Cloning the quantum oscillator

2000 J. Phys. A: Math. Gen. 33 5059

(http://iopscience.iop.org/0305-4470/33/28/310)

J. Phys. A: Math. Gen. **33** (2000) 5059–5076. Printed in the UK PII: S0305-4470(00)10679-1

Cloning the quantum oscillator

Göran Lindblad

Theoretical Physics, Royal Institute of Technology, SE-100 44 Stockholm, Sweden

E-mail: gli@theophys.kth.se

Received 6 January 2000, in final form 17 April 2000

Abstract. A class of completely positive maps are constructed which perform an approximate cloning of arbitrary states of a multi-mode quantum oscillator. Inside this class we find the optimal maps which do the cloning with greatest accuracy. The cloning errors appear in the characteristic functions of the states as additive Gaussian noise. The construction is extended to multiple clones, and it is shown that the minimal noise has an upper bound as the multiplicity goes to infinity. It is also shown that the construction is closely related to the formalism for linear quantum amplifiers and beamsplitters used in quantum optics.

1. Introduction

The no-cloning theorem points to one of the fundamental and characteristic differences between classical and quantum information. The theorem says that there is no way of constructing an apparatus capable of accepting an arbitrary quantum state as input, and as output giving back the original state plus a copy of some of the information in it. In particular, it is not possible to produce exact copies of the input states while retaining the originals intact. This impossibility is a direct consequence of the linearity and non-commutativity of quantum theory.

A number of different versions of no-cloning theorems have been published, e.g. [1–5]. In particular, the no-broadcasting theorem by Barnum *et al* [4] is a very general result. The idea of broadcasting is that the original state may be a mixed state, and that the two states in the output are partial states of a composite system, where the full state will inevitably be entangled in non-trivial cases. In this paper we will use this approach to the copying problem, and the terms 'clone' and 'copy' will be used interchangeably. We will also include the final state of the input system in the clones, the number of which will be two or more.

There have been a number of studies on copying machines which are optimal in the sense of producing a final state where the partial states of the clones are as close to the input state as quantum theory will allow [6–16]. The analysis of the possible final entangled states of the clones is complex even if we restrict ourselves to spin-$\frac{1}{2}$ systems. The problem of classification of cloning operations and the analysis of their accuracy is made more tractable if we restrict the maps to a set which can be parametrized in a useful way. In this paper we introduce a set of cloning maps which have a simple parametrization and which act in a particularly simple way on the characteristic function of the state.

0305-4470/00/285059+18\$30.00

The basic idea is that the cloning apparatus must contain degrees of freedom which are not included in the description (as in the case of a measuring instrument), thus the cloning maps represent the dynamics of an open system, and they belong to the scheme of operational quantum theory [17]. It follows that the cloning operations will be completely positive (CP) maps from the space of initial states to the space of entangled final states [10].

The layout of the paper is as follows. Sections 2 and 3 give a short introduction to the mathematical apparatus used. Section 4 defines a family of Gaussian (quasi-free) CP maps in terms of matrix-valued parameters. It is convenient to introduce them as acting on the observables (Heisenberg picture), through their action on the Weyl operators which represent the integrated form of the canonical commutation relations (CCR). They are, in fact, defined on all observables in the Hilbert space, and by the standard duality on the full set of input quantum states defined by density matrices. There is a simple convex structure and partial order on this class of maps. In this structure there are 'extreme' or 'minimal' maps with minimal noise. The value of this minimal noise is related to the uncertainty product in coherent and squeezed states. In general, the product of two minimal maps will not be minimal. Section 5 introduces Gaussian CP maps which create a pair of clones out of a single original system. In section 6 we can then apply a simple criterion for finding the maps giving the most accurate copies: the maps should be minimal in the sense defined in section 5. The thus defined cloning maps are optimal in the sense of preserving the expectations of the canonical variables and adding minimal noise to their variances. This criterion can be applied both to the entangled final state of the pair, and in a more restrictive way, to each of the clones.

In section 7 the method is extended to the production of multiple clones, and we can see how the quality of the clones will go down with the multiplicity. However, the value of the noise has a limit as the multiplicity goes to infinity which is just twice the value for the twofold cloning. The multi-clone state is highly correlated, and a quantitative entropy measure for this is calculated.

In section 8 we describe the relations between the present formalism and the standard theory of linear amplifiers and beamsplitters in quantum optics. Using a beamsplitter and amplification of the outgoing beams we can construct a cloning apparatus, but one with a noise which is not minimal.

Finally, in the appendix the partial order and convex structures of the Gaussian states and CP maps are described in some detail.

2. Weyl form of the CCR

In this section the necessary notation for the CCR is introduced, for more details see, e.g., [18, 19]. Let there be given a $2n$-dimensional real Hilbert space $\mathcal{H}$, with vectors denoted by $x, y, \ldots$ and a symplectic (real skew-symmetric bilinear) form $\sigma(x, y)$ defined on $\mathcal{H}$. In the standard representation of the CCR and for $n = 1$ the choice is

$$\sigma(x, y) = \tfrac{1}{2}\hbar(x_1 y_2 - y_1 x_2).$$

In the following we will set $\hbar = 1$. The form σ is defined by a real skew-symmetric matrix S: $\sigma(x, y) = \langle x|S|y\rangle$. Using unitary Weyl operators $W(x) = W(-x)^\dagger$ acting in a separable complex Hilbert space $\mathcal{K}$, we can write the CCR in the Weyl form

$$W(x)^\dagger W(y) = W(y - x)\, \mathrm{e}^{\mathrm{i}\sigma(x,y)} = W(y)W(x)^\dagger\, \mathrm{e}^{2\mathrm{i}\sigma(x,y)}. \tag{1}$$

In terms of the canonical operators $\{X_1, \ldots, X_{2n}\}$ acting in $\mathcal{K}$ we have

$$W(x) = \exp\{-\mathrm{i}X(x)\} \qquad X(x) := \sum_{j=1}^{2n} x_j X_j$$

and the self-adjoint operators $X(x)$ satisfy the CCR

$$[X(x), X(y)] = 2\mathrm{i}\langle x|S|y\rangle \mathbb{1}_{\mathcal{K}}.$$

We will assume the matrix S to be non-degenerate, in which case it is possible to choose the following normal form, in terms of the $n \times n$ unit matrix

$$S = \tfrac{1}{2}\begin{pmatrix} 0 & \mathbb{1}_n \\ -\mathbb{1}_n & 0 \end{pmatrix}. \tag{2}$$

Then the real linear transformations V in $\mathcal{H}$ which leave the CCR invariant

$$x \mapsto Vx \quad \forall x \in \mathcal{H} \qquad S \mapsto V^\dagger S V = S$$

are the Bogoliubov (symplectic) transformations, forming the real symplectic group $Sp(2n, \mathbb{R})$.

