isid/ms/2014/8
May 12, 2014
http://www.isid.ac.in/ statmath/eprint

Symplectic Dilations, Gaussian States and Gaussian Channels

K. R. PARTHASARATHY

Indian Statistical Institute, Delhi Centre
7, SJSS Marg, New Delhi–110 016,India

Symplectic Dilations, Gaussian States and Gaussian Channels

K. R. Parthasarathy

Dedicated to Professor Kalyan B. Sinha on his 70th birthday

Abstract By elementary matrix algebra we show that every real $2n \times 2n$ matrix admits a dilation to an element of the real symplectic group $Sp(2(n+m))$ for some nonnegative integer m. Our methods do not yield the minimum value of m, for which such a dilation is possible.
After listing some of the main properties of Gaussian states in $L^2(\mathbb{R}^n)$, we analyse the implications of symplectic dilations in the study of quantum Gaussian channels which lead to some interesting open problems, particularly, in the context of the work of Heinosaari, Holevo and Wolf [3].

Key words: Symplectic matrix and dilation; Weyl operator; Gaussian state, symmetry operator and channel.

1 Symplectic Dilation Theorem

Throughout this section we shall deal with matrices having real entries. Denote by M_n the real linear space of all $n \times n$ matrices. Write

K. R. Parthasarathy
Indian Statistical Institute, Delhi Centre, 7, S. J. S. Sansanwal Marg, New Delhi 110016, e-mail: krp@isid.ac.in

$$J_2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$
$$J_{2n} = \begin{bmatrix} J_2 & 0 & 0 & \dots & 0 \\ 0 & J_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & J_2 \end{bmatrix} \tag{1}$$

where the right hand side is a block diagonal matrix with diagonal blocks J_2 and the nondiagonal entries are 2×2 zero matrices. Let

$$Sp(2n) = \left\{ L \,|\, L \in M_{2n},\, L^T J_{2n} L = J_{2n} \right\}. \tag{2}$$

be the real *symplectic Lie group* of order $2n$, where the index T stands for transpose. It is known that every element L in $Sp(2n)$ has determinant unity and has the property that $L^T \in Sp(2n)$. Any element of $Sp(2n)$ will be called a *symplectic* matrix of order $2n$.

The importance of $Sp(2n)$ in quantum probability lies in the property that the linear transformation

$$L \begin{bmatrix} p_1 \\ q_1 \\ \vdots \\ p_n \\ q_n \end{bmatrix} = \begin{bmatrix} p_1' \\ q_1' \\ \vdots \\ p_n' \\ q_n' \end{bmatrix}$$

of the canonical position and momentum observables in $L^2(\mathbb{R}^n)$ preserves the Heisenberg canonical commutation relations (CCR) if and only if $L \in Sp(2n)$.

The main aim of this section is to establish a dilation theorem according to which any real linear transformation A of the canonical momentum and position observables $\{p_r, q_r, r = 1, 2, \dots, n\}$ can be dilated to a symplectic linear transformation of a larger system $\{p_r, q_r, r = 1, 2, \dots, n+m\}$ of such canonical observables obeying CCR. This is the essence of the following theorem in linear algebra whose proof will be accomplished by examining several special cases.

Theorem 1. *Let $A \in M_{2n}$. Then there exists a nonnegative integer m, not depending on A and matrices B, C, D of respective order $2n \times 2m$, $2m \times 2n$, $2m \times 2m$ such that the block matrix*

$$\widetilde{A} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \tag{3}$$

is a symplectic matrix of order $2(n+m)$.

Lemma 1. *The following matrices of order 4×4 are symplectic.*

(i) $\begin{bmatrix} 0 & B \\ C & 0 \end{bmatrix}$ *where $B, C \in SL(2, \mathbb{R})$.*

(ii) $\begin{bmatrix} \alpha & 0 & 0 & x \\ 0 & 0 & y & 0 \\ 0 & x & \alpha & 0 \\ y & 0 & 0 & 0 \end{bmatrix}$ *where* $\alpha \neq 0, 1+xy=0$.

