## General sequential quantum cloning

This article has been downloaded from IOPscience. Please scroll down to see the full text article.
2008 J. Phys. A: Math. Theor. 41155303
(http://iopscience.iop.org/1751-8121/41/15/155303)
View the table of contents for this issue, or go to the journal homepage for more

Download details:
IP Address: 171.66.16.148
The article was downloaded on 03/06/2010 at 06:43

Please note that terms and conditions apply.

# General sequential quantum cloning 

Gui-Fang Dang and Heng Fan<br>Institute of Physics, Chinese Academy of Sciences, Beijing 100080, People's Republic of China

Received 20 November 2007, in final form 27 February 2008
Published 2 April 2008
Online at stacks.iop.org/JPhysA/41/155303


#### Abstract

Some multipartite quantum states can be generated in a sequential manner which may be implemented by various physical setups such as microwave and optical cavity QED, trapped ions, quantum dots, etc. We analyze the general $N$ to $M(N \leqslant M)$ qubits' universal quantum cloning machine (UQCM) within a sequential generation scheme. We show that the $N$ to $M$ sequential UQCM is available. The case of $d$-level quantum states' sequential cloning is also presented.


PACS numbers: 03.67.Mn, 03.65.Ud, 42.50.Dv

Quantum entanglement plays a key role in quantum computation and quantum information [1]. Multipartite entangled states arise as a resource for quantum information processing tasks such as the well-known quantum teleportation [2], quantum communication [3, 4], clock synchronization [5], etc. In general, it is extremely difficult to generate experimentally multipartite entangled states through single global unitary operations. In this sense, the sequential generation of the entangled states appears to be promising. Actually, most of the quantum computation networks are designed to implement quantum logic gates through a sequential procedure [6]. Recently, sequential implementation of quantum information processing tasks has been attracting much attention. It is pointed out that photonic multiqubit states can be generated by letting a source emit photonic qubits in a sequential manner [7]. The general sequential generation of entangled multiqubit states in the realm of cavity QED was systematically studied in $[8,9]$. It is also shown that the class of sequentially generated states is identical to the matrix-product state (MPS), which is very useful in the study of spin chains of condensed matter physics [10].

On the other hand, much progress has already been made in the past few years in studying quantum cloning machines; for reviews see, for example, [11-13]. Various quantum cloning machines have been implemented experimentally by polarization of photons [14-18], nuclear spins in nuclear magnetic resonance [19, 20], etc. However, these experiments are for 1 to 2 (one-qubit input and two-qubit output) or 1 to 3 cloning machines. The more general case will be much more difficult. There are some schemes proposed for the general quantum cloning machines which are not in a sequential manner; see, for example, [21, 22]. Recently, a 1 to $M$ sequential universal quantum cloning is proposed [23] by using the cloning transformation presented in [24]. Since it is in a sequential procedure, potentially it reduces the difficulty
in implementing this quantum cloning machine. However, as is well known the collective quantum cloning machine (the $N$ identical input states are cloned collectively to $M$ copies) is better than the quantum cloning machine which can only deal with the individual input (only one input is copied to several copies each time). We know that the general $N$ to $M$ cloning transformation is also available in [24,25]. Then a natural question arises: whether the general $N$ to $M$ sequential cloning machine is possible? In this paper, we will present the general sequential universal quantum cloning machine.

The 1 to $M$ cloning transformations used in [23] was proposed by Gisin and Massar in [24]. The $N$ to $M$ universal quantum cloning machine (UQCM) was also presented in [24]. However, to use the method proposed in $[8,23]$ to find the sequential cloning machine, the input state $|\Phi\rangle^{\otimes N}$ should be expanded in computational basis $\{|0\rangle,|1\rangle\}$. The explicit quantum cloning transformations with this kind of input were proposed by Fan et al in [25]. In this paper, based on the result of [23,25], the general sequential UQCM will be presented.

