterwards Bob (Charlie) measures his qutrit. Alice keeps her choice secret.
- Bob (Charlie) transmits his choice of transformation to Alice but keeps the measurement outcome secret. If all three unitary transformations coincide, Alice declares the outcomes of the measurements to be a valid part of the key. In this case, Bob and Charlie can deduce Alice's result if they share the outcomes of their measurements.
- In order to study the security of the key generated by this protocol Alice requests from Bob and Charlie a subset of the outcomes of their measurements.

4 Security of the quantum key sharing protocol

As a general investigation of security is beyond the scope of this contribution, we restrict our subsequent discussion to a cut-and-resend attack which does not involve coherent measurements. In such an attack an external or internal eavesdropper could try to obtain information about the key by attaching an ancilla state to the three qutrits. Subsequently, measurement of the ancilla could reveal information about the outcomes of measurements performed on the qutrits.

The most general state of a system composed of qutrits and an ancilla is given by

$$|E\rangle \equiv \sum_{i_1,i_2,i_3=0}^{2} |i_1\rangle|i_2\rangle|i_3\rangle \otimes |E_{i_1,i_2,i_3}\rangle. \tag{9}$$

Thereby, the ancilla system is described by the states $|E_{i_1,i_2,i_3}\rangle$. These states need not be mutually orthogonal but they obey a normalization condition, namely $\langle E|E\rangle = 1$. If the eavesdropper wants to remain undetected he must design the state $|E\rangle$ in such a way that the probabilities $P(i_1, i_2, i_3)$ remain unchanged. This imposes a set of constraints onto the states $|E_{i_1,i_2,i_3}\rangle$. If we choose $\mathcal{U} = \{\mathbf{1}, F\}$ with F denoting the discrete Fourier transform these constraints are given by the equations

$$\begin{aligned}
|E_{012}\rangle + |E_{021}\rangle + |E_{120}\rangle + |E_{102}\rangle + |E_{201}\rangle + |E_{210}\rangle &= 0,\\
|x|^2(|E_{012}\rangle + |E_{021}\rangle) + x^*(|E_{102}\rangle + |E_{120}\rangle) + x(|E_{210}\rangle + |E_{201}\rangle) &= 0,\\
x^*(|E_{012}\rangle + |E_{210}\rangle) + |x|^2(|E_{102}\rangle + |E_{201}\rangle) + x(|E_{120}\rangle + |E_{021}\rangle) &= 0,\\
x(|E_{012}\rangle + |E_{102}\rangle) + x^*(|E_{201}\rangle + |E_{021}\rangle) + |x|^2(|E_{210}\rangle + |E_{120}\rangle) &= 0,\\
|x|^2(|E_{012}\rangle + |E_{021}\rangle) + x(|E_{102}\rangle + |E_{120}\rangle) + x^*(|E_{210}\rangle + |E_{201}\rangle) &= 0,\\
x(|E_{012}\rangle + |E_{210}\rangle) + |x|^2(|E_{102}\rangle + |E_{201}\rangle) + x^*(|E_{120}\rangle + |E_{021}\rangle) &= 0,\\
x^*(|E_{012}\rangle + |E_{102}\rangle) + x(|E_{201}\rangle + |E_{021}\rangle) + |x|^2(|E_{210}\rangle + |E_{120}\rangle) &= 0
\end{aligned}$$

with $x \equiv e^{-i\frac{2\pi}{3}}$. The unique solution of this set of equations is given by

$$|E_{i_1,i_2,i_3}\rangle = \varepsilon_{i_1,i_2,i_3}|R\rangle. \tag{10}$$

This result implies that, provided the eavesdropper wants to remain undetected, the state $|E\rangle$ has to have the form

$$|E\rangle = \left(\frac{1}{3!}\sum_{i_1,i_2,i_3=0}^{2}\varepsilon_{i_1,i_2,i_3}|i_1\rangle|i_2\rangle|i_3\rangle\right)|R\rangle. \tag{11}$$

Thus, the state of the ancilla factorizes from the qutrit-system so that the eavesdropper cannot obtain any information about the key. If the eavesdropper wants to retrieve information about the key he must perturb the state in such a way that the correlations of the outcomes of the measurements are changed.