(iii) $\begin{bmatrix} \alpha & 0 & x & 0 \\ 0 & \alpha & 0 & y \\ -y & 0 & \alpha & 0 \\ 0 & -x & 0 & \alpha \end{bmatrix}$ *where* $xy = 1-\alpha^2$.

(iv) $\begin{bmatrix} \alpha & 0 & x & 0 \\ 0 & -\alpha & 0 & y \\ y & 0 & \alpha & 0 \\ 0 & x & 0 & -\alpha \end{bmatrix}$ *where* $xy = 1+\alpha^2$.

Proof. Straightforward verificaion. □

Lemma 2. *Theorem 1 holds for* $n = 1$ *with* $m = 1$.

Proof. We make a general observation that if an $2n \times 2n$ matrix A satisfies Theorem 1, then so does any matrix L_1AL_2 where L_1 and L_2 are arbitrary elements of $Sp(2n)$. Since $Sp(2) = SL(2,\mathbb{R})$ and for any 2×2 matrix A there exist L_1, L_2 in $SL(2,\mathbb{R})$ such that L_1AL_2 has one of the following forms:

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} \alpha & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}, \begin{bmatrix} \alpha & 0 \\ 0 & -\alpha \end{bmatrix}$$

where $\alpha \neq 0$ is a real scalar. By Lemma 1 each of the four matrices above satisfies Theorem 1 with $m = 1$. □

Definition 1. Let $A \in M_{2n}$. If there exists a matrix $\widetilde{A} \in Sp(2(n+m))$ such that (3) holds we say that $\widetilde{A}$ is a *symplectic dilation* of A of *order* $2(n+m)$.

Lemma 3. *If* $A_i \in M_{2n_i}$ *admits a symplectic dilation of order* $2(n_i+m_i)$, $i = 1,2,\ldots,k$ *then their direct sum*

$$\bigoplus_{i=1}^{k} A_i = \begin{bmatrix} A_1 & 0 & 0 & \ldots & 0 \\ 0 & A_2 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & A_k \end{bmatrix}$$

admits a symplectic dilation of order $2\sum_{i=1}^{k}(n_i+m_i)$.

Proof. It is enough to prove for the case $k = 2$. Let

$$\widetilde{A}_i = \begin{bmatrix} A_i & B_i \\ C_i & D_i \end{bmatrix}$$

be a symplectic dilation of A_i of order $2(n_i+m_i), i = 1,2$. Then

$$\widetilde{A}_1 \oplus \widetilde{A}_2 = \begin{bmatrix} A_1 & B_1 & 0 & 0 \\ C_1 & D_1 & 0 & 0 \\ 0 & 0 & A_2 & B_2 \\ 0 & 0 & C_2 & D_2 \end{bmatrix}$$

is symplectic. First, interchange rows 2 and 3 followed by an interchange of columns 2 and 3 in order to obtain the symplectic matrix

$$\begin{bmatrix} A_1 & 0 & B_1 & 0 \\ 0 & A_2 & 0 & B_2 \\ C_1 & 0 & D_1 & 0 \\ 0 & C_2 & 0 & D_2 \end{bmatrix}$$

of order $2(n_1+m_1+n_2+m_2)$. This is clearly a symplectic dilation of $A_1 \oplus A_2$. □

Lemma 4. *Let A_i, $1 \le i \le k$ be elements of M_{2n}, admitting symplectic dilations $\widetilde{A}_i$ of order $2(n+m)$ for each i. If $p_i > 0$, $1 \le i \le k$ and $\sum_{i=1}^{k} p_i = 1$, then $\sum_{i=1}^{k} p_i A_i$ admits a symplectic dilation of order $2k(n+m)$.*