As presented in [8, 23], the sequential generation of a multiqubit state is as follows. Let $\mathcal{H}_{\mathcal{A}}$ be a $D$-dimensional Hilbert space which acts as the ancillary system and a single qubit (e.g., a time-bin qubit) is in a two-dimensional Hilbert space $\mathcal{H}_{\mathcal{B}}$. In every step of the sequential generation of a multiqubit state, a unitary time evolution will be acting on the joint system $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$. We assume that each qubit is initially in the state $|0\rangle$ which is like a blank or an empty state and will not be written out in the formulae. So the unitary time evolution is written in the form of an isometry $V: \mathcal{H}_{\mathcal{A}} \rightarrow \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$, where $V=\sum_{i, \alpha, \beta} V_{\alpha, \beta}^{i}|\alpha, i\rangle\langle\beta|$, each $V^{i}$ is a $D \times D$ matrix and the isometry condition takes the form $\sum_{i=0}^{1} V^{i \dagger} V^{i}=1$. By successively applying $n$ operations of $V$ (not necessarily the same) on an initial ancillary state $\left|\phi_{I}\right\rangle \in \mathcal{H}_{\mathcal{A}}$, we obtain $|\Psi\rangle=V^{[n]} \ldots V^{[2]} V^{[1]}\left|\phi_{I}\right\rangle$. The generated $n$ qubits are in general an entangled state, but the last step qubit-ancilla interaction can be chosen so as to decouple the final multiqubit entangled state from the auxiliary system; so the sequentially generated state is

$$
\begin{equation*}
|\psi\rangle=\sum_{i_{1} \ldots i_{n}=0}^{1}\left\langle\phi_{\mathrm{F}}\right| V^{[n] i_{n}} \ldots V^{[1] i_{1}}\left|\phi_{I}\right\rangle\left|i_{n}, \ldots, i_{1}\right\rangle, \tag{1}
\end{equation*}
$$

where $\left|\phi_{\mathrm{F}}\right\rangle$ is the final state of the ancilla. This is the MPS. It was proven that any MPS can be sequentially generated [8].

Suppose that there are $N$ identical pure quantum states $|\Phi\rangle^{\otimes N}=\left(x_{0}|0\rangle+x_{1}|1\rangle\right)^{\otimes N}$ which need to be cloned to $M$ copies, where $\left|x_{0}\right|^{2}+\left|x_{1}\right|^{2}=1$. We know that the input state can be represented by a basis in symmetric subspace

$$
\begin{equation*}
|\Phi\rangle^{\otimes N}=\sum_{m=0}^{N} x_{0}^{N-m} x_{1}^{m} \sqrt{C_{N}^{m}}|(N-m) 0, m 1\rangle, \tag{2}
\end{equation*}
$$

where $|(N-m) 0, m 1\rangle$ denotes the symmetric and normalized state with $(N-m)$ qubits in the state $|0\rangle$ and $m$ qubits in the state $|1\rangle$, and we have $C_{N}^{m}=N!/(N-m)!m!$ in standard notation. So if we find the quantum cloning transformations for all states in symmetric subspace, we can clone $N$ pure states to $M$ copies. The UQCM with input in symmetric subspace can be written as [25]

$$
\begin{equation*}
|(N-m) 0, m 1\rangle \rightarrow\left|\Phi_{M}^{m}\right\rangle \tag{3}
\end{equation*}
$$

where

$$
\begin{equation*}
\left|\Phi_{M}^{m}\right\rangle=\sum_{j=0}^{M-N} \beta_{m j}|(M-m-j) 0,(m+j) 1\rangle \otimes R_{j} \tag{4}
\end{equation*}
$$

$$
\begin{equation*}
\beta_{m j}=\sqrt{C_{M-m-j}^{M-N-j} C_{(m+j)}^{j} / C_{M+1}^{N+1}} \tag{5}
\end{equation*}
$$

where $R_{j}$ are the ancillary states of the cloning machine and are orthogonal with each other for different $j$. For a sequential quantum cloning machine in this paper, we choose a realization $R_{j} \equiv|(M-N-j) 1, j 0\rangle$ for the ancilla states. This UQCM is optimal in the sense that the fidelity between the single qubit output state reduced density operator $\rho_{\text {reduced }}^{\text {out }}$ and the single input $|\Phi\rangle$ is optimal. The optimal fidelity is $F=\langle\Phi| \rho_{\text {reduced }}^{\text {out }}|\Phi\rangle=(M N+M+N) / M(N+2)$; see [11-13] for reviews and the references therein. A realization of this UQCM with photonstimulated emission can be found in [22] which is not in a sequential manner. Next we show that this general $N$ to $M$ UQCM can be generated through a sequential procedure.

The basic idea is to show that the final state of the cloning, $\left|\Phi_{M}^{m}\right\rangle$ in (4), can be expressed in its MPS form. As shown in [8], any MPS can be sequentially generated. We shall follow the method, for example, as in [23, 26]. By Schmidt decomposition, we first express the quantum state $\left|\Phi_{M}^{m}\right\rangle$ as a bi-partite state across $1: 2 \ldots$ cut,

$$
\begin{align*}
\left|\Phi_{M}^{m}\right\rangle & =\lambda_{1}^{[1]}|0\rangle\left|\phi_{1}^{[2 \ldots(2 M-N)]}\right\rangle+\lambda_{2}^{[1]}|1\rangle\left|\phi_{2}^{[2 \ldots(2 M-N)]}\right\rangle \\
& =\sum_{\alpha_{1} i_{1}} \Gamma_{\alpha_{1}}^{[1] i_{1}} \lambda_{\alpha_{1}}^{[1]}\left|i_{1}\right\rangle\left|\phi_{\alpha_{1}}^{[2 \ldots(2 M-N)]}\right\rangle, \tag{6}
\end{align*}
$$

where $\Gamma_{\alpha_{1}}^{[1]]}=\delta_{\alpha_{1}, 1}, \Gamma_{\alpha_{1}}^{[1] 1}=\delta_{\alpha_{1}, 2}$, and $\lambda_{\alpha_{1}}^{[1]}$ are eigenvalues of the first qubit reduced density operator, and we find $\lambda_{1}^{[1]}=\sqrt{\sum_{k=-m}^{M-m-1} \beta_{m k}^{2} C_{M-1}^{m+k} / C_{M}^{m+k}}, \lambda_{2}^{[1]}=$ $\sqrt{\sum_{k=-m}^{M-m-1} \beta_{m(k+1)}^{2} C_{M-1}^{m+k} / C_{M}^{m+k+1}}$. To correspond with the MPS in (1), we can define $V_{\alpha_{1}}^{[1] i_{1}}=\Gamma_{\alpha_{1}}^{[1] i_{1}} \lambda_{\alpha_{1}}^{[1]}$. Successively by Schmidt decomposition, the quantum state $\left|\Phi_{M}^{m}\right\rangle$ in (4) is divided into a bi-partite state with the first $n$ qubits as one part and the rest as another part, where $1<n \leqslant M-1$. We find

$$
\begin{equation*}
\left|\Phi_{M}^{m}\right\rangle=\sum_{j=0}^{n^{\prime}} \lambda_{j+1}^{[n]}|(n-j) 0, j 1\rangle\left|\phi_{j+1}^{[(n+1) \ldots(2 M-N)]}\right\rangle, \tag{7}
\end{equation*}
$$

when $1<n \leqslant M-N+m, n^{\prime}=n$; when $M-N+m<n \leqslant M-1, n^{\prime}=M-N+m, \lambda_{j+1}^{[n]}$ are eigenvalues of the first $n$ qubits reduced density operator of $\left|\Phi_{M}^{m}\right\rangle$. According to the results in equations (4) and (5), we can obtain

$$
\begin{equation*}
\lambda_{j+1}^{[n]}=\sqrt{C_{n}^{j} \sum_{k=-m}^{M-m-n} \beta_{m(j+k)}^{2} \frac{C_{M-n}^{m+k}}{C_{M}^{m+j+k}}} \tag{8}
\end{equation*}
$$

We also have
$\left|\phi_{j+1}^{[(n+1) \ldots(2 M-N)]}\right\rangle=\frac{\sqrt{C_{n}^{j}}}{\lambda_{j+1}^{[n]}} \sum_{k=-m}^{M-m-n} \beta_{m(j+k)}^{2} \sqrt{\frac{C_{M-n}^{(m+k)}}{C_{M}^{m+j+k}}|(M-n-m-k) 0,(m+k) 1\rangle \otimes R_{j+k} .}$
By induction and a concise formula, we have

$$
\begin{align*}
\left|\phi_{j+1}^{[n \ldots(2 M-N)]}\right\rangle & =\sum_{\alpha_{n}, i_{n}} \Gamma_{(j+1) \alpha_{n}}^{[n] i_{n}} \lambda_{\alpha_{n}}^{[n]}\left|i_{n}\right\rangle\left|\phi_{\alpha_{n}}^{[(n+1) \ldots(2 M-N)]}\right\rangle \\
& =\frac{\sqrt{C_{n-1}^{j}}}{\lambda_{j+1}^{[n-1]}}\left[|0\rangle\left|\phi_{j+1}^{[(n+1) \ldots(2 M-N)]}\right\rangle \frac{\lambda_{j+1}^{[n]}}{\sqrt{C_{n}^{j}}}+|1\rangle\left|\phi_{j+2}^{[(n+1) \ldots(2 M-N)]}\right\rangle \frac{\lambda_{j+2}^{[n]}}{\sqrt{C_{n}^{j+1}}}\right] \tag{9}
\end{align*}
$$

where we denote

$$
\begin{align*}
& \Gamma_{(j+1) \alpha_{n}}^{[n] 0}=\delta_{(j+1) \alpha_{n}} \sqrt{C_{n-1}^{j}} /\left(\lambda_{j+1}^{[n-1]} \sqrt{C_{n}^{j}}\right),  \tag{10}\\
& \Gamma_{(j+1) \alpha_{n}}^{[n] 1}=\delta_{(j+2) \alpha_{n}} \sqrt{C_{n-1}^{j}} /\left(\lambda_{j+1}^{[n-1]} \sqrt{C_{n}^{j+1}}\right) . \tag{11}
\end{align*}
$$

Still, we define that

$$
\begin{equation*}
V_{\alpha_{n} \alpha_{n-1}}^{[n] i_{n}}=\Gamma_{\alpha_{n-1} \alpha_{n}}^{[n] i_{n}} \lambda_{\alpha_{n}}^{[n]} . \tag{12}
\end{equation*}
$$

It is thus in the MPS representation. We can further consider other cases including the ancilla state of the cloning machine represented as $R_{j}$ (note that it is not the ancilla state in the MPS representation). We can find that the output state of the general UQCM can be expressed as a MPS as in form (1). So it can be created sequentially. The explicit results are summarized in the appendix.

We have shown that the output states of the general UQCM in (4) and (5) are MPSs and thus can be generated sequentially. The sequential matrices $V^{[n]}$ of course depend on the input $|(N-m) 0, m 1\rangle$, which are $W$-like states and are generally multiqubit entangled. For later convenience, we denote $V(m)$ to express that it depends on the the input state for different $m$. By a straightforward method, the sequential cloning operation, i.e. the isometrices, depending on different inputs may take the form $\sum_{m}|(N-m) 0, m\rangle\langle(N-m) 0, m 1| \otimes V(m)$. However, this operation may need a single global unitary operator which involves $N$-qubit entangled states except for $m=0, m=N$. This contradicts with our aim that each operation should be divided into sequential unitary operators in a quDit (quantum state in $D$-dimensional space) times qubit system. Here, we can use a scheme as follows: the ancillary state interacts with each qubit according to the $(N+1) \times D$-dimensional isometrices as $\sum_{m} \sqrt{C_{N}^{m}}|0\rangle\left\langle\left. 0\right|^{\otimes N-m} \otimes \mid 1\right\rangle\left\langle\left. 1\right|^{\otimes m} \otimes V(m)\right.$ sequentially; here a whole normalization factor is omitted. We know that the operation $|0\rangle\left\langle\left. 0\right|^{\otimes N-m} \otimes \mid 1\right\rangle\left\langle\left. 1\right|^{\otimes m}\right.$ acts on each qubit individually. Thus, this scheme reduces the complexity of the operation. This finishes our general sequential UQCM for the case of qubit. In the case $N=1$, we recover the result of [23] for 1 to $M$ cloning. We should remark that similar as the case of sequential 1 to $M$ UQCM in [23], for the general sequential UQCM, the minimal dimension $D$ of the ancillary state grows linearly at most with $M-N / 2+1$ for even $N$ or $M-(N-1) / 2$ for odd $N$.

Next, we will consider a more general case that the sequential cloning machine is about the quantum state in $d$-dimensional Hilbert space. We will use the $d$-dimensional UQCM proposed by Fan et al in [25]. This UQCM is a generalization of the cloning machine proposed in [24] and we can use this UQCM to study its sequential form for the $d$-dimensional case.

An arbitrary $d$-dimensional pure state takes the form $|\Phi\rangle=\sum_{i=0}^{d-1} x_{i}|i\rangle$ with $\sum_{i=0}^{d-1}\left|x_{i}\right|^{2}=$ 1. $N$ identical pure states can be expanded in terms of state in symmetric subspace $|\Phi\rangle^{\otimes N}=\sum_{\vec{m}=0}^{N} \sqrt{\frac{N!}{m_{1}!\ldots m_{d}!}} x_{0}^{m_{1}} \ldots x_{d-1}^{m_{d}}|\vec{m}\rangle$, where $|\vec{m}\rangle \equiv\left|m_{1}, \ldots, m_{d}\right\rangle$ is a symmetric state with $m_{i}$ states of $|i-1\rangle$, and also $m_{i}$ should satisfy a relation $\sum_{i=1}^{d} m_{i}=N$. The cloning transformations with states in the symmetric subspace can be written as

$$
\begin{align*}
& |\vec{m}\rangle \rightarrow\left|\Phi_{M}^{\vec{m}}\right\rangle=\sum_{\vec{j}=0}^{M-N} \beta_{\vec{m} j}|\vec{m}+\vec{j}\rangle \otimes|\vec{j}\rangle,  \tag{13}\\
& \beta_{\vec{m} \vec{j}}=\sqrt{\frac{\prod_{i=1}^{d} C_{m_{i}+j}^{j}}{C_{M+d-1}},} \tag{14}
\end{align*}
$$

where $\vec{j}$ should satisfy $\sum_{i} j_{i}=M-N$. This cloning machine is optimal and the corresponding fidelity of a single quantum state between the input and output is $F=$ $(N(d+M)+M-N) /(d+N) M$.

As for a $d$-dimensional system, we next show that the output states for all symmetric states input can be expressed as the sequential form. We consider the case $1<n \leqslant M-1$, and the state $\left|\Phi_{M}^{\vec{m}}\right\rangle$ is a bipartite state across $1, \ldots, n:(n+1) \ldots$ cut,

$$
\begin{equation*}
\left|\Phi_{M}^{\vec{m}}\right\rangle=\sum_{\vec{j}=0}^{M} \sum_{\vec{k}=0}^{M-n} \lambda_{\vec{j}}^{[n]}|\vec{j}\rangle\left|\phi_{\vec{j}}^{[(n+1) \ldots(2 M-N)]}\right\rangle \tag{15}
\end{equation*}
$$

where

$$
\begin{align*}
& \lambda_{\vec{j}}^{[n]}=\sqrt{\sum_{\vec{k}=0}^{M-n} \beta_{\vec{m}(\vec{j}-\vec{m}+\vec{k})}^{2} \frac{\prod_{i=1}^{d} C_{j_{i}+k_{i}}^{j_{i}}}{C_{M}^{n}}},  \tag{16}\\
& \left|\phi_{\vec{j}}^{[(n+1) \ldots(2 M-N)]}\right\rangle=\sum_{\vec{k}=0}^{M-n} \beta_{\vec{m}(\vec{j}-\vec{m}+\vec{k})} \sqrt{\frac{\prod_{i=1}^{d} C_{j_{i}+k_{i}}^{j_{i}}}{C_{M}^{n}}|\vec{k}\rangle|\vec{j}-\vec{m}+\vec{k}\rangle / \lambda_{\vec{j}}^{[n]} .} \tag{17}
\end{align*}
$$

By the same procedure as that of the qubit case, we can obtain the following:

$$
\begin{equation*}
\left|\phi_{j}^{[n \ldots(2 M-N)]}\right\rangle=\sum_{\alpha_{n} i_{n}} \Gamma_{j \alpha_{n}}^{[n] i_{n}} \lambda_{\alpha_{n}}^{[n]}\left|i_{n}\right\rangle\left|\phi_{\alpha_{n}}^{(n+1) \ldots(2 M-N)]}\right\rangle \tag{18}
\end{equation*}
$$

Then we have

$$
\begin{equation*}
\Gamma_{j \alpha_{n}}^{[n] i_{n}}=\delta_{\alpha_{n}\left(\vec{j}+\overrightarrow{e_{i n}+1}\right)} \sqrt{\frac{j_{i_{n}+1}+1}{n}} / \lambda_{\vec{j}}^{[n-1]} . \tag{19}
\end{equation*}
$$

Still we can define $V_{\alpha_{n} \alpha_{n-1}}^{[n] i_{n}}=\Gamma_{\alpha_{n-1} \alpha_{n}}^{[n] i_{n}} \lambda_{\alpha_{n}}^{[n]}$, and thus we can find that each state $\left|\Phi_{M}^{\vec{m}}\right\rangle$ is a MPS and thus can be sequentially generated. The detailed result of this part will be presented elsewhere [27].

In conclusion, we show that the general $N$ to $M$ universal quantum cloning machine can be implemented by a sequential manner. This general sequential quantum cloning machine may be implemented much more easily than the single global implementation scheme, since the sequential generation of a multipartite state can be implemented in various physical setups such as microwave and optical cavity QED, trapped ions, quantum dots, etc. This reduces dramatically the complexity in implementing the general UQCM. We also show that for $d$-dimensional quantum state, the sequential UQCM is also available. Besides the universal cloning machine, the 1 to $M$ phase-covariant quantum cloning machine can also be sequentially implemented. It will be interesting to consider similarly the general $N$ to $M$ phase-covariant cloning and the economic phase-covariant cloning. The sequential asymmetric quantum cloning machine may also be an interesting topic.

## Acknowledgments

HF was supported by 'Bairen’ program, NSFC and '973' program (2006CB921107).

## Appendix

The explicit forms of matrices $V$ are presented as

$$
V_{\alpha_{n} \alpha_{n-1}}^{[n] 0}=\delta_{\alpha_{n} \alpha_{n-1}}\left(\frac{\sum_{k=-m}^{M-m-n} X \frac{C_{M-n}^{m+k}}{C_{M}^{m+\alpha_{n}-1+1+k}}}{\sum_{k=-m}^{M-m+n+1} X \frac{C_{M-n+1}^{m+k}}{C_{M}^{m+\alpha_{n}-1-1+k}}}\right)^{1 / 2}
$$

$$
V_{\alpha_{n} \alpha_{n-1}}^{[n] 0}=\delta_{\alpha_{n} \alpha_{n-1}+1}\left(\frac{\sum_{k=-m}^{M-m-n} X^{\prime} \frac{C_{+-n}^{m+k}}{C_{M}^{m+\alpha_{n}-1+k}}}{\sum_{k=-m}^{M-m-n+1} X \frac{C_{M+n+k+1}^{m+k}}{C_{M}^{m+\alpha_{n}-1+1+k}}}\right)^{1 / 2}
$$

where notations $X=\beta_{m\left(\alpha_{n-1}-1+k\right)}^{2}$ and $X^{\prime}=\beta_{m\left(\alpha_{n-1}+k\right)}^{2}$ are used. For the case $1<n \leqslant$ $M-N+m, \alpha_{n-1}=1, \ldots, n, \alpha_{n}=1, \ldots,(n+1)$, and for the case $M-N+m<n \leqslant$ $M-1, \alpha_{n-1}, \alpha_{n}=1, \ldots,(M-N+m+1)$. We can check that the above-defined $V$ satisfies the isometry condition $\sum_{i_{n}}\left[V^{[n] i_{n}}\right]^{\dagger} V^{[n] i_{n}}=1$. Similarly, we have

$$
\begin{aligned}
& V_{\alpha_{M} \alpha_{M-1}}^{[M] 0}=\delta_{\alpha_{M} \alpha_{M-1}}\left(\frac{\frac{\beta_{m\left(\alpha_{M-1}-1-m\right)}^{2}}{C_{M}^{\alpha_{M-1}}}}{\left.\frac{\beta_{m\left(\alpha_{M-1}-1-m\right)}^{2}}{C_{M}^{\alpha_{M-1}-1}}+\frac{\beta_{m\left(\alpha_{M-1}-m\right)}^{2}}{C_{M}^{\alpha_{M-1}}}\right)^{1 / 2}}\right. \\
& V_{\alpha_{M} \alpha_{M-1}}^{[M] 1}=\delta_{\alpha_{M}\left(\alpha_{M-1}+1\right)}\left(\frac{\beta_{m\left(\alpha_{M-1}-m\right)}^{2}}{C_{M}^{\alpha_{M-1}}}\right. \\
& \frac{\beta_{m\left(\alpha_{M-1}-1-m\right)}^{2}}{\left.C_{M}^{\alpha_{M-1}-1}+\frac{\beta_{m\left(\alpha_{M-1}-m\right)}^{2}}{C_{M}^{\alpha_{M-1}}}\right)^{1 / 2}} \text {, }
\end{aligned}
$$

where $0 \leqslant m \leqslant N-m, \alpha_{M-1}, \alpha_{M}=1,2, \ldots,(M-N+m+1)$.
For the case concerned about the ancilla state of the UQCM, assume $1 \leqslant l \leqslant M-N$; we have

$$
\begin{aligned}
& V_{\alpha_{M+l} l \alpha_{M+l-1}}^{[M+l]}=\delta_{\alpha_{M+l}\left(\alpha_{M+l-1}-1\right)}\left(\frac{\alpha_{M+l-1}-m-1}{M-N-l+1}\right)^{1 / 2}, \\
& V_{\alpha_{M+l} \alpha_{M+l-1}}^{[M+l] 1}=\delta_{\alpha_{M+l} \alpha_{M+l-1}}\left(\frac{M-N-l-\alpha_{M+l-1}+m+1}{M-N-l+1}\right)^{1 / 2} .
\end{aligned}
$$

(1) For $(m+1) \leqslant \alpha_{M+l} \leqslant(M-N+m-l+1),(m+2) \leqslant \alpha_{M+l-1} \leqslant(M-N+m-$ $l+2), V_{\alpha_{M+1} \alpha_{M+l-1}}^{[M+l] 0}=\delta_{\alpha_{M+l}\left(\alpha_{M+l-1}-1\right)} \sqrt{\frac{\alpha_{M+l-1}-m-1}{M-N-l+1}}$. For $\alpha_{M+l}=(M-N+m-l+2), 1 \leqslant$ $\alpha_{M+l-1} \leqslant(M-N+m+1), V_{\alpha_{M+l} \alpha_{M+l-1}}^{[M+l] 0}=0$. Otherwise $V_{\alpha_{M+l} \alpha_{M+l-1}}^{[M+l] 0}=\delta_{\alpha_{M+1} \alpha_{M+l-1}} \frac{1}{\sqrt{2}}$.
(2) For $(m+1) \leqslant \alpha_{M+l}, \alpha_{M+l-1} \leqslant(M-N+m-l+1), V_{\alpha_{M+l} \alpha_{M+l-1}}^{[M+l]}=$ $\delta_{\alpha_{M+l} \alpha_{M+l-1}} \sqrt{\frac{M-N-l-\alpha_{M+l-1}+m+2}{M-N-l+1}}$. For $\alpha_{M+l}=(M-N+m-l+2), 1 \leqslant \alpha_{M+l-1} \leqslant$ $(M-N+m+1), V_{\alpha_{M+1} \alpha_{M+l-1}}^{[M+l] 0}=0$. Otherwise $V_{\alpha_{M+l} \alpha_{M+l-1}}^{[M+l] 0}=\delta_{\alpha_{M+1} \alpha_{M+l-1}} \frac{1}{\sqrt{2}}$.