5 A protocol for quantum state sharing

Totally antisymmetric states are also well suited for distributing d-dimensional quantum states between $N = d$ parties. The task of quantum state sharing to be realized may be viewed as a generalization of the well-known bipartite entanglement-assisted teleportation protocol. The aim of the protocol is to send the state $|\chi\rangle$ from a source to a particular receiver. However, due to security reasons it should be possible to reconstruct this state only if all participants cooperate. Thus, reconstruction of the state $|\chi\rangle$ by the receiver should be possible only if at least one additional mediator communicates additional classical information properly. In the simplest case of three parties, i.e. $N = d = 3$, the protocol implementing this task is characterized by the following identity

$$|\chi\rangle_1|A_3\rangle_{234} \equiv \sum_{l,\rho=0}^{2}\frac{1}{3}|\Psi_{l,\rho}\rangle_{12}\sum_{k=0}^{2}\frac{1}{\sqrt{3}}e^{i\frac{2\pi}{3}k\rho}F_3^{-1}|k\rangle_3\,U(l,\rho,k)|\chi\rangle_4. \tag{12}$$

This identity involves four particles, namely particle one which carries the quantum state $|\chi\rangle$ and particles two, three and four which are distributed between the three parties involved in the protocol. The orthonormal states $|\Psi_{l,\rho}\rangle_{12}$ are defined by

$$|\psi_{l,\rho}\rangle_{12} = \frac{1}{\sqrt{3}}\sum_{k=0}^{2}e^{i\frac{2\pi}{3}lk}|k\rangle_1|k\ominus\rho\rangle_2 \mod 3. \tag{13}$$

These orthonormal states generalize the Bell basis to the case of two qutrits. The unitary transformation $U(l,\rho,k)$ is given by

$$U(l,\rho,k)|m\rangle_4 \equiv e^{-i\frac{2\pi}{3}lm}\sum_{q,r=1}^{3}e^{i\frac{2\pi}{3}kq}\varepsilon_{m-\rho,q,r}|r\rangle_4. \tag{14}$$

F^{-1} denotes the inverse discrete Fourier transform.

The identity of Eq.(12) suggests the following protocol for quantum state sharing: The sender obtains particle two of the totally antisymmetric quantum state. Particles three and

four are sent to the other two parties. The sender who is now holding particles one and two performs a maximal quantum test on these two particles by projecting onto the orthonormal basis of generalized Bell states (13). As a consequence he obtains two measurement results, say l and ρ, which specify the Bell state particles one and two have been projected onto. Now, one of the other parties applies a discrete Fourier transformation onto particle three and performs a maximal quantum test on this particle. The result of this measurement yields the label of the quantum state particle three has been projected onto, say k. The three classical labels, namely (l, ρ, k) are communicated to the receiver. Only after having received this combined classical information from the other two parties is the receiver able to apply the proper inverse transformation, namely $U^{\dagger}(l, \rho, k)$, onto his particle which enables him to recover the original quantum state $|\chi\rangle$.

6 Comparison of two quantum states I

Quantum state identification and state comparison constitute two other interesting applications of totally antisymmetric quantum states [7]. Thereby one wants to answer the basic question whether *two given quantum states are identical or different*. The simplest version of this problem can be illustrated in the case of two qubits. We shall comment on two separate cases, namely on the case of two unknown and on the case of two known pure states.