Proof. Consider the symplectic matrix $L = \bigoplus_{i=1}^{k} \widetilde{A}_i$ of order $2k(n+m)$. Let $((s_{ij}))$ be a real orthogonal matrix with its first row equal to $\left(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k}\right)$. Then

$$S = ((s_{ij}\, I_{2(n+m)}))$$

where I_r denotes identity matrix of order r, is a symplectic matrix of order $2(n+m)k$. Thus SLS^T is also symplectic. Considering this as a block matrix of the form (3) we see that SLS^T is a symplectic dilation of $\sum_{i=1}^{k} p_i A_i$. □

Lemma 5. *Let A be a real strictly positive definite matrix of order $2n$. Then A admits a symplectic dilation of order $4n$.*

Proof. By Williamson's theorem [1], [9] there exists a symplectic matrix L of order $2n$ such that

$$L^T A L = \kappa_1 I_2 \oplus \kappa_2 I_2 \oplus \cdots \oplus \kappa_n I_2$$

where I_2 is the identity matrix of order 2 and $\kappa_1 \ge \kappa_2 \ge \cdots \ge \kappa_n > 0$ are the unique Williamson parameters of A. By expression (iii) in Lemma 1, each $\kappa_j I_2$ has a symplectic dilation of order 4. Now Lemma 3 implies that $L^T A L$ has a symplectic dilation of order $4n$. □

Lemma 6. *Let A be a symmetric matrix of order $2n$. Then A admits a symplectic dilation of order $8n$.*

Proof. Choose and fix a constant $\lambda > 0$ so that $\lambda I + A$ and $\lambda I - A$ are both strictly positive definite. By Lemma 5 both $\lambda I + A$ and $\lambda I - A$ admit symplectic dilations of order $4n$. When L is symplectic so is $-L$ and therefore $A - \lambda I$ has a symplectic

dilation of order $4n$. Now, by Lemma 4, $A = \frac{1}{2}(A+\lambda I + A - \lambda I)$ admits a symplectic dilation of order $8n$. □

Lemma 7. *Let D,E,F,G be 2×2 matrices such that $\begin{bmatrix} D & E \\ F & G \end{bmatrix}$ is symplectic of order 4. Then the 8×8 matrix*

$$\begin{bmatrix} 0 & D & E & 0 \\ -D^T & 0 & 0 & -F^T \\ 0 & F & G & 0 \\ -E^T & 0 & 0 & -G^T \end{bmatrix}$$

is symplectic. In particular, any 4×4 skew symetric matrix of the form $\begin{bmatrix} 0 & D \\ -D^T & 0 \end{bmatrix}$ admits a symplectic dilation of order 8.

Proof. Straightforward algebra. □

Proof of Theorem 1. By Lemma 1 it is enough to consider the case $n > 1$. Express the $2n \times 2n$ matrix A as an $n \times n$ block matrix

$$A = [A_{ij}], \quad i,j \in \{1,2,\ldots,n\}$$

where each A_{ij} is of order 2×2. Then A can be written as

$$A = A_1 + A_2 + A_3$$

where $A_1 = \frac{1}{2}(A + A^T)$ is symmetric, A_2 is the block diagonal matrix

$$\frac{1}{2}\left\{(A_{11} - A_{11}^T) \oplus (A_{22} - A_{22}^T) \oplus \cdots \oplus (A_{nn} - A_{nn}^T)\right\}$$

and

$$A_3 = \sum_{1\le i<j\le n} B_{ij}$$

with B_{ij} being a block matrix with ijth block $\frac{1}{2}\left(A_{ij} - A_{ji}^T\right)$ and jith block $\frac{1}{2}\left(A_{ji} - A_{ij}^T\right)$ and all other blocks equal to 0. Write $A_1 = A_1^+ - A_1^-$ where $A^{\pm}$, are positive and negative parts of A_1. Put $B_1 = A_1^+ + \varepsilon I$, $B_2 = A_1^- + \varepsilon I$ where $\varepsilon > 0$, so that B_1 and B_2 are strictly positive definite. Then $A_1 = B_1 - B_2$ where, by Lemma 5, B_1 and B_2 admit symplectic dilations of order $4n$. By Lemma 2 and Lemma 3, A_2 has a symplectic dilation of order $4n$. Now each of the matrices B_{ij} can be looked upon as a direct sum of