The Weyl operators form an irreducible set of operators in $\mathcal{K}$, and their linear combinations span the algebra $B(\mathcal{K})$ of all bounded operators in $\mathcal{K}$. We note that the expression (1) has the following obvious positive-definiteness property (the scalar product is that of $\mathcal{K}$):

$$\sum_{j,k} (\varphi_j^*, W(x_j)^\dagger W(x_k)\varphi_k) \geqslant 0 \qquad \forall x_j \in \mathcal{H} \quad \varphi_j \in \mathcal{K}. \tag{3}$$

3. Gaussian states

This section recalls the most important facts about Gaussian states. See the appendix for more details, which include some derivations. A state ρ is uniquely defined by the quantum characteristic function, i.e. the expectation of the Weyl operator

$$\chi(\rho, x) := \langle W(x)\rangle_\rho = \chi(\rho, -x)^* \qquad x \in \mathcal{H}$$

a continuous, complex-valued function of x [19, 20]. We assume it to be normalized: $\chi(\rho, 0) = \langle \mathbb{1}\rangle_\rho = 1$, and write it as an exponential

$$\chi(\rho, x) = \exp\{-\mathrm{i}\langle x|\xi\rangle + f(x)\} \tag{4}$$

where $\xi \in \mathcal{H}$ and f is a continuous function satisfying $f(0) = 0$, $f(x)^* = f(-x)$. The positivity of a state means that the expectation maps the positive-definite operator expression (1) into a positive-definite form. This leads to a positivity condition on (4): ρ is a state if and only if

$$\begin{gathered} \sum_{j,k} \lambda_j^* \lambda_k \phi(x_j, x_k) \geqslant 0 \qquad \forall x_j \in \mathcal{H} \quad \lambda_j \in \mathbb{C} \\ \phi(x, y) := \langle W(x)^\dagger W(y)\rangle_\rho = \chi(\rho, y - x)\exp\{\mathrm{i}\sigma(x, y)\}. \end{gathered} \tag{5}$$

The linear part $\langle x|\xi\rangle$ turns out to give a trivial contribution to this condition, it can be left out in most contexts. The state defined on the Weyl operators extends to a normal state (density operator) defined on all of $B(\mathcal{K})$.

There is an important class of states defined by real quadratic forms

$$f(x) = -\tfrac{1}{2}\langle x|F|x\rangle$$

with F a real symmetric matrix. The condition (5) can then be transformed into the simpler but equivalent matrix relation (see Holevo [19] equation (4.14) and theorem 5.1)

$$F + \mathrm{i}S \geqslant 0. \tag{6}$$

This inequality ensures the positivity of the state, the normalization is automatically fulfilled as $\chi(\rho, 0) = 1$, and so is the continuity. We note that the two inequalities $F \pm \mathrm{i}S \geqslant 0$ are equivalent, and that we can add them to conclude that $F \geqslant 0$. (For simplicity a Hermitian matrix with non-negative eigenvalues will be called positive; if it is non-degenerate they are strictly positive.)

There are other, equivalent, ways of writing the inequality (6). We can represent the complexification of the real Hilbert space $\mathcal{H}$ as a $4n$-dimensional real Hilbert space $\mathcal{H} \oplus \mathcal{H}$, and (6) takes the form

$$\begin{pmatrix} F & S \\ S^\dagger & F \end{pmatrix} \geqslant 0. \tag{7}$$

It is shown in the appendix that this inequality is equivalent to

$$0 \leqslant S^\dagger F^{-1} S \leqslant F. \tag{8}$$

The class of states defined by (4) and (6) we can call Gaussian, as in [19, 20], or quasi-free, a term used in the mathematical literature [21]. The average of the canonical operator is given by the linear term in the exponential of (4): $\langle X_k \rangle = \xi_k$. This term is inessential and removed by a translation implemented by a unitary Weyl operator

$$X_k \mapsto X_k - \xi_k \mathbb{1}. \tag{9}$$

In the following we can restrict the attention to states centred at the origin ($\langle X_k \rangle_\rho = 0$) in most places.

The role of the matrix F and the inequality (6) is readily understood when expressed in terms of the canonical operators: the variance matrix (for centred states)

$$\langle X_j X_k \rangle_\rho = \tfrac{1}{2} \langle \{X_j, X_k\} + [X_j, X_k] \rangle_\rho = F_{jk} + \mathrm{i}S_{jk} \tag{10}$$

must be positive. Like the Gaussian random variables of probability theory the Gaussian states are uniquely defined by their first and second moments. The higher-order moments are given by a simple formula (see [20] equation (4.4.119)).

The set of matrices F satisfying (6) for given S (and hence (7) and (8)) evidently form a convex set, and there is a partial order defined by the matrix order:

$$F_1 \leqslant F \quad \Leftrightarrow \quad F - F_1 \geqslant 0.$$

The matrix F is an extreme element in this convex set if and only if it satisfies

$$F = S^\dagger F^{-1} S \tag{11}$$

and it is known that all such elements F are conjugate under symplectic transformations [21]. In fact, with the standard representation of S one solution is $F_0 = \mathbb{1}/2$, and the general solution $F = \mathcal{F}^{1/2} F_0 \mathcal{F}^{1/2}$ where $\mathcal{F} = 2F$ is an element of the symplectic group $Sp(2n, \mathbb{R})$. If we include all translations, these states are the multi-mode coherent states for $\mathcal{F} = \mathbb{1}$, and generally the squeezed coherent states. They are also the pure Gaussian states, and the minimum uncertainty states in the sense that they give equality in the Robertson–Schrödinger inequality (Robertson intelligent states) [22, 23].

For general F satisfying (6) there are also non-Gaussian states with the same variance matrix (10), but if F satisfies (11) then the squeezed coherent states are the only solutions. This is illustrated by taking a convex combination of two Gaussian states: the characteristic function

$$\chi(\rho, x) = p\chi(\rho_1, x) + (1-p)\chi(\rho_0, x) \qquad 0 < p < 1$$

will not be that of a Gaussian state unless the two states are the same. However, there is a Gaussian state defined by $F = pF_1 + (1-p)F_0$ with the same variance matrix. Of all states with the same variance matrix the Gaussian state is that of maximum entropy [24].

It is interesting to note the simple relation between the inequality (8) and the entropy of the state. Recall that the entropy of a quantum state

$$H(\rho) := -\operatorname{tr}\, \rho \ln \rho$$

is a measure of the deviation from purity: the entropy is zero for a pure state and positive for a mixed state due to the concavity

$$H(p\rho_1 + (1-p)\rho_0) \geqslant pH(\rho_1) + (1-p)H(\rho_0) \qquad 0 < p < 1$$

with equality if and only if $\rho_0 = \rho_1$. In [24] a formula for the entropy of a Gaussian state is given. First note that from (8) follows directly the following inequality:

$$\mathbb{1} \leqslant M := F^{1/2} S^{-1\dagger} F S^{-1} F^{1/2}$$

where $M = \mathbb{1}$ for pure states. From this it follows that

$$N := \tfrac{1}{2}(M^{1/2} - \mathbb{1}) \geqslant 0.$$

The formula for the entropy of the Gaussian state ρ defined by F is then

$$H(\rho) = \tfrac{1}{2}\operatorname{tr}\{(N+\mathbb{1})\ln(N+\mathbb{1}) - N\ln N\}. \qquad (12)$$

In [24] the entropy is defined in terms of the matrix $M' = S^{-1\dagger} F S^{-1} F = F^{-1/2} M F^{1/2}$, but then $\operatorname{tr} f(M') = \operatorname{tr} f(M)$ for any function f.

4. Gaussian CP maps

We define a family of Gaussian (quasi-free) maps by their action on the Weyl operators

$$T: \ W(x) \mapsto W(Ax)\, \mathrm{e}^{g(x)} \qquad (13)$$

where A is a real $2n \times 2n$ matrix, and g is a quadratic form satisfying $g(-x) = g(x)^*$. Because the Weyl operators span $B(\mathcal{K})$, this relation also defines T on $B(\mathcal{K})$. These maps are the quantum analogues of the convolutions with Gaussian measures, and the dual maps acting on the state space maps Gaussian states into themselves. The map (13) is completely positive (CP) precisely when the positive-definite quantity (1) is mapped into a positive-definite quantity, i.e. when the expression

$$W(A(y-x))\, \mathrm{e}^{\mathrm{i}\sigma(x,y)+g(y-x)} = W(Ax)^\dagger W(Ay)\, \mathrm{e}^{\mathrm{i}\sigma(x,y)-\mathrm{i}\sigma(Ax,Ay)+g(y-x)} \qquad (14)$$

satisfies (3) [25, 26].

We note that the translations (9) are of the form (13) ($A = \mathbb{1}$, $g(x) = \mathrm{i}\langle x|\xi\rangle$). In the present context we can leave these out, and it is enough to look at quadratic forms g without a linear term, defined by a real symmetric matrix G:

$$g(x) = -\tfrac{1}{2}\langle x|G|x\rangle.$$

From (14) we obtain an inequality similar to (5); again this can be translated into an inequality for the exponent. This condition on (A, G) for the map to be CP was given in [25, 26]

$$G + \mathrm{i}S - \mathrm{i}A^\dagger SA \geqslant 0. \tag{15}$$

In particular, putting $A = 0$ we obtain the condition for a Gaussian state, and all states are mapped into the single state defined by $F = G$ satisfying (6). If we let A be a symplectic transformation, i.e. $A^\dagger SA = S$, then we can choose $G = 0$, which means that the map (13) has an inverse which is also CP. In fact, from the expression (13) we can write down the form of the inverse transformation and see that it is CP if and only if G and (15) are both zero.

The maps (13) act in a very simple way on the characteristic functions of the states:

$$\chi(\rho, x) \mapsto \chi(\rho', x) := \chi(\rho, Ax)\,\mathrm{e}^{g(x)}. \tag{16}$$

In particular, for a Gaussian state ρ defined by the pair $\{\xi, F\}$, we find that the final state ρ' is defined by the pair $\{\xi', F'\}$ where $\xi' = \xi A$ and

$$F' = A^\dagger FA + G \tag{17}$$

and that the variance matrix (10) for ρ' is

$$A^\dagger(F + \mathrm{i}S)A + G + \mathrm{i}S - \mathrm{i}A^\dagger SA \geqslant 0. \tag{18}$$

In the standard formalism of quantum optics the same mathematics is represented in a different but equivalent form [27]. The action of an environment of passive and active linear optical elements on a finite number of modes of the EM field is described by transforming the canonical operators for a system plus environment

$$X_j \mapsto X'_j = \sum_k X_k A_{kj} + N_j$$

and the CCR is assumed for the operators $\{X'_j\}$. Using this method one obtains the formulae above by imposing that the 'noise' symbols N has a variance matrix $\langle N_j N_k \rangle$ equal to (15); here the average denotes an expectation in a 'reservoir' state. This matrix describes the noise coming from the interaction with the environment, but it is the quantum nature of the system which implies that this noise cannot be zero.

The non-commutative, quantum nature of the system also means there is only a partial order on the noise matrices, and no unique definition of the minimal noise. Instead there is a family of minimal G satisfying (15) for the given values of S, A (see the appendix for the definition). These pure (extremal) solutions G of (15) are obtained in analogy with the pure Gaussian states. We can write (15) in the familiar form

$$0 \leqslant K^\dagger G^{-1} K \leqslant G \qquad K := A^\dagger SA - S = -K^\dagger \tag{19}$$

and it is shown in the appendix that the minimal solutions of (19) for given (S, A) are the solutions of

$$G = K^\dagger G^{-1} K. \tag{20}$$

It is evident from (18) that the minimal solutions for the map give a minimal variance matrix for the final state, given the initial state and (S, A).

The family of Gaussian CP maps (for given $\mathcal{H}$, S) is closed under composition of maps: let there be two such maps T_1, T_2 defined by matrices A_j, G_j, $j = 1, 2$, then the composite map $T = T_1 T_2$ is defined by

$$A = A_1 A_2 \qquad G = G_2 + A_2^\dagger G_1 A_2.$$

We also find that $K = K_2 + A_2^\dagger K_1 A_2$ which means that (15) is fulfilled by T if this is true for T_1 and T_2. However, if both T_1 and T_2 satisfy the minimal noise condition (20) this it not necessarily so for the composite map T. It is true in some cases, for instance if one of the maps is a reversible symplectic transformation, i.e. K_1 or K_2 is zero, and the corresponding minimal noise matrix is zero. Consider the case where K_1 and K_2 (and hence K) are non-singular. (The details are a bit more complex for singular K_1 and K_2, and we will leave them out.) From the appendix we know that the minimality condition (20) is satisfied by G if and only if $G \pm \mathrm{i}K$ satisfy

$$(G \pm \mathrm{i}K)G^{-1}(G \mp \mathrm{i}K) = 0 \tag{21}$$

and this is equivalent to $G \pm \mathrm{i}K$ being positive matrices of rank n. Because

$$G \pm \mathrm{i}K = G_2 \pm \mathrm{i}K_2 + A_2^\dagger(G_1 \pm \mathrm{i}K_1)A_2$$

we see that the composite map is minimal if and only if $A_2^\dagger(G_1 \pm \mathrm{i}K_1)A_2$ has a support projection contained in that of $G_2 \pm \mathrm{i}K_2$ (of rank n). For positive matrices A, B their support projections satisfy

$$AB = 0 \quad \Leftrightarrow \quad \operatorname{supp} A \perp \operatorname{supp} B.$$

If we use this lemma on (21) applied to $G_2 \pm \mathrm{i}K_2$ we will find that the conditions on the supports are fulfilled precisely when it holds that

$$A_2^\dagger(G_1 \pm \mathrm{i}K_1)A_2 G_2^{-1}(G_2 \mp \mathrm{i}K_2) = 0.$$

These are then necessary and sufficient conditions for the composite map to be minimal; it is not satisfied in general, not even in the case $T_1 = T_2$. A simple example is provided by the minimal maps (with standard form for S) $A_j = a_j \mathbb{1}$, $G_j = |a_j^2 - 1|\mathbb{1}/2$. We find that the product is minimal if and only if $|a_1|$, $|a_2|$ are either both >1 or both <1 or one of them $= 1$.

5. The cloning map

A cloning map will take the initial-state space of the oscillator to the final-state space of two similar oscillators. We will treat the two final systems in a symmetric way, making no distinction between the 'original' and the 'clone'. In the Heisenberg picture the map goes the opposite way, from the final system observables to those of the initial system.

We choose the maps to be of the form defined in section 4, for the reasons indicated in the introduction: this set has a simple parametrization and each map acts in a simple way on the characteristic function of the state. These facts allow us to find among this set the best cloning maps; they map each initial state into two clone states which are as close to the initial state as possible. Here we let 'close' mean that they have the same averages for the canonical operators, while as little noise as possible is added.

The Heisenberg picture version of the cloning map is then assumed to be a Gaussian CP map $T : B(\mathcal{K} \otimes \mathcal{K}) \to B(\mathcal{K})$ defined by

$$W(x_1, x_2) \mapsto W(A_1 x_1 + A_2 x_2)\,\mathrm{e}^{g(x_1, x_2)} \tag{22}$$

where g is again assumed to be quadratic, and A_1, A_2 are real $2n \times 2n$ matrices. Again the quadratic form g can be written as matrix elements

$$g(y_1, y_2) = -\tfrac{1}{2}\{\langle y_1|G_1|y_1\rangle + \langle y_2|G_2|y_2\rangle + \langle y_1|K|y_2\rangle + \langle y_2|K^\dagger|y_1\rangle\}$$

where G_1, G_2, K are real matrices and we can choose G_1, G_2 to be symmetric. We find that

$$W(x_1,x_2)^\dagger W(y_1,y_2) \mapsto W(A_1x_1+A_2x_2)^\dagger W(A_1y_1+A_2y_2)\,\mathrm{e}^{\mathrm{i}\xi(x_1,x_2,y_1,y_2)}$$

where the exponent is still a quadratic form

$$g(y_1-x_1,y_2-x_2)+\mathrm{i}\sigma(x_1,y_1)+\mathrm{i}\sigma(x_2,y_2)-\mathrm{i}\sigma(A_1x_1+A_2x_2,A_1y_1+A_2y_2).$$

Using (15) the CP property of the map T is translated into the following matrix inequality:

$$\begin{pmatrix} G_1 & K \\ K^\dagger & G_2 \end{pmatrix} + \mathrm{i}\begin{pmatrix} S & 0 \\ 0 & S \end{pmatrix} - \mathrm{i}\begin{pmatrix} A_1^\dagger & 0 \\ A_2^\dagger & 0 \end{pmatrix}\begin{pmatrix} S & 0 \\ 0 & S \end{pmatrix}\begin{pmatrix} A_1 & A_2 \\ 0 & 0 \end{pmatrix} \geqslant 0$$

and in simplified form

$$\begin{pmatrix} G_1+\mathrm{i}S-\mathrm{i}A_1^\dagger SA_1 & K-\mathrm{i}A_1^\dagger SA_2 \\ K^\dagger-\mathrm{i}A_2^\dagger SA_1 & G_2+\mathrm{i}S-\mathrm{i}A_2^\dagger SA_2 \end{pmatrix} \geqslant 0. \tag{23}$$

Perfect cloning of all states would be equivalent to the following relations for the partial transformations on the algebras of observables:

$$T[W(x,0)] = W(x) \qquad T[W(0,y)] = W(y).$$

The no-cloning theorems forbid these relations to hold exactly, but we can demand that the two transformations are as close to the identity map as is possible. With this end in mind it is clear that we should choose $A_1 = A_2 = \mathbb{1}$ in (22). This choice implies that the averages $\langle X_j\rangle$ will be the same for both clones as for the input state; it also means that the cloning process is invariant under the translations (9). With this choice the cloning map (22) is

$$W(x_1,x_2) \mapsto W(x_1+x_2)\,\mathrm{e}^{g(x_1,x_2)}. \tag{24}$$

If we apply the cloning process to a Gaussian state defined by a matrix F satisfying (6), we obtain a final state which is a Gaussian defined by the real symmetric matrix

$$\begin{pmatrix} F+G_1 & F+K \\ F+K^\dagger & F+G_2 \end{pmatrix}$$

which satisfies (7):

$$\begin{pmatrix} F+G_1+\mathrm{i}S & F+K \\ F+K^\dagger & F+G_2+\mathrm{i}S \end{pmatrix} \geqslant 0.$$

The partial states of the two clones are also Gaussian and defined by the diagonal terms $F+G_1$ and $F+G_2$, respectively. Here G_1, G_2 are the 'noise' terms coming from the cloning process, we will minimize them in next section. The off-diagonal term $F+K$ in the block matrix measures the correlation between the two clones in the final state. We can have an uncorrelated final state only for a single value of F, setting $K=-F$.

From (24) we also find how the characteristic function transforms from the initial state ρ into a final state ρ':

$$\chi(\rho,x) \mapsto \chi(\rho',x_1,x_2) := \chi(\rho,x_1+x_2)\mathrm{e}^{g(x_1,x_2)}.$$

The characteristic functions for the partial states are obtained from $\chi(\rho',x_1,x_2)$ by setting one of the variables equal to zero, and they are just the input characteristic function multiplied by a Gaussian

$$\chi(\rho_1',x) = \chi(\rho',x,0) = \chi(\rho,x)\,\mathrm{e}^{g(x,0)} \qquad \chi(\rho_2',x) = \chi(\rho,x)\,\mathrm{e}^{g(0,x)}. \tag{25}$$

The Wigner function is a Fourier transform of the characteristic function [20]

$$\mathcal{W}(\rho, \xi) := (2\pi)^{-n} \int \mathrm{d}x\, \chi(\rho, x)\, \mathrm{e}^{-\mathrm{i}\langle x|\xi\rangle} \qquad \xi \in \mathcal{H}$$

with normalization $\int \mathrm{d}\xi\, \mathcal{W}(\rho, \xi) = 1$. From (25) we can directly find the Wigner functions of the partial states, they are simply convolutions of the input Wigner function by Gaussian distributions:

$$\mathcal{W}(\rho'_k, \xi) = \int \mathrm{d}\eta\, \mathcal{W}(\rho, \xi - \eta)\, \mathcal{G}_k(\eta) \qquad k = 1, 2$$

$$\mathcal{G}_k(\xi) := (2\pi)^{-n}(\det G_k)^{-1/2} \exp\{-\tfrac{1}{2}\langle\xi|G_k^{-1}|\xi\rangle\}.$$

From the Wigner function we can recover the density matrix of the state in a suitable basis. This is done by inverting the familiar Wigner formula which gives the Wigner function as the Fourier transform of a family of density matrix elements [20]. The resulting formulae are cumbersome in the multimode case, and we leave them out.

We note that for general states the variance matrix (10) is found from the characteristic functions (differentiating twice), and we see from (25) that the cloning map acts on it in the same way as it does for the Gaussian states.

6. Noise in the cloning process

The cloning map (24) still has an unspecified exponent g, which includes the noise terms G_1, G_2 which enter into the partial states of the two clones. We can now define what we mean by a maximal fidelity for the cloning map: a minimal choice of the noise terms G_1, G_2 consistent with (23). We will first describe the minimal property of the noise added in the final two-clone state, according to the general scheme set out in the appendix, and which was already used in section 5. After that it is a simple modification to find the minimal noise added to the two clones separately.

Setting $A_1 = A_2 = \mathbb{1}$ the matrix inequality (23) is simplified into

$$\begin{pmatrix} G_1 & K - \mathrm{i}S \\ K^\dagger - \mathrm{i}S & G_2 \end{pmatrix} \geqslant 0. \tag{26}$$

This inequality is of the standard form $G_{(2)} - \mathrm{i}S_{(2)} \geqslant 0$ if we introduce

$$G_{(2)} := \begin{pmatrix} G_1 & K \\ K^\dagger & G_2 \end{pmatrix} \qquad S_{(2)} = \begin{pmatrix} 0 & S \\ S & 0 \end{pmatrix}.$$

We then obtain the equivalent variant of (26) from (19), $S_{(2)}^\dagger\, G_{(2)}^{-1}\, S_{(2)} \leqslant G_{(2)}$, and the minimal solutions of this inequality are found in the appendix to be the solutions of

$$S_{(2)}^\dagger\, G_{(2)}^{-1}\, S_{(2)} = G_{(2)}. \tag{27}$$

Again, using the standard form for S we find one solution of (27) to be $G_{(2)0} = \mathbb{1}_{4n}/2$; a full set of solutions of (27) is generated as follows. It is shown in the appendix that for any real symmetric matrix $\mathcal{B}$ we obtain a solution from equation (A3), here it has the form

$$G_{(2)} = \tfrac{1}{2} \exp\{\mathcal{B} - 4S_{(2)}^\dagger \mathcal{B} S_{(2)}\} \tag{28}$$

it is also proved there that every solution of (27) is of this form.

The solutions of (28) give a minimal noise in the composite two-system final state. In practice we are likely to be interested in minimizing just the noise terms G_1, G_2 in the two partial states. We do this by setting $K = 0$; this corresponds to choosing a block diagonal $\mathcal{B}$. In order to see that this is true we note that using the methods of the appendix, equation (26) is equivalent to

$$0 \leqslant (K^\dagger - \mathrm{i}S)\, G_1^{-1}(K - \mathrm{i}S) \leqslant G_2.$$

We can also complex conjugate this inequality, using $S^\dagger = -S$, sum the two inequalities and divide by 2 to find that

$$0 \leqslant K^\dagger\, G_1^{-1} K + S^\dagger\, G_1^{-1} S \leqslant G_2. \tag{29}$$

From (29) and the calculations in the appendix it is clear that if we want to make the noise terms G_1, G_2 for the two clones as small as possible, then we should first choose $K = 0$, reducing the quadratic form to

$$g(y_1, y_2) = -\tfrac{1}{2}\{\langle y_1|G_1|y_1\rangle + \langle y_2|G_2|y_2\rangle\}.$$

Setting $K = 0$ in (29) we obtain the following inequality:

$$0 \leqslant S^\dagger\, G_1^{-1} S \leqslant G_2. \tag{30}$$

For any choice of a real positive non-degenerate G_1 there is a minimal solution of (30):

$$G_2 = S^\dagger\, G_1^{-1} S. \tag{31}$$

The solutions of (31) also satisfy (27) for $K = 0$. We obtain a family of symmetric solutions setting $G_1 = G_2 = G$ where G satisfies (11). A larger set of solutions is given by $\lambda G_1 = \lambda^{-1} G_2 = G$, $\lambda > 0$, where G again satisfies (11).

We recall from the previous section that if the initial state is defined by the matrix F, then the partial states of the two clones are defined by $F + G_1$ and $F + G_2$, and their characteristic functions are given by (25). If F is also a solution of (11), representing a pure initial state, then we can see how an optimal cloning process defined by minimal noise terms G_1, G_2 will make the clones mixed states, but also that we have the choice of putting more of the noise in one of the clones, and less in the other.

For general solutions of (31) we can find a transformation in $Sp(2n, \mathbb{R})$ which transforms G_1 to a diagonal form, while preserving the normal form (2) of S [28, 29]. From (31) we then find that G_2 will also be diagonal. There is then real positive $n \times n$ diagonal matrices D_1, D_2 such that

$$G_1 = \tfrac{1}{2}\begin{pmatrix} D_1 & 0 \\ 0 & D_2 \end{pmatrix} \qquad G_2 = \tfrac{1}{2}\begin{pmatrix} D_2^{-1} & 0 \\ 0 & D_1^{-1} \end{pmatrix}. \tag{32}$$

In order to see the consequences of this structure as simply as possible, consider the case $n = 1$. It is informative to display the solution in the squeezed form

$$G_1 = \frac{1}{2\lambda}\begin{pmatrix} \kappa & 0 \\ 0 & \kappa^{-1} \end{pmatrix} \qquad G_2 = \lambda^2 G_1.$$

We can thus let the two clones be of different fidelity, but we cannot make two clones which have high fidelity for two complementary quadratures of the same degree of freedom.

We can easily introduce a formal classical limit by setting $\hbar = 0$; this means that $S = 0$, and that all the positivity conditions are reduced to $G_1 \geqslant 0, G_2 \geqslant 0$. In particular, we can then choose the Gaussian functions $\mathcal{G}_1, \mathcal{G}_2$ in the convolution of the Wigner functions to have as small variances as we like, and there is no restriction on the accuracy of the copies.

7. Multiple clones

It is interesting to generalize the formalism to the generation of multiple clones. We will see that the simultaneous creation of multiple clones is more efficient than a succession of cloning operations. If we want $m > 2$ clones in all, the map (24) is replaced by

$$W(x_1, x_2, \ldots, x_m) \mapsto W(x_1 + x_2 + \cdots + x_m)\, \mathrm{e}^{g(x_1,x_2,\ldots,x_m)}. \tag{33}$$

We write the exponent in the form

$$g(x_1, x_2, \ldots, x_m) = -\tfrac{1}{2}\sum_k \langle x_k|G_k|x_k\rangle - \tfrac{1}{2}\sum_{j\neq k}\langle x_j|K_{jk}|x_k\rangle$$

where G_k, $K_{jk} = K_{kj}^{\dagger}$ are real matrices of dimension $2n \times 2n$, and $j, k = 1, \ldots, m$. In the case $m = 2$ we could choose the cross terms to be zero for a minimal solution, i.e. setting $K = 0$ in (26); in the general case we have to keep them. Introduce the real matrices, of dimension $2mn \times 2mn$:

$$G_{(m)} = \delta_{jk}\, G_k + (1 - \delta_{jk})K_{jk} \qquad S_{(m)} = (1 - \delta_{jk})\, S. \tag{34}$$

For each $m \geqslant 2$ the matrix $G_{(m)}$ is symmetric, $S_{(m)}$ is skew-symmetric and non-degenerate, in fact, $\det S_{(m)} = 2^{-mn}(m-1)^{2n}$. The inequality (26) is replaced by either of the two equivalent relations

$$G_{(m)} - \mathrm{i}S_{(m)} \geqslant 0 \qquad \begin{pmatrix} G_{(m)} & S_{(m)} \\ S_{(m)} & G_{(m)} \end{pmatrix} \geqslant 0 \tag{35}$$

which again are equivalent to

$$0 \leqslant S_{(m)}^{\dagger} G_{(m)}^{-1} S_{(m)} \leqslant G_{(m)}. \tag{36}$$

We can then apply the same argument used in section 6, and in the appendix, to find a solution to the condition for minimality

$$S_{(m)}^{\dagger} G_{(m)}^{-1} S_{(m)} = G_{(m)}. \tag{37}$$

Again, there is one obvious solution $G_{(m),0} = (S_{(m)}^{\dagger} S_{(m)})^{1/2}$. With the standard representation (2) of S we obtain after some calculations

$$G_{(m),0} = \frac{1}{2}\left(\frac{m-2}{m} + \delta_{jk}\right)\mathbb{1}_{2n}.$$

The two parts defined in (34) are then

$$G_k = \frac{m-1}{m}\,\mathbb{1}_{2n} \qquad K_{jk} = \frac{m-2}{2m}\,\mathbb{1}_{2n}. \tag{38}$$

We see that in creating an increasing number of clones, the optimum accuracy of the cloning becomes progressively worse, but with a bound as $m \to \infty$ which is just twice that for $m = 2$. A simultaneous m-fold cloning is definitely better than a succession of $m - 1$ twofold cloning operations, but it comes at the price of a highly entangled final state.

We find a representation of the full set of minimal solutions using the methods described in the appendix. Introduce the real, skew-symmetric and unitary matrix

$$V = G_{(m),0}^{-1/2} S_{(m)} G_{(m),0}^{-1/2} = \left(-\delta_{jk} + \frac{2}{m}\right) 2S.$$

For any real, symmetric $2mn \times 2mn$ matrix $\mathcal{B}$ we find a solution of (37) using (A3):

$$G_{(m)} = G(s) = G_{(m),0}^{1/2} \exp\{\mathcal{B} - V^{\dagger}\mathcal{B}V\} G_{(m),0}^{1/2} \tag{39}$$

satisfies (37), and all minimal solutions are of this form.

We will not try to investigate this full set of minimal solutions, but only look at those which are symmetric under the permutations of the m clones. These solutions are defined by $2n \times 2n$ matrices G, K:

$$G_j = G \qquad K_{jk} = K \qquad \forall j, k = 1, \ldots, m.$$

We must then choose the matrix $\mathcal{B}$ to have the same structure as $G_{(m)}$, the diagonal ($j = k$) blocks of dimension $2n \times 2n$ all the same, the off-diagonal ($j \neq k$) blocks all the same. Some relatively straightforward calculations give the full set of solutions in terms of two arbitrary solutions F_1, F_2 of equation (11):

$$G = \frac{m-1}{m}(F_1 + F_2) \qquad K = \frac{1}{m}[(m-1)F_2 - F_1].$$

If our goal is to minimize the noise term in each clone, that is G, it is clear from the discussion of the convex structure in the appendix that we should pick $F_1 = F_2$. In particular, for $m = 2$ we then find $K = 0$ and thus the family of solutions given in section 6 for the symmetric case.

We can now apply the entropy formula (12) to the final m-clone state to see that this is, in fact, a highly correlated state. For simplicity we assume the initial state to be the pure state defined by $F_0 = \mathbb{1}/2$, and the cloning map to be the minimal symmetric one defined above by $F_1 = F_2 = F_0$, hence

$$G = \frac{m-1}{m} 2F_0 \qquad K = \frac{m-2}{m} F_0.$$

The final m-clone state is then defined by the $2mn \times 2mn$ matrix

$$F_{(m)} = F + \delta_{jk} G + (1 - \delta_{jk}) K = \left[2\frac{m-1}{m} + \delta_{jk} \right] F_0.$$

From this expression we can calculate the matrix N defining the entropy (12)

$$N = F_{(m)} - \tfrac{1}{2}\mathbb{1}_{2mn} = (m-1) P \otimes \mathbb{1}_{2n}$$

where every element of the $m \times m$ matrix P has the value $1/m$. Thus P is a projection of rank 1, consequently N has the eigenvalues $m - 1$ with multiplicity $2n$, and 0 with multiplicity $2(m-1)n$. The entropy of the final state is then

$$H(\rho'_{(m)}) = n\,\{m \ln m - (m-1)\ln(m-1)\}$$

and the asymptotic behaviour as the number of clones goes to infinity

$$H(\rho'_{(m)}) \to n \ln m \qquad m \to \infty.$$

Each of the clones has a partial state defined by the matrix

$$F = \frac{3m-2}{m} F_0$$

and the entropy is determined by the matrix

$$N = 2\frac{m-1}{m} F_0$$

with the $2n$-fold eigenvalue $(m-1)/m$, hence

$$H(\rho_1') = \frac{n}{m}\{(2m-1)\ln(2m-1) - (m-1)\ln(m-1) - m\ln m\}$$

and the asymptotic value as $m \to \infty$ is $2n \ln 2$. The correlation in the final state is measured by the quantity $mH(\rho_1') - H(\rho_{(m)}')$ which has the asymptotic value $n(2m\ln 2 - \ln m)$.

It is clear from these calculations that the final state of the composite m-fold clone system is highly correlated. This fact will let us use the cloning as the first stage in a 'minimal perturbation' type of measurement process. We can then see the partial state of the clones as the final state of the measured system, while the $m-1$ other clones appear as a 'pointer' system where we can choose to make any quantum measurement. The investigation of this aspect will be left to another occasion.

Without using the correlations, we can determine the final state on $m-1$ of the clones using quantum tomography [30], while still retaining one 'original' in this state. Letting $m \to \infty$ we will be able to do so with negligible error.

8. Amplifiers and beamsplitters

The formalism of Gaussian CP maps in section 4 can be used for a streamlined derivation of important relations in quantum optics. When the canonical operators are those describing the quadratures of one or more modes of the EM field, these transformations will describe linear amplifiers and attenuators for light beams. Standard derivations use the CCR of the relevant modes and their environment to derive the properties of the quantum noise (see, for instance, [27, 31, 32]). Such considerations are automatically included in the description of the open quantum system dynamics given by the formalism in section 4. Thus the relation (15) contains the fundamental amplifier uncertainty principle of Caves [31]. However, due to the matrix nature of the inequality, it sums up the different cases (phase preserving, phase conjugating, multimode case, etc) in a simple way.

Matrix A describes the amplification or attenuation of a radiation mode due to the interaction with the environment, while G is a measure of the noise introduced by the amplification due to the quantum nature of the dynamics. Take a simple example, with a single mode ($n = 1$), and the basis is chosen such that A is diagonal, in which case the family of minimal G will also be diagonal. We find that (15) now reads

$$\begin{pmatrix} G_1 & \mathrm{i}(1 - A_1A_2)/2 \\ -\mathrm{i}(1 - A_1A_2)/2 & G_2 \end{pmatrix} \geqslant 0$$

where $G_j, A_j \in \mathbb{R}$, and that an equivalent form is $G_1G_2 \geqslant (1 - A_1A_2)^2/4$, which can be compared with the relation (3.35) in Caves [31], with due regard of the different notation (interchanging A and G and a renormalization). In particular, if $A_1A_2 = 1$ then the transformation A is symplectic, i.e. preserves the CCR, and the lower bound on the noise is zero.

There is also a considerable similarity of the cloning map approach of section 5 to the formalism used in quantum optics to describe beamsplitters (see, e.g., [33]). In a lossless beamsplitter two ingoing radiation beams, each with one or more modes, are transformed into two outgoing beams in a reversible way, i.e. one conserving the CCR. In our formalism there is first a reversible transformation from the Weyl operators of the two outgoing systems to those of the two incoming systems:

$$W(x_1, x_2) \mapsto W(x_1', x_2')$$
$$x_1' = B_{11}x_1 + B_{12}x_2 \qquad x_2' = B_{21}x_1 + B_{22}x_2.$$

The conservation of the CCR says that

$$B_{11}^\dagger S B_{11} + B_{21}^\dagger S B_{21} = B_{12}^\dagger S B_{12} + B_{22}^\dagger S B_{22} = S \qquad B_{11}^\dagger S B_{12} + B_{21}^\dagger S B_{22} = 0 \tag{40}$$

(and the higher coefficients of the latter equation). If there is just the vacuum state in one of the incoming beams, then we should average over this initial state (for the x_2' variable):

$$W(x_1', x_2') \mapsto W(x_1') \exp\{f(x_2')\}.$$

Comparing this expression with (22) we find that $g(x_1, x_2) = f(B_{21}x_1 + B_{22}x_2)$ and finally

$$G_1 = B_{21}^\dagger F B_{21} \qquad G_2 = B_{22}^\dagger F B_{22} \qquad K = B_{21}^\dagger F B_{22}.$$

We can now compare with (23), using (40), to find that this expression is equal to

$$\begin{pmatrix} B_{21}^\dagger (F + \mathrm{i}S) B_{21} & B_{21}^\dagger (F + \mathrm{i}S) B_{22} \\ B_{22}^\dagger (F + \mathrm{i}S) B_{21} & B_{22}^\dagger (F + \mathrm{i}S) B_{22} \end{pmatrix} \geqslant 0. \tag{41}$$

It is clearly enough that $F + \mathrm{i}S \geqslant 0$, which is fulfilled when we set the QHO ground state for the incoming vacuum beam $F = \mathbb{1}/2$. This condition is also necessary when the B_{jk} are non-degenerate.