Let us first assume that we are given two completely unknown pure quantum states and that we want to decide with maximum probability whether these states are identical or different. In the case of two unknown states, say $|\psi\rangle$ and $|\phi\rangle$, we cannot give an affirmative answer to the question whether *these two states are the same*. We can only determine whether theses states are different or whether the answer is inconclusive. The fact that a positive answer to this question cannot be obtained can be demonstrated in several ways. The most straightforward argument relies on continuity. For any pair of different states the affirmative answer should yield a zero result even in cases in which these states are only infinitessimally different. As a consequence the probability for a non-zero result would have to be discontinuous. This contradicts the fact that quantum mechanical probabilities are continuous functions of projection operators.

In view of this impossibility the natural question arises how to proceed in order to obtain at least a negative and an inconclusive answer. The product state of two qubits $|\psi\rangle|\phi\rangle$ can be decomposed uniquely into the symmetric states $|0\rangle|0\rangle, |1\rangle|1\rangle, (|0\rangle|1\rangle + |1\rangle|0\rangle)$ and into the antisymmetric state $(|1\rangle|0\rangle - |0\rangle|1\rangle)$. If we find a non-zero projection onto the antisymmetric state, the two states cannot be identical. If the measurement yields an overlap with one of the symmetric states the answer is inconclusive. What can we say about the relative frequency of these two possible outcomes? The overlap between the decomposition components is given by

$$P_s - P_a = |\langle\psi|\phi\rangle|^2 \geq 0, \tag{15}$$

where $P_s = 1 - P_a$ and $P_a = |(\langle 1|\langle 0| - \langle 0|\langle 1|)|\psi\rangle|\phi\rangle|^2/2$ is the overlap between the tested product state $|\psi\rangle|\phi\rangle$ and the antisymmetric state. Thus, the measurement will show the inconclusive result (projection onto the symmetric subspace) more often than a negative one.

A realization of this state comparison using passive optical elements (detection in the Bell basis) seems feasible. We have to distinguish in a reliable way the presence of the antisymmetric state from any element of the symmetric subspace. For this purpose also a

simple coincidence measurement could be used. The two states can be sent into a multiport, for example, and at the output the coincidences can be detected. Only if both states are identical certain coincidences are absent.

Procedures which are applicable to more than two copies require a more detailed study of the group structure of the corresponding state spaces. If the number of copies equals the dimension of the one-particle Hilbert spaces, i.e. $N = d$, then a comparison is simple as a totally antisymmetric state $|A_N\rangle$ exists. Otherwise we have to use projections onto combinations of the "most antisymmetric" states available. Let us consider the simple example of $N = 2$ and $d > 2$. The two-particle Hilbert space can be decomposed into two subspaces, namely a symmetric one, spanned by the vectors $|i\rangle|i\rangle$ and $(|i\rangle|j\rangle + |j\rangle|i\rangle)$, and an antisymmetric one, spanned by the states $(|i\rangle|j\rangle - |j\rangle|i\rangle)$ with $i, j = 0, ..., d-1$. Successful projection onto the latter state indicates that the two quantum states are different. Another simple case arises if $N = 3$ and $d = 2$. The eight dimensional three-particle Hilbert space can be decomposed into two subspaces spanned by the states $|1\rangle|1\rangle|1\rangle, |0\rangle|0\rangle|0\rangle, (|1\rangle|1\rangle|0\rangle + |1\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|1\rangle), (|1\rangle|0\rangle|0\rangle + |0\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|0\rangle)$ and by the states $(2|1\rangle|1\rangle|0\rangle - |1\rangle|0\rangle|1\rangle - |0\rangle|1\rangle|1\rangle), (2|0\rangle|0\rangle|1\rangle - |0\rangle|1\rangle|0\rangle - |1\rangle|0\rangle|0\rangle), (|1\rangle|0\rangle|1\rangle - |0\rangle|1\rangle|1\rangle), (|0\rangle|1\rangle|0\rangle - |1\rangle|0\rangle|0\rangle)$. The latter four dimensional subspace can be used to decide whether three two-level states are different.