$$\begin{bmatrix} 0 & \frac{1}{2}\left(A_{ij} - A_{ji}^T\right) \\ \frac{1}{2}\left(A_{ji} - A_{ij}^T\right) & 0 \end{bmatrix}$$

and the zero matrix of order $(2n-4)\times(2n-4)$. By Lemma 7 and Lemma 3 and the fact that

$$\begin{bmatrix} 0 & I_{2n-4} \\ I_{2n-4} & 0 \end{bmatrix} \in Sp(4n-8)$$

it follows that each B_{ij} has a symplectic dilation of order $8+4n-8=4n$. The same arguments apply to scalar multiples of B_1, B_2, A_2 and the B_{ij}'s. Put $k=\binom{n}{2}+3$ and write

$$A=\frac{1}{k}\left(kB_1+(-k)B_2+kA_2+\sum_{1\le i<j\le n} kB_{ij}\right), \tag{4}$$

a convex combination of the summands within the brackets ( ). Each summand on the right hand side of (4) has a symplectic dilation of order $4n$. By Lemma 4 it now follows that A admits a symplectic dilation of order $4n(\binom{n}{2}+3)$. □

Remark 1. Theorem 1 and its proof show that every real matrix A of order $2n\times 2n$ admits a symplectic dilation of order $4n(\binom{n}{2}+3)$. The problem of finding the size of the minimal symplectic dilation of a matrix of order $n\times n$ remains open.

2 The Symplectic Group, Weyl operators and Gaussian States

We shall present in this section a brief account of the role of the group $Sp(2n)$ in describing Gaussian states in $L^2(\mathbb{R})$ and some of their properties which are important in the formulation of the notion of Gaussian channels in quantum information theory. For proofs of results stated here we refer to Holevo [4] and Parthasarathy [6], [7].

Consider the complex Hilbert space $\mathbb{C}^n$ and $L^2(\mathbb{R}^n)$, the space of complex-valued, absolutely square integrable functions with respect to the n-dimensional Lebesgue measure. We shall write all scalar products in the Dirac notation. For any $\mathbf{u}=(u_1,u_2,\ldots,u_n)^T$ in $\mathbb{C}^n$, associate the *exponential vector* $e(\mathbf{u})$ in $L^2(\mathbb{R}^n)$ by

$$e(\mathbf{u})(\mathbf{x})=(2\pi)^{-n/4}\exp\sum_{j=1}^{n}\left(u_jx_j-\frac{1}{2}u_j^2-\frac{1}{4}x_j^2\right) \tag{5}$$

for $\mathbf{x}\in\mathbb{R}^n$. Exponential vectors span a dense linear manifold $\mathscr{E}\subset L^2(\mathbb{R}^n)$ and any finite number of exponential vectors are linearly independent. Furthermore,

$$\begin{aligned}\langle e(\mathbf{u})\big|e(\mathbf{v})\rangle &= \exp\langle\mathbf{u}|\mathbf{v}\rangle \\ &= \exp\sum_{j=1}^{n}\overline{u}_jv_j.\end{aligned}$$

In particular,

$$|\psi(\mathbf{u})\rangle=e^{-\frac{1}{2}\|\mathbf{u}\|^2}|e(\mathbf{u})\rangle$$

is a unit vector and the pure state determined by this vector is called the *coherent state* associated with $\mathbf{u}$.