## References

[1] Bennett C H and DiVincenzo D P 2000 Nature 404247
[2] Bennett C H, Brassard G, Crepeau C, Jozsa R, Peres A and Wootters W 1993 Phys. Rev. Lett. 701895
[3] Gottesman D and Chuang I 1999 Nature 402390
[4] Raussendorf R and Briegel Hans J 2000 Phys. Rev. Lett. 865188
[5] Giovannetti V, Lloyd S and Maccone L 2001 Nature 412417
[6] Barenco A, Bennett C H, Cleve R, DiVincenzo D P, Margolus N, Shor P, Sleator T, Smolin J A and Weinfurter H 1995 Phys. Rev. A 523457
[7] Saavedra C, Gheri K M, Torma T, Cirac J I and Zoller P 2000 Phys. Rev. A 61062311
[8] Schon C, Solano E, Verstraete F, Cirac J I and Wolf M M 2005 Phys. Rev. Lett. 95110503
[9] Schon C, Hammerer K, Wolf M M, Cirac J I and Solano E 2006 Preprint quant-ph/0612101
[10] Affleck A, Kennedy T, Lieb E H and Tasaki H 1987 Phys. Rev. Lett. 59799
[11] Scarani V, Iblisdir S, Gisin N and Acin A 2005 Rev. Mod. Phys. 771225
[12] Cerf N J and Fiurasek J 2006 Progress in Optics vol 49 (Amsterdam: Elsevier) pp 455
[13] Fan H 2006 Top. Appl. Phys. 10263
[14] Lamas-Linares A, Simon C, Howell J C and Bouwmeester D 2002 Science 296712
[15] Martini F De, Bužek V, Sciarrino F and Sias C 2002 Nature 419815
[16] Pelliccia D, Schettini V, Sciarrino F, Sias C and Martini F De 2003 Phys. Rev. A 68042306
[17] Irvine M T M, Linares A Lamas, de Dood M J A and Bouwmeester D 2004 Phys. Rev. Lett. 92047902
[18] Ricci M, Sciarrino F, Sias C and De Martini F 2004 Phys. Rev. Lett. 92047901
[19] Cummins H K, Jones C, Furze A, Soffe N F, Mosca M, Peach J M and Jones J A 2002 Phys. Rev. Lett. 88187901
[20] Du J F, Durt T, Zou P, Li H, Kwek L C, Lai C H, Oh C H and Ekert A 2005 Phys. Rev. Lett. 94040505
[21] Simon C, Weihs G and Zeilinger A 2000 Phys. Rev. Lett. 842993
[22] Fan H, Weihs G, Matsumoto K and Wang X B 2003 Phys. Rev. A 67022317
[23] Delgado Y, Lamata L, Leon J, Salgado D and Solano E 2007 Phys. Rev. Lett. 98150502
[24] Gisin N and Massar S 1997 Phys. Rev. Lett. 792153
[25] Fan H, Matsumoto K and Wadati M 2001 Phys. Rev. A 64064301
[26] Vidal G 2003 Phys. Rev. Lett. 91147902
[27] Dang G F and Fan H in preparation