7 Comparison of two quantum states II

Let us now assume that two qubits are each prepared in one of the known states

$$|\psi_{1,2}\rangle = \cos\theta|+\rangle \pm \sin\theta|-\rangle. \tag{16}$$

The problem of comparing these two states can be solved either by the strategy of minimum probability of error or by the strategy of unambiguous state identification (for a review see Ref.[6] and references therein). In the first case the minimum error with which both states can be distinguished is given by

$$P_e^{comp} = \frac{1}{2}\cos^2(2\theta). \tag{17}$$

In the second case the minimum probability of obtaining an inconclusive answer is given by

$$P_?^{comp} = \cos(2\theta)[2 - \cos(2\theta)]. \tag{18}$$

The question is whether these two strategies are optimal. Indeed, the minimum error strategy is optimal [7]. In the case of unambiguous state identification strategy we can do better. In this latter case the optimum strategy is the following: First we use the Bell state decomposition

$$\begin{aligned} |\psi_i\rangle|\psi_j\rangle \quad = \quad & \cos^2\theta|+\rangle|+\rangle + (-1)^{i+j}\sin^2\theta|-\rangle|-\rangle + \\ & (-1)^i\cos\theta\sin\theta[-\delta_{ij}(|+\rangle|-\rangle + |-\rangle|+\rangle) + \\ & (1-\delta_{ij})(|+\rangle|-\rangle - |-\rangle|+\rangle)]. \end{aligned} \tag{19}$$

If we project successfully onto the antisymmetric state $(|+\rangle|-\rangle - |-\rangle|+\rangle)$, the two states are different. If we project onto the symmetric state $(|+\rangle|-\rangle + |-\rangle|+\rangle)$, both states have to be

identical. If the state is found neither in the symmetric nor in the antisymmetric subspace, it is in one of the two possible states

$$|\Phi_{\pm}\rangle = \frac{\cos^2\theta|+\rangle|+\rangle \pm \sin^2\theta|-\rangle|-\rangle}{\sqrt{1-\frac{1}{2}\sin^2 2\theta}} \tag{20}$$

which can be discriminated unambiguously. Thus, the overall probability for an inconclusive result reads

$$P_?^{comp1} = (1-\frac{1}{2}\sin^2 2\theta)|\langle\Phi_+|\Phi_-\rangle| = \cos 2\theta \tag{21}$$

and

$$P_?^{comp1} < P_?^{comp}. \tag{22}$$

These simple considerations illustrate that the unambiguous method of state comparison is not the optimal one. It can be shown, however, that the two-step method proposed is the optimal one. The interesting aspect of our analysis is that the unambiguous state discrimination may be viewed as a two-step state comparison. First we find out whether the two states are identical or not and afterwards we determine the label.

8 Conclusions

We have demonstrated that totally antisymmetric quantum states are useful for various tasks in quantum information processing. Their special features are particularly useful for implementing multi-partite key-sharing and quantum state sharing protocols and for comparing quantum states. All the applications discussed here rely on the high symmetry and the peculiar correlation properties of these quantum states. It is expected that the future development of multi-partite protocols for quantum information processing will stimulate many more interesting applications of totally antisymmetric quantum states.

Acknowledgments

This work was supported by the European IST-1999-13021 QUIBITS, DLR (CZE00/023) and GAČR (202/01/0318).

References

[1] S. M. Barnett and S. J. D. Phoenix Phys. Rev. A **40** (1989) 2404

[2] Ch. H. Bennett and G. Brassard, Int. Conf. Computers, Systems & Signal Processing, Bangalore, India, (1984) 175

[3] A. Ekert, Phys. Rev. Lett. **67** (1991) 661

[4] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59** (1999) 1829

[5] A. Karlsson, M. Koashi and N. Imoto, Phys. Rev. A **59** (1999) 162

[6] A. Chefles, Contemp. Physics **41** (2000) 401

[7] S. M. Barnett, A. Chefles, I. Jex, quant-phys/0202087