For any $\mathbf{u} \in \mathbb{C}^n$, there exists (an exponential like) unitary operator $W(\mathbf{u})$ in $L^2(\mathbb{R}^n)$, called *Weyl operator* associated with $\mathbf{u}$, satisfying the relations

$$W(\mathbf{u})|e(\mathbf{v})\rangle = e^{-\frac{1}{2}\|\mathbf{u}\|^2 - \langle \mathbf{u}|\mathbf{v}\rangle} \ |e(\mathbf{u}+\mathbf{v})\rangle \tag{6}$$

for all $\mathbf{v} \in \mathbb{C}^n$. For a given $\mathbf{u}$ such a $W(\mathbf{u})$ is uniquely defined. They obey the Weyl commutation relations

$$W(\mathbf{u})W(\mathbf{v}) = e^{-i\mathscr{I}m\langle \mathbf{u}|\mathbf{v}\rangle}W(\mathbf{u}+\mathbf{v}). \tag{7}$$

It is a multiplicative family of operators modulo a scalar multiplier. From (7) one gets

$$W(\mathbf{u})W(\mathbf{v})W(\mathbf{u})^{-1} = e^{-2i\mathscr{I}m\langle \mathbf{u}|\mathbf{v}\rangle}W(\mathbf{v}). \tag{8}$$

The correspondence $\mathbf{u} \to W(\mathbf{u})$ is a strongly continuous, projective, unitary and irreducible representation of the additive group $\mathbb{C}^n$. If we identify $L^2(\mathbb{R}^{n+m})$ with $L^2(\mathbb{R}^n) \otimes L^2(\mathbb{R}^m)$ and $\mathbb{C}^{n+m}$ with $\mathbb{C}^n \oplus \mathbb{C}^m$, then $W(\mathbf{u} \oplus \mathbf{v})$ gets identified with $W(\mathbf{u}) \otimes W(\mathbf{v})$ and we simply write $W(\mathbf{u} \oplus \mathbf{v}) = W(\mathbf{u}) \otimes W(\mathbf{v})$. This is called the *factorizability* property of the Weyl representation $\mathbf{u} \to W(\mathbf{u})$.

Suppose $\mathbf{u} \to W'(\mathbf{u})$ is a strongly continuous map from $\mathbb{C}^n$ into the unitary group of a complex separable Hilbert space $\mathscr{H}$ satisfying equation (7) with W replaced by W'. Then, according to Stone-von Neumann theorem there is a unitary isomorphism Γ from $\mathscr{H}$ onto $L^2(\mathbb{R}^n) \otimes k$ for some Hilbert space k such that

$$\Gamma W'(\mathbf{u})\Gamma^{-1} = W(\mathbf{u}) \otimes I_k \quad \forall \quad \mathbf{u} \in \mathbb{C}^n,$$

I_k being the identity opertor in k. If W' is also irreducible then W and W' are unitarily equivalent.

For any $L \in Sp(2n)$ define the action of L on $\mathbf{u}$ by $L \cdot \mathbf{u} = \mathbf{u}'$ where

$$L \begin{bmatrix} \mathscr{R}e\, u_1 \\ \mathscr{I}m\, u_1 \\ \vdots \\ \mathscr{R}e\, u_n \\ \mathscr{I}m\, u_n \end{bmatrix} = \begin{bmatrix} \mathscr{R}e\, u'_1 \\ \mathscr{I}m\, u'_1 \\ \vdots \\ \mathscr{R}e\, u'_n \\ \mathscr{I}m\, u'_n \end{bmatrix} \quad \forall \quad \mathbf{u} \in \mathbb{C}^n.$$

Then such an action preserves the real bilinear form $\mathscr{I}m\langle \mathbf{u}|\mathbf{v}\rangle$ and therefore

$$W(L \cdot \mathbf{u})W(L \cdot \mathbf{v}) = e^{-i\mathscr{I}m\langle \mathbf{u}|\mathbf{v}\rangle}W(L \cdot (\mathbf{u}+\mathbf{v})).$$

Hence by the discussion above there exists a unitary operator, say $\Gamma(L)$, such that

$$\Gamma(L)W(\mathbf{u})\Gamma(L)^{-1} = W(L \cdot \mathbf{u}) \quad \forall\, \mathbf{u} \in \mathbb{C}^n. \tag{9}$$