It is quite natural to ask if we can obtain the cloning maps in section 5 through the action of an ideal beamsplitter followed by an amplification of the two output beams. We can choose a symmetric beamsplitter and pick a phase shift (necessary to preserve unitarity)

$$B_{11} = B_{12} = -B_{21} = B_{22} = \frac{\mathbb{1}}{\sqrt{2}}$$

and find $G_1 = G_2 = F/2 = \mathbb{1}/4$. We then have to amplify each of the two outgoing beams, setting $A = \sqrt{2}\,\mathbb{1}$, with a minimal noise matrix, from (15), which we can choose to be $G_0 = F = \mathbb{1}/2$. The total noise matrix for each beam is then $G = G_0 + A^\dagger F A/2 = 2F = \mathbb{1}$, to be compared with the minimal noise $G = F = \mathbb{1}/2$ given in section 6.

Acknowledgment

This research was supported by the Swedish Natural Science Research Council.

Appendix

In this appendix we collect some useful results for the Gaussian states and Gaussian CP maps. For more background material see, for instance, [19, 22, 23, 28, 29]. We return to the matrix inequalities of the equivalent forms (6)–(8). The set of solutions to these inequalities (for a given S) has a partial order and a convex structure. We need to identify the solutions which are minimal in the partial order; these solutions can be interpreted as the pure Gaussian states (section 3). It will be shown that the minimal solutions are precisely the solutions of the equality (11). The method is then modified to deal with the inequalities (15), (26) and (35) for the Gaussian CP maps. The minimal solutions are the Gaussian CP maps with minimal noise (section 4), and they satisfy relations like (20), (27) and (37).

In the following F and G denote real, symmetric and positive matrices in the $2n$-dimensional Hilbert space $\mathcal{H}$. When S is the standard, non-degenerate symplectic form (2), then any solution F of (7) must also be non-degenerate, i.e. all eigenvalues are strictly positive. The invertible real transformation

$$V = \begin{pmatrix} 1\!\!1 & -F^{-1}S \\ 0 & 1\!\!1 \end{pmatrix} \qquad \det V = 1$$

gives to (7) an equivalent block-diagonal form

$$V^\dagger \begin{pmatrix} F & S \\ S^\dagger & F \end{pmatrix} V = \begin{pmatrix} F & 0 \\ 0 & F - S^\dagger F^{-1} S \end{pmatrix} \geqslant 0$$

which is clearly equivalent to (8). Now assume that $0 \leqslant F \leqslant G$. It is then known that $0 \leqslant G^{-1} \leqslant F^{-1}$. In order to see this, note first that it is obvious for $G = 1\!\!1$, then replace F by $G^{-1/2}FG^{-1/2}$ to obtain the statement. It follows that if F satisfies (8), then so does G. Furthermore, if F satisfies (8) and G satisfies the equality (11), i.e. $S^\dagger G^{-1} S = G$, then $F = G$. Thus we find that the solutions of (11) are minimal solutions of (8).

We can add a converse statement. If G satisfies (8) but $S^\dagger G^{-1} S \neq G$, then we can find a $F \leqslant G$ such that (11) holds. The calculation is simple: the real skew-symmetric matrix $S_1 := G^{-1/2} S G^{-1/2}$ is still non-degenerate, and

$$G_1 := (S_1^\dagger S_1)^{1/2} \quad \Rightarrow \quad S_1^\dagger G_1^{-1} S_1 = G_1 \leqslant 1\!\!1.$$

Then check that $F := G^{1/2} G_1 G^{1/2} \leqslant G$ satisfies (11) with the original choice of S.

There are other useful characterizations of the solutions of (11). From (6) and (8) it follows that $\det F \geqslant \det S$ and that equality holds precisely for the solutions of (11) (see the appendix of [22]). Introduce the self-adjoint matrices

$$W_\pm := \tfrac{1}{2}\left\{1\!\!1 \pm \mathrm{i}\, F^{-1/2} S F^{-1/2}\right\}.$$

Using (8) and (11) we find that $W_+ + W_- = 1\!\!1_{2n}$ and that

$$W_\pm^2 \geqslant W_\pm \qquad W_+ W_- \geqslant 0$$

where equality holds in the two inequalities precisely when (11) is fulfilled. Thus, for the solutions of (11) the two matrices $W_\pm$ are two complementary projections, each of rank n. From this it follows that $F \pm \mathrm{i}S$ are two positive matrices which are of rank n precisely when (11) is fulfilled.

If we use the standard representation (2) of S, then $S^\dagger S = 1\!\!1/4$, and one solution of the minimality relation (11) is $F_0 = (S^\dagger S)^{1/2} = 1\!\!1/2$. This choice in (4) gives the characteristic function for a multimode coherent state (the vacuum state if $\xi = 0$). A way of finding the full range of solutions of (11) is provided by the following argument. Normalize the matrix F to determinant 1: $\mathcal{F} = 2F$, use (2) for S, thus obtaining the form

$$\mathcal{F} = 4 S^\dagger \mathcal{F}^{-1} S$$

for (11). We can rewrite this relation as $\mathcal{F} S \mathcal{F} = S$, and with $\mathcal{F}^\top = \mathcal{F}^\dagger = \mathcal{F}$ we see that $\mathcal{F}$ is a symplectic transformation. It also follows that $F = \mathcal{F}^{1/2} F_0 \mathcal{F}^{1/2}$, and this is a solution of (11) for any positive symplectic transformation $\mathcal{F}$. Thus the general solution of (11) is a symplectic transform of the coherent minimal solution, i.e. a squeezed multimode state.

There is also a convex structure associated with the solutions of (8), and the equivalent (6) and (7). If we have two solutions $\{F_0, F_1\}$, then for every $0 < p < 1$ the convex combination $F_p = (1 - p)F_0 + pF_1$ satisfies the same inequality. We say that F is an extreme element in this convex structure when $F = (1 - p)F_0 + pF_1$ for some p implies that $F = F_0 = F_1$. It is then easy to see that F is an extreme element if and only if it is a minimal solution. To show this, first a little lemma: let A, B be positive and non-degenerate. For all $0 < p < 1$ it holds that

$$((1 - p)A + pB)^{-1} \leqslant (1 - p)A^{-1} + pB^{-1}$$

with equality if and only if $A = B$. First, consider the case $B = \mathbb{1}$, then the statement follows from the spectral resolution for A. Then replace A by $B^{-1/2}AB^{-1/2}$ and we obtain the statement. We now know that

$$S^\dagger F^{-1} S \leqslant (1 - p)S^\dagger F_0^{-1} S + pS^\dagger F_1^{-1} S \leqslant (1 - p)F_0 + pF_1 = F$$

where the first inequality is an equality if and only if $F_0 = F_1$. We conclude that if F is minimal, then it is also extreme. Conversely, if it is not minimal, then there is a non-zero real symmetric positive Δ such that $F \pm \Delta$ are both solutions of (8), and then $F = (F + \Delta)/2 + (F - \Delta)/2$.

In discussing the properties of Gaussian CP maps it is interesting to also apply the previous arguments to the case where S is allowed to be degenerate, i.e. it is a general real, skew-symmetric matrix. Let P be the support projection of $S^\dagger S$; it must be real and symmetric. We must clearly let P be contained in the support of F such that the expression $S^\dagger F^{-1} S$ is well defined. If we assume (8), we can use the inequality

$$(PFP)^{-1} \leqslant PF^{-1}P$$

to conclude that PFP also satisfies (8). The proof of the inequality is simple. Let

$$|x\rangle \in P\mathcal{H} \qquad |y\rangle := F^{-1}|x\rangle \in \mathcal{H} \qquad |z\rangle := (PFP)^{-1}|x\rangle \in P\mathcal{H}.$$

Then the statement follows from

$$\langle y - z|F|y - z\rangle = \langle y|x\rangle - \langle z|x\rangle \geqslant 0 \qquad \forall |x\rangle \in P\mathcal{H}.$$

From this result it follows that for finding the solutions of (11) we can restrict ourselves to matrices F in the subspace $P\mathcal{H}$, and define the matrix inverse in this subspace. One solution of (11) is still $F_0 = (S^\dagger S)^{1/2}$. Introduce the following matrices with support in $P\mathcal{H}$:

$$\mathcal{F} := F_0^{-1/2} F F_0^{-1/2} \qquad V := F_0^{-1/2} S F_0^{-1/2}.$$

We then find that V is real and skew-symmetric with $V^\dagger V = -V^2 = P$, while $\mathcal{F}$ is a real positive (hence symmetric) matrix which satisfies

$$\mathcal{F} = V^\dagger \mathcal{F}^{-1} V. \tag{A1}$$

An explicit construction of all the solutions of (A1) proceeds as follows. First we note that any positive $\mathcal{F}$ is of the form $\mathcal{F} = P \exp \mathcal{L}$ for a real symmetric $\mathcal{L}$. In the subspace $P\mathcal{H}$ it holds that $\det V = \pm 1$, and from (A1) it follows that $\det \mathcal{F} = \pm 1$, and as $\mathcal{F} \geqslant 0$ the only solution is $\det \mathcal{F} = 1$. This means that $\mathcal{L}$ is traceless. Thus, any solution of (A1) is of the exponential form for a real symmetric traceless $\mathcal{L} \in P\mathcal{H}$. Clearly $\mathcal{F}^{-1} = P \exp(-\mathcal{L})$, and by considering the power-series expansion of the exponential it is clear that

$$V^\dagger \mathcal{F}^{-1} V = P\mathrm{e}^{-V^\dagger \mathcal{L} V}.$$

The equality (A1) then implies that

$$\mathcal{L} + V^\dagger \mathcal{L} V = 0. \tag{A2}$$

Conversely, it is clear that any real symmetric $\mathcal{L}$ which satisfies (A2) will be traceless and define a real positive $\mathcal{F}$ of determinant 1 which solves (A1). We now find all the solutions of (A2); for each real symmetric matrix $\mathcal{B}$ in $P\mathcal{H}$ the combination $\mathcal{L} = \mathcal{B} - V^\dagger \mathcal{B} V$ is traceless and satisfies (A2), and every solution of (A2) is of this form (choose $\mathcal{B} = \mathcal{L}/2$). Consequently, we have found all the solutions of (A1). Finally, returning to the original problem, we obtain that the solutions of (11) are precisely the matrices of the form

$$F = F_0^{1/2} \exp\{\mathcal{B} - V^\dagger \mathcal{B} V\} F_0^{1/2}. \tag{A3}$$

We can then easily adapt this form to find all the solutions of (20), (27) and (37).

References

[1] Dieks D 1982 Communication by EPR devices *Phys. Lett.* A **92** 271–2

[2] Wootters W W and Zurek W H 1982 A single quantum cannot be cloned *Nature* **299** 802

[3] Yuen H P 1986 Amplification of quantum states and noiseless photon amplifiers *Phys. Lett.* A **113** 405–7

[4] Barnum H, Caves C M, Fuchs C A, Jozsa R and Schumacher B 1996 Noncommuting mixed states cannot be broadcast *Phys. Rev. Lett.* **76** 2818–21

[5] Lindblad G 1999 A general no-cloning theorem *Lett. Math. Phys.* **47** 189–96

[6] Buzek V and Hillery M 1996 Quantum copying: beyond the no-cloning theorem *Phys. Rev.* A **54** 1844–52

[7] Hillery M and Buzek V 1997 Quantum copying: fundamental inequalities *Phys. Rev.* A **56** 1212–6

[8] Gisin N and Massar S 1997 Optimal quantum cloning machines *Phys. Rev. Lett.* **79** 2153–6

[9] Bruss D, DiVincenzo D P, Ekert A, Macchiavello C and Smolin J A 1998 Optimal universal and state-dependent quantum cloning *Phys. Rev.* A **57** 2368–78

[10] Bruss D, Ekert A and Macchiavello C 1998 Optimal universal quantum cloning and state estimation *Phys. Rev. Lett.* **81** 2598–601

[11] Buzek V and Hillery M 1998 Universal optimal cloning of arbitrary quantum states: from qubits to quantum clones *Phys. Rev. Lett.* **81** 5003–6

[12] Cerf N J 1998 Quantum cloning and the capacity of the Pauli channel *Preprint* quant-ph/9803058

[13] Werner R F 1998 Optimal cloning of pure states *Phys. Rev.* A **58** 1827–32

[14] Cerf N J 1998 Asymmetric quantum cloning machines *Acta Phys. Slovaca* **48** 115–32

[15] Niu C-S and Griffiths R B 1998 Optimal copying of one quantum bit *Phys. Rev.* A **58** 4377–93

[16] Keyl M and Werner R F 1999 Optimal cloning of pure states, judging single clones *J. Math. Phys.* **40** 3283–99

[17] Kraus K 1983 *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Berlin: Springer)

[18] Manuceau J, Sirugue M, Testard D and Verbeure A 1973 The smallest C*-algebra for canonical commutation relations *Commun. Math. Phys.* **32** 231–43

[19] Holevo A S 1982 *Probabilistic and Statistical Aspects of Quantum Theory* (Amsterdam: North-Holland)

[20] Gardiner C W 1991 *Quantum Noise* (Berlin: Springer)

[21] Manuceau J and Verbeure A 1968 Quasi-free states of the CCR-algebra and Bogoliubov transformations *Commun. Math. Phys.* **9** 293–302

[22] Robertson H P 1936 An indeterminacy relation for several observables and its classical interpretation *Phys. Rev.* **48** 794–801

[23] Trifonov D A 1997 Robertson intelligent states *J. Phys. A: Math. Gen.* **30** 5941–57

[24] Holevo A S, Sohma M and Hirota O 1999 Capacity of quantum Gaussian channels *Phys. Rev.* A **59** 1820–28

[25] Demoen B, Vanheuverzwijn P and Verbeure A 1977 Completely positive maps on the CCR algebra *Lett. Math. Phys.* **2** 161–6

[26] Demoen B, Vanheuverzwijn P and Verbeure A 1979 Completely positive quasi-free maps on the CCR algebra *Rep. Math. Phys.* **15** 27–39

[27] Haus H A and Mullen J A 1962 Quantum noise in linear amplifiers *Phys. Rev.* **128** 2407–13

[28] Simon R, Mukunda N and Dutta B 1994 Quantum-noise matrix for multimode systems—$U(n)$ invariance, squeezing and normal forms *Phys. Rev.* A **49** 1567–83

[29] Arvind, Dutta B, Mukunda N and Simon R R 1995 The real symplectic groups in quantum mechanics and optics *Pramana J. Phys.* **45** 471–97

[30] Leonhardt U 1997 *Measuring the Quantum State of Light* (Cambridge: Cambridge University Press)
[31] Caves C M 1982 Quantum limits on noise in linear amplifiers *Phys. Rev.* D **26** 1817–39
[32] Stenholm S 1986 The theory of quantum amplifiers *Phys. Scr.* T **12** 55–66
[33] Campos R A, Saleh B E A and Teich M C 1989 Quantum-mechanical lossless beam splitter: $SU(2)$ symmetry and photon statistics *Phys. Rev.* A **40** 1371–84