State tomography for two qubits using reduced densities

This article has been downloaded from IOPscience. Please scroll down to see the full text article. 2006 J. Phys. A: Math. Gen. 3910901
(http://iopscience.iop.org/0305-4470/39/34/020)
View the table of contents for this issue, or go to the journal homepage for more

Download details:
IP Address: 171.66.16.106
The article was downloaded on 03/06/2010 at 04:48

Please note that terms and conditions apply.

# State tomography for two qubits using reduced densities 

D Petz ${ }^{1,3}$, K M Hangos ${ }^{2,3}$, A Szántó ${ }^{1,3}$ and F Szöllősi ${ }^{1,3}$<br>${ }^{1}$ Department for Mathematical Analysis, Budapest University of Technology and Economics, H-1521 Budapest, Po Box 91, Hungary<br>${ }^{2}$ Systems and Control Laboratory, Computer and Automation Research Institute, H-1518<br>Budapest, Po Box 63, Hungary

Received 4 May 2006, in final form 13 July 2006
Published 9 August 2006
Online at stacks.iop.org/JPhysA/39/10901


#### Abstract

The optimal state determination (or tomography) is studied for a composite system of two qubits when measurements can be performed on one of the qubits and interactions of the two qubits can be implemented. The goal is to minimize the number of interactions to be implemented. The algebraic method used in the paper leads to an extension of the concept of mutually unbiased measurements.


PACS numbers: $03.67 .-\mathrm{a}, 03.65 . \mathrm{Wj}, 03.65 . \mathrm{Fd}$

## 1. Introduction

An $n$-level quantum system is described by an $n$-dimensional Hilbert space $\mathcal{H}$, or equivalently by the algebra $M_{n}(\mathbb{C})$ of the $n \times n$ complex matrices. When an orthogonal basis of $\mathcal{H}$ is chosen, operators acting on $\mathcal{H}$ correspond to $n \times n$ matrices. A positive operator $\rho$ of trace 1 is called state. If we choose and fix an orthonormal basis $\left\{e_{1}, e_{2}, \ldots, e_{n}\right\}$, then a state $\rho$ is determined by the matrix elements $\rho_{i j}=\left\langle e_{i}\right| \rho\left|e_{j}\right\rangle$. Determination of $\rho$ involves $n^{2}-1$ real parameters, namely, $\rho_{i i}(1 \leqslant i \leqslant n-1)$, $\operatorname{Re} \rho_{i j}$ and $\operatorname{Im} \rho_{i j}(1 \leqslant i<j \leqslant n)$.

A von Neumann measurement on the system is a family $\mathcal{M}=\left\{P_{1}, P_{2}, \ldots, P_{d}\right\}$ of pairwise orthogonal projections such that $\sum_{i} P_{i}=I$. When the measurement $\mathcal{M}$ is performed in the state $\rho$, the outcome $1 \leqslant j \leqslant d$ appears with probability $p_{j}=\operatorname{Tr} \rho P_{i}$ for each $j[6,7]$. Independent measurements on several copies of our quantum system give the relative frequencies $f_{j}$ for each outcome $j$ and $f_{j}$ is an estimate of the probability $p_{j}$. The repeated measurement provides $d-1$ degree of freedom concerning the density $\rho$, since $\sum_{j} p_{j}=1$. The information we obtained is maximal if $d=n$ which means that all the projections $P_{j}$ are of rank 1. $\rho$ is determined by $n^{2}-1$ parameters, hence at least $n+1$ different measurements are to be performed to cover all degrees of freedom. Of course, the $n+1$ different measurements are sufficient in the case when they provide 'non-overlapping' information.

[^0]The literature of state tomography is very rich, there are several protocols, and the efficiency of state reconstruction can be increased if the later measurements depend on the outcomes of the former ones $[1,8,10]$.

The composite system of two qubits is a four-level quantum system which is described on the space $\mathbb{C}^{4} \equiv \mathbb{C}^{2} \otimes \mathbb{C}^{2}$. A state is described by 15 real parameters. Therefore, at least five kinds of elementary measurements should be made to determine the state of the system.

Denote by $A$ and $B$ the two qubits. Then $M_{4}(\mathbb{C})=B\left(\mathcal{H}_{A}\right) \otimes B\left(\mathcal{H}_{B}\right)$, where $B\left(\mathcal{H}_{A}\right)$ and $B\left(\mathcal{H}_{B}\right)$ are isomorphic to $M_{2}(\mathbb{C})$. Assume that we can perform measurements only on the qubit $A$. If the total system has the statistical operator $\rho_{A B}$, then we can reconstruct the reduced density

$$
\rho_{A}^{(1)}:=\operatorname{Tr}_{B} \rho_{A B}
$$

after some measurements. In order to get more information, we switch on an interaction between the two qubits. If $H$ is the Hamiltonian, then the new state is

$$
\begin{equation*}
\mathrm{e}^{\mathrm{i} H} \rho_{A B} \mathrm{e}^{-\mathrm{i} H}=W_{1} \rho_{A B} W_{1}^{*} \tag{1}
\end{equation*}
$$

after the interaction. (For the sake of simplicity, the interaction is kept for a time unit.) The new reduced density is

$$
\rho_{A}^{(2)}:=\operatorname{Tr}_{B} W_{1} \rho_{A B} W_{1}^{*} .
$$

This procedure may be continued by using other interactions and ends with a sequence of reduced states $\rho_{A}^{(1)}, \rho_{A}^{(2)}, \ldots, \rho_{A}^{(k)}$. We want to determine the minimal $k$ such that this sequence of reduced densities determines $\rho_{A B}$. In other words, we want to minimize the number of interactions between the two qubits. It turns out that the minimum number is 5 .

Minimal realizations play an important role in systems theory, too [4], because they represent the state of the system with the minimum possible number of parameters. Minimal realizations are known to be jointly controllable and observable for most of the known system classes. The above problem of finding the minimum number of reduced states can be regarded as a minimal representation problem for a system that consists of a pair of coupled qubits.

If only one qubit is given for state determination, then the minimal number of measurements is 3 . There are many possibilities to choose the three measurements, or equivalently the three bases of the two-dimensional space. It was argued in paper [13] that a complete set of mutually unbiased bases is optimal for state determination. Following this argument [13], we try to find five measurements in the above-described situation of two qubits such that the information obtained should be optimal.

## 2. Algebraic formulation

Instead of the transformation (1) of the density matrix $\rho_{A B}$, we can change the subalgebra and we have an equivalent algebraic formulation. The total system is described by the algebra $M_{4}(\mathbb{C})$. We look for subalgebra $\mathcal{A}_{1}, \mathcal{A}_{2}, \ldots, \mathcal{A}_{k}$ such that
(i) Each $\mathcal{A}_{j}$ is algebraically isomorphic to $M_{2}(\mathbb{C}), 1 \leqslant j \leqslant k$.
(ii) The linear span of the subspaces $\mathcal{A}_{1}, \mathcal{A}_{2}, \ldots, \mathcal{A}_{k}$ is $M_{4}(\mathbb{C})$.

Given a subalgebra $\mathcal{A}_{j}$, there is a unitary $W_{j}$ such that $W_{j}^{*} \mathcal{A}_{j} W_{j}=B\left(\mathcal{H}_{A}\right) \otimes \mathbb{C} I_{B}$. The reduced density $\rho_{j} \in \mathcal{A}_{j}$ is the same as the reduction of $W_{j} \rho_{A B} W_{j}^{*}$ to the first spin. Therefore, instead of the reduction of density after the interaction, we can work with the reduced density of $\rho_{A B}$ in $\mathcal{A}_{j}$. The second condition makes sure that the reduced densities in $\mathcal{A}_{1}, \mathcal{A}_{2}, \ldots, \mathcal{A}_{k}$ determine $\rho_{A B}$ completely.

The traceless subspace of $M_{4}(\mathbb{C})$ has dimension 15 , while the traceless subspace of $\mathcal{A}_{j}$ has dimension 3 , therefore we need $k \geqslant 5$ to fulfil the requirements. It will turn out that $k=5$ is possible.

The algebra $M_{2}(\mathbb{C})$ is linearly spanned by the Pauli matrices:
$\sigma_{0}:=\left[\begin{array}{ll}1 & 0 \\ 0 & 1\end{array}\right], \quad \sigma_{1}:=\left[\begin{array}{ll}0 & 1 \\ 1 & 0\end{array}\right], \quad \sigma_{2}:=\left[\begin{array}{cc}0 & -\mathrm{i} \\ \mathrm{i} & 0\end{array}\right], \quad \sigma_{3}:=\left[\begin{array}{cc}1 & 0 \\ 0 & -1\end{array}\right]$.
Recall that they satisfy the multiplication rules

$$
\begin{equation*}
\sigma_{i} \sigma_{j}=\delta_{i j} I+\mathrm{i} \sum_{k=1}^{3} \epsilon_{i j k} \sigma_{k} \quad(1 \leqslant i, j \leqslant 3) \tag{2}
\end{equation*}
$$

where $\epsilon_{i j k}$ is the Levi-Civita tensor:

$$
\epsilon_{i_{1} i_{2} \cdots i_{n}}= \begin{cases}0 & \text { if } \exists j, k \text { such that } i_{j}=i_{k} \\ 1 & \text { if } \quad \text { the permutation }\left(i_{1} i_{2} \cdots i_{n}\right) \text { is even, } \\ -1 & \text { if } \quad \text { the permutation }\left(i_{1} i_{2} \cdots i_{n}\right) \text { is odd. }\end{cases}
$$

The above rules can be essentially simplified by posing the following two requirements:
(i) $\sigma_{j}$ is a self-adjoint unitary $(1 \leqslant j \leqslant k)$ and $\sigma_{3}=-\mathrm{i} \sigma_{1} \sigma_{2}$.
(ii) $\sigma_{1} \sigma_{2}+\sigma_{2} \sigma_{1}=0$.

When a triplet $\left(S_{1}, S_{2}, S_{3}\right)$ satisfies these condition, it will be called a Pauli triplet. For such a triplet $\operatorname{Tr} S_{i}=0$ and $\operatorname{Tr} S_{i} S_{j}=0$ for $i \neq j$. The latter relation is interpreted as the orthogonality of $S_{i}$ and $S_{j}$ with respect to the Hilbert-Schmidt inner product $\langle A, B\rangle:=\operatorname{Tr} A^{*} B$. Furthermore, it can be seen that the two relations above imply (2).

Given a Pauli triplet ( $S_{1}, S_{2}, S_{3}$ ), the linear mapping defined as

$$
\sigma_{0} \mapsto I, \quad \sigma_{1} \mapsto S_{1}, \quad \sigma_{2} \mapsto S_{2}, \quad \sigma_{3} \mapsto-\mathrm{i} S_{1} S_{2}
$$

is an algebraic isomorphism between $M_{2}(\mathbb{C})$ and the linear span of the operators $I, S_{1}, S_{2}$ and $S_{3}$.

In the algebra $M_{4}(\mathbb{C})$, the elementary tensors $\sigma_{i} \otimes \sigma_{j}$ form an orthogonal basis $(0 \leqslant i, j \leqslant 3)$. All these operators are self-adjoint unitaries and can be chosen to be $S_{i}$ 's.

Proposition 1. There are five subalgebras of $B\left(\mathcal{H}_{A}\right) \otimes B\left(\mathcal{H}_{B}\right)$ such that each of them is isomorphic to $M_{2}(\mathbb{C})$ and the reduced states determine an arbitrary state $\rho_{A B}$ of the two qubits A and B. Moreover, the Pauli triplets of four subalgebras (of the 5) are pairwise orthogonal.

Proof. First we take the following Pauli triplets consisting of elementary tensors:
$\left\{\sigma_{0} \otimes \sigma_{1},-\sigma_{1} \otimes \sigma_{3}, \sigma_{1} \otimes \sigma_{2}\right\}$

$$
=\left\{\left[\begin{array}{llll}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{array}\right],\left[\begin{array}{cccc}
0 & 0 & -1 & 0 \\
0 & 0 & 0 & 1 \\
-1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0
\end{array}\right],\left[\begin{array}{cccc}
0 & 0 & 0 & -\mathrm{i} \\
0 & 0 & \mathrm{i} & 0 \\
0 & -\mathrm{i} & 0 & 0 \\
\mathrm{i} & 0 & 0 & 0
\end{array}\right]\right\},
$$

$\left\{\sigma_{3} \otimes \sigma_{1}, \sigma_{1} \otimes \sigma_{1}, \sigma_{2} \otimes \sigma_{0}\right\}$

$$
=\left\{\left[\begin{array}{cccc}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 \\
0 & 0 & -1 & 0
\end{array}\right],\left[\begin{array}{cccc}
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0
\end{array}\right],\left[\begin{array}{cccc}
0 & 0 & -\mathrm{i} & 0 \\
0 & 0 & 0 & -\mathrm{i} \\
\mathrm{i} & 0 & 0 & 0 \\
0 & \mathrm{i} & 0 & 0
\end{array}\right]\right\}
$$

$\left\{\sigma_{1} \otimes \sigma_{0}, \sigma_{2} \otimes \sigma_{2}, \sigma_{3} \otimes \sigma_{2}\right\}$

$$
=\left\{\left[\begin{array}{llll}
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0
\end{array}\right],\left[\begin{array}{cccc}
0 & 0 & 0 & -1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
-1 & 0 & 0 & 0
\end{array}\right],\left[\begin{array}{cccc}
0 & -\mathrm{i} & 0 & 0 \\
\mathrm{i} & 0 & 0 & 0 \\
0 & 0 & 0 & \mathrm{i} \\
0 & 0 & -\mathrm{i} & 0
\end{array}\right]\right\},
$$

$\left\{\sigma_{0} \otimes \sigma_{2}, \sigma_{2} \otimes \sigma_{3}, \sigma_{2} \otimes \sigma_{1}\right\}$

$$
=\left\{\left[\begin{array}{cccc}
0 & -\mathrm{i} & 0 & 0 \\
\mathrm{i} & 0 & 0 & 0 \\
0 & 0 & 0 & -\mathrm{i} \\
0 & 0 & \mathrm{i} & 0
\end{array}\right],\left[\begin{array}{cccc}
0 & 0 & -\mathrm{i} & 0 \\
0 & 0 & 0 & \mathrm{i} \\
\mathrm{i} & 0 & 0 & 0 \\
0 & -\mathrm{i} & 0 & 0
\end{array}\right],\left[\begin{array}{cccc}
0 & 0 & 0 & -\mathrm{i} \\
0 & 0 & -\mathrm{i} & 0 \\
0 & \mathrm{i} & 0 & 0 \\
\mathrm{i} & 0 & 0 & 0
\end{array}\right]\right\} .
$$

Together with the identity, each triplet linearly spans a subalgebra $\mathcal{A}_{j}(1 \leqslant j \leqslant 4)$. It is important to observe that all the matrices have a vanishing diagonal; moreover the matrices are pairwise orthogonal; therefore they are linearly independent. An orthogonal Pauli triplet does not exist, since the orthogonal complement of the subalgebras $\mathcal{A}_{j}(1 \leqslant j \leqslant 4)$ is a commutative algebra.

If we find another Pauli triplet $\left(S_{1}, S_{2}, S_{3}\right)$ such that the diagonals are linearly independent, then we have a fifth algebra $\mathcal{A}_{5}$ such that $\left\{\mathcal{A}_{k}: 1 \leqslant k \leqslant 5\right\}$ spans linearly $M_{4}(\mathbb{C})$. Indeed, if $A$ is any matrix, then we can find $T \in \mathcal{A}_{5}$ such that $A-T$ has 0 diagonal and this is in the linear hull of $\left\{\mathcal{A}_{j}: 1 \leqslant j \leqslant 4\right\}$. It follows that the reduced densities in $\left\{\mathcal{A}_{j}: 1 \leqslant j \leqslant 5\right\}$ determines $\rho_{A B}$ uniquely.

Here is an example of the above-described triplet:
$\frac{1}{2}\left[\begin{array}{cccc}1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1\end{array}\right], \quad \frac{1}{2}\left[\begin{array}{cccc}1 & \mathrm{i} & \mathrm{i} & -1 \\ -\mathrm{i} & -1 & -1 & \mathrm{i} \\ -\mathrm{i} & -1 & 1 & -\mathrm{i} \\ -1 & -\mathrm{i} & \mathrm{i} & -1\end{array}\right], \quad \frac{1}{2}\left[\begin{array}{cccc}-1 & \mathrm{i} & 1 & \mathrm{i} \\ -\mathrm{i} & 1 & \mathrm{i} & 1 \\ 1 & -\mathrm{i} & 1 & \mathrm{i} \\ -\mathrm{i} & 1 & -\mathrm{i} & -1\end{array}\right]$.
These matrices are not elementary tensors (but they are Hadamard matrices [11] up to a constant multiple and were found by means of an exhaustive search algorithm on a computer for curiosity). If we do not insists on a very particular triplet, then we can get one by a random selection [3].

If we only want to find linearly independent Pauli triplets, we can make random selection successfully with large probability. The triplets

$$
\left(W_{i}\left(\sigma_{1} \otimes \sigma_{0}\right) W_{i}^{*}, W_{i}\left(\sigma_{2} \otimes \sigma_{0}\right) W_{i}^{*}, W_{i}\left(\sigma_{3} \otimes \sigma_{0}\right) W_{i}^{*}\right)
$$

are linearly independent if the unitaries $W_{1}, \ldots, W_{5}$ are chosen independently and randomly (according to the Haar measure on the unitary group). Our simulation written in the Maple package can be seen in [3].

Proposition 2. If all the matrices of the Pauli triplet generating the subalgebras $\mathcal{A}_{j}$ are of the form $\pm \sigma_{k} \otimes \sigma_{l}(0 \leqslant k, l \leqslant 3)$, then we need at least six triplets to span $M_{4}(\mathbb{C})$.

Proof. Assume that a Pauli triplet $\left(T_{1}, T_{2}, T_{3}\right)$ in $M_{4}(\mathbb{C})$ is such that every element is of the form $\pm \sigma_{i} \otimes \sigma_{j}(0 \leqslant i, j \leqslant 3)$.

If $T_{1}= \pm \sigma_{i} \otimes \sigma_{j}$ and $T_{2}= \pm \sigma_{k} \otimes \sigma_{l}$, then

$$
\begin{aligned}
\pm \mathrm{i} T_{3}=-\sum_{m, n} & \left(\epsilon_{i k m} \epsilon_{j l n} \sigma_{m} \otimes \sigma_{n}\right) \\
& +\mathrm{i}\left(\delta_{i k} \sum_{n}\left(\epsilon_{j l n} \sigma_{0} \otimes \sigma_{n}\right)+\delta_{j l} \sum_{m}\left(\epsilon_{i k m} \sigma_{m} \otimes \sigma_{0}\right)\right)+\delta_{i k} \delta_{j l} \sigma_{0} \otimes \sigma_{0}
\end{aligned}
$$

Since $T_{3}$ is self-adjoint but $\sigma_{i} \otimes \sigma_{j}$ is not, it follows that exactly one of the relations $i=k$ and $j=l$ must hold. At least one of the operators $T_{i}$ should be of the form $\sigma_{0} \otimes \sigma_{j}$ or $\sigma_{j} \otimes \sigma_{0}$.

We have three operators in the form $\sigma_{0} \otimes \sigma_{j}$ and three in the form $\sigma_{j} \otimes \sigma_{0}(1 \leqslant j \leqslant 3)$. If we have five Pauli triplets, then at least one should contain two of the above tensor products (up to a sign). One can see that $\sigma_{0} \otimes \sigma_{j}$ and $\sigma_{i} \otimes \sigma_{0}$ cannot be in a triplet; therefore a triplet contains two operators in the form $\sigma_{0} \otimes \sigma_{j}$ or two operators like $\sigma_{j} \otimes \sigma_{0}$. In both cases, the third operator has similar form. Hence one of the operators $\sigma_{0} \otimes \sigma_{j}$ and $\sigma_{j} \otimes \sigma_{0}$ appears in two triplets and in this case five triplets cannot span the whole space.

Six subalgebras described in the proposition can be given by the following Pauli triplets:

$$
\begin{align*}
& \left\{\sigma_{1} \otimes \sigma_{1}, \sigma_{1} \otimes \sigma_{2}, \sigma_{0} \otimes \sigma_{3}\right\} \\
& \left\{\sigma_{2} \otimes \sigma_{2}, \sigma_{2} \otimes \sigma_{3}, \sigma_{0} \otimes \sigma_{1}\right\} \\
& \left\{\sigma_{3} \otimes \sigma_{3}, \sigma_{3} \otimes \sigma_{1}, \sigma_{0} \otimes \sigma_{2}\right\} \\
& \left\{\sigma_{2} \otimes \sigma_{2}, \sigma_{3} \otimes \sigma_{2}, \sigma_{1} \otimes \sigma_{0}\right\}  \tag{3}\\
& \left\{\sigma_{3} \otimes \sigma_{3}, \sigma_{1} \otimes \sigma_{3}, \sigma_{2} \otimes \sigma_{0}\right\} \\
& \left\{\sigma_{1} \otimes \sigma_{1}, \sigma_{2} \otimes \sigma_{1}, \sigma_{3} \otimes \sigma_{0}\right\}
\end{align*}
$$

Together with $I$ each triplet linearly spans a subalgebra $\mathcal{A}_{j}(1 \leqslant j \leqslant 6)$ and the six subalgebras linearly span the whole $M_{2}(\mathbb{C}) \otimes M_{2}(\mathbb{C})$.

The orthogonality of the Pauli triplets shows analogy with the mutually unbiased bases. This is discussed in the next section.

## 3. Generalizations

Mutually unbiased bases (or measurements) are interesting from many point of view [2, 5, 13] and the maximal number of such bases is not completely known [12]. The above-discussed setting of state determination is somewhat similar. In this setting we may look for essentially orthogonal non-commutative subalgebras while unbiased elementary measurements are given by essentially orthogonal maximal Abelian subalgebras, see proposition 2.2 of [9]. The next statement is an analogue of Parthasarathy's proposition.

Proposition 3. Let $\mathcal{A}_{1}$ and $\mathcal{A}_{2}$ be subalgebras of $M_{n}(\mathbb{C})$ and assume that they are isomorphic to $M_{k}(\mathbb{C})$. Then the following conditions are equivalent:
(i) If $P \in \mathcal{A}_{1}$ and $Q \in \mathcal{A}_{2}$ are minimal projections, then $\operatorname{Tr} P Q=n / k^{2}$.
(ii) The subspaces $\mathcal{A}_{1} \ominus \mathbb{C} I$ and $\mathcal{A}_{2} \ominus \mathbb{C} I$ are orthogonal in $M_{n}(\mathbb{C})$.

Proof. It follows from the conditions that $n=m k$ and $\operatorname{Tr} P=\operatorname{Tr} Q=m$ for the minimal projections. Therefore, condition (i) is equivalent to $\operatorname{Tr}(I-k P)(I-k Q)=0$ which means that $(I-k P) \perp(I-k Q)$. Since the subspaces in (ii) are linearly spanned by these operators, the proposition follows.

Now we generalize Proposition 2 for $n$ qubits.
Proposition 4. If all the matrices of the Pauli triplet generating the subalgebras $\mathcal{A}_{j}$ of $M_{2^{n}}(\mathbb{C})$ are of the form $\pm \sigma_{k(1)} \otimes \cdots \otimes \sigma_{k(n)}(0 \leqslant k(i) \leqslant 3,1 \leqslant i \leqslant n)$, then we need more than $\left(2^{2 n}-1\right) / 3$ triplets to span $M_{2^{n}}(\mathbb{C})$.

Proof. First note that a matrix $\pm \sigma_{k(1)} \otimes \cdots \otimes \sigma_{k(n)}$ has only real elements or only imaginary elements. Among the three matrices of a Pauli triplet $\left(T_{1}, T_{2}, T_{3}\right)$, there is one imaginary or there are three imaginary matrices. Let $N$ be the number of triplets with one imaginary matrix and $M$ be the number of triplets with three imaginary ones. If the $N+M$ triplets with identity linearly span the self-adjoint subspace, then $3(N+M)+1 \geqslant 2^{2 n}$. Assume that

$$
\begin{equation*}
N+M=\frac{2^{2 n}-1}{3} . \tag{4}
\end{equation*}
$$

Since the dimension of the subspace of self-adjoint matrices with imaginary elements is $\left(2^{2 n}-2^{n}\right) / 2$, we must have

$$
\begin{equation*}
N+3 M=\frac{2^{2 n}-2^{n}}{2} \tag{5}
\end{equation*}
$$

One can see that equations (4) and (5) do not have integer solution.
We call a family $\mathcal{M}_{1}, \mathcal{M}_{2}, \ldots, \mathcal{M}_{d}$ of subalgebras mutually unbiased if the conditions in Proposition 3 hold for any pair. The maximal number of mutually unbiased subalgebras is not known to us even in the simplest case when the large algebra is $M_{4}(\mathbb{C})$ and the subalgebras are isomorphic to $M_{2}(\mathbb{C})$.

## 4. Discussion and conclusions

The optimal state tomography has been studied for a composite system of two qubits when measurements can be performed on one of the qubits and interactions of the two qubits can be implemented. Equivalently, we found physically realizable minimal set of reduced densities determined by Pauli triplets. The transformation described by (1) is realized by a properly designed measurement apparatus (see the experimental devices in [10]).

The construction of five Pauli triplets of $4 \times 4$ matrices from the tensor products of Pauli matrices contains heuristic steps as far as the orthogonal part is concerned. In our construction four triplets are orthogonal and the fifth is only linearly independent. It is not known to us if five orthogonal Pauli triplets exist. (The number of pairwise orthogonal Pauli triplets can be asked for more qubits.)

The orthogonality is motivated by the work of Wootters and Field [13]. Their work leads naturally to the concept of unbiased subalgebras. One can expect that the argument of [13] extends to our situation and the unbiased subalgebras provide more information than the simply linearly independent ones during state determination. This subject will be investigated in a forthcoming paper.

## References

[^1][4] Isidoni A 1995 Nonlinear Control Systems (Berlin: Springer)
[5] Kraus K 1987 Complementarity and uncertainty relations Phys. Rev. D 35 3070-5
[6] Nielsen M A and Chuang I L 2000 Quantum Computation and Quantum Information (Cambridge: Cambridge University Press)
[7] Ohya M and Petz D 1993 Quantum Entropy and its Use (Berlin: Springer)
[8] Paris M G A and Rehácek J (ed) 2004 Quantum State Estimation (Lecture Notes in Physics) (Berlin: Springer)
[9] Parthasarathy K R 2004 On estimating the state of a finite level quantum system Infin. Dimens. Anal. Quantum Probab. Relat. Top. 7 607-17
[10] Rehácek J, Englert B and Kaszlikowski D 2004 Minimal qubit tomography Phys. Rev. A 70052321
[11] Tadej W and Zyczkowski K 2005 A concise guide to complex Hadamard matrices Preprint quant-ph/0512154
[12] Werner R http://www.imaph.tu-bs.de/qi/problems/13.html
[13] Wootters W K and Fields B D 1989 Optimal state determination by mutually unbiased measurements Ann. Phys., NY 191 363-81


[^0]:    ${ }^{3}$ Supported by the Hungarian Research Grants OTKA T042710, T063066 and T032662.

[^1]:    [1] Bergou J A, Buzek V, Feldman E, Herzog U and Hillery M 2006 Programmable quantum state discriminators with simple programs Preprint quant-ph/0602164
    [2] Boykin P O, Sitharam M, Tiep P H and Wocjan P 2005 Mutually unbiased bases and orthogonal decompositions of Lie algebras Preprint quant-ph/0506089
    [3] Hangos K M 2006 Systems and control methods for quantum systems, http://daedalus.scl.sztaki.hu/PCRG/ quantum