Since the projective representation $\mathbf{u} \to W(L \cdot \mathbf{u})$ is also irreducible it follows that the choice of the unitary operator $\Gamma(L)$ is unique upto a scalar multiple of modulus unity. Thus the map $L \to \Gamma(L)$ is a projective unitary representation of $Sp(2n)$. If U

is a unitary matrix of order $n \times n$, U preserves the scalar product in $\mathbb{C}^n$ and hence preserves $\mathscr{I}m\langle \mathbf{u}|\mathbf{v}\rangle$. In other words there exists a matrix $L^U \in Sp(2n) \cap SO(2n)$ such that $L^U \cdot \mathbf{u} = U\mathbf{u}$. There exists a unique unitary operator $\Gamma_0(U)$ in $L^2(\mathbb{R}^n)$ such that

$$\Gamma_0(U)e(\mathbf{u}) = e(U\mathbf{u}) \quad \forall \quad \mathbf{u} \in \mathbb{C}^n.$$

Then $\Gamma_0(U)\Gamma_0(U') = \Gamma_0(UU')$ for any $U, U' \in U(n)$ and $\Gamma(L^U)$ can be chosen to be $\Gamma_0(U)$. The representation $U \to \Gamma_0(U)$ of $U(n)$ is called the *second quantization* map. Thus we get a projective unitary representation $L \to \Gamma(L)$ of $Sp(2n)$ such that (9) holds, $\Gamma(L_1)\Gamma(L_2) = \Gamma(L_1L_2)$ whenever L_1 and L_2 are symplectic and orthogonal but, in general,

$$\Gamma(L_1)\Gamma(L_2) = \sigma(L_1, L_2)\Gamma(L_1L_2)$$

where $\sigma(L_1, L_2)$ is a scalar of modulus unity.

Definition 2. A *state* ρ in $L^2(\mathbb{R}^n)$ is a positive operator of unit trace and its *quantum Fourier transform* $\widehat{\rho}(\mathbf{u})$ is the complex-valued function on $\mathbb{C}^n$ defined by

$$\widehat{\rho}(\mathbf{u}) = \text{Tr } \rho W(\mathbf{u}) \quad \forall \quad \mathbf{u} \in \mathbb{C}^n.$$

The quantum Fourier transform of a state satisfies the following properties:

(i) $\widehat{\rho}(\mathbf{0}) = 1$ and the map $\mathbf{u} \to \widehat{\rho}(\mathbf{u})$ is continuous on $\mathbb{C}^n$.

(ii) The kernel

$$k_\rho(\mathbf{u}, \mathbf{v}) = e^{i\mathscr{I}m\langle \mathbf{u}|\mathbf{v}\rangle}\widehat{\rho}(\mathbf{v} - \mathbf{u}), \mathbf{u}, \mathbf{v} \in \mathbb{C}^n$$

is positive definite, i.e., for any finite set $\{\mathbf{u}_r, 1 \leq r \leq m\} \subset \mathbb{C}^n$ and scalars $c_r, 1 \leq r \leq m$

$$\Sigma \overline{c}_r c_s \, k_\rho(\mathbf{u}_r, \mathbf{u}_s) \geq 0.$$

(iii) (Inversion formula) For any state ρ in $L^2(\mathbb{R}^n)$

$$\begin{aligned} \rho &= \frac{1}{\pi^n} \int \widehat{\rho}(\mathbf{u}) \, W(-\mathbf{u}) d^{2n}\mathbf{u} \\ &= \frac{1}{\pi^n} \int \overline{\widehat{\rho}(\mathbf{u})} \, W(\mathbf{u}) d^{2n}\mathbf{u}, \end{aligned}$$

where $d^{2n}\mathbf{u}$ is the $2n$-dimensional Lebesgue measure when $\mathbb{C}^n$ is considered as the real linear space $\mathbb{R}^{2n}$.

(iv) (Quantum Bochner's Theorem) let φ be any complex-valued continuous function on $\mathbb{C}^n$ such that $\varphi(\mathbf{0}) = 1$ and the kernel $k(\mathbf{u}, \mathbf{v}) = \varphi(\mathbf{v} - \mathbf{u}) \exp i\langle \mathbf{u}|\mathbf{v}\rangle$ is positive definite. Then there exists a unique state ρ in $L^2(\mathbb{R}^n)$ such that $\widehat{\rho} = \varphi$

(v) For any state ρ in $L^2(\mathbb{R}^n)$ and any $L \in Sp(2n)$

$$\left[\Gamma(L) \, \rho \, \Gamma(L)^{-1}\right]^\wedge(\mathbf{u}) = \widehat{\rho}(L^{-1}\mathbf{u}) \quad \forall \quad \mathbf{u} \in \mathbb{C}^n.$$

(vi) For any state ρ in $L^2(\mathbb{R}^{n+m}) = L^2(\mathbb{R}^n) \otimes L^2(\mathbb{R}^m)$ define the *marginal* states ρ_1 and ρ_2 in $L^2(\mathbb{R}^n)$ and $L^2(\mathbb{R}^m)$ respectively by

$$\rho_1 = \mathrm{Tr}_2\,\rho, \quad \rho_2 = \mathrm{Tr}_1\,\rho$$

where Tr_1 and Tr_2 are the relative traces of ρ over the factors $L^2(\mathbb{R}^n)$ and $L^2(\mathbb{R}^m)$ respectively. Then

$$\widehat{\rho}_1(\mathbf{u}) = \widehat{\rho}(\mathbf{u}\oplus\mathbf{0}),$$
$$\widehat{\rho}_2(\mathbf{v}) = \widehat{\rho}(\mathbf{0}\oplus\mathbf{v})$$

where $\mathbf{u}\in\mathbb{C}^n$, $\mathbf{v}\in\mathbb{C}^m$.

Definition 3. A state ρ in $L^2(\mathbb{R}^n)$ is said to be *Gaussian* if its quantum Fourier transform has the form

$$\widehat{\rho}(\mathbf{u}) = \exp\, P(x_1,y_1,\ldots,x_n,y_n) \quad \forall \quad \mathbf{u}\in\mathbb{C}^n$$

where $x_j = \mathrm{Re}\,u_j$, $y_j = Im\,u_j$ and P is a polynomial in $2n$ variables of degree at most 2.

Theorem 2. *A state ρ in $L^2(\mathbb{R}^n)$ is Gaussian if and only there exist vectors ℓ, $\mathbf{m}$ in $\mathbb{R}^n$ and a real positive definite matrix S of order $2n$ satisfying the inequality*

$$2S - i\,J_{2n} \geq 0, \tag{10}$$

such that the quantum Fourier transform $\widehat{\rho}(\mathbf{u})$ is given by

$$\widehat{\rho}(\mathbf{u}) = \exp -i\sqrt{2}\left(\ell^T\,\mathbf{x} - \mathbf{m}^T\mathbf{y}\right) - \left(\mathbf{x}^T,\mathbf{y}^T\right) S\begin{pmatrix}\mathbf{x}\\ \mathbf{y}\end{pmatrix} \quad \forall\,\mathbf{u}\in\mathbb{C}^{2n} \tag{11}$$

where $x_j = Re\,u_j$, $y_j = Im\,u_j$, $1\leq j\leq n$ and J_{2n} is given by (1).

Proof. See [6].

Remark 2. We shall give now an interpretation of the parameters ℓ, $\mathbf{m}$ and S occuring in (11) and also the matrix inequality (10) in the language of the momentum and position observables obeying CCR. To this end we first observe that (7) implies that for any fixed $\mathbf{u}$, $\{W(t\mathbf{u}), t\in\mathbb{R}\}$ is a strongly continuous one parameter group of unitary operators admitting a self adjoint Stone generator $p(\mathbf{u})$ so that

$$W(t\mathbf{u}) = e^{-it\,p(\mathbf{u})}, \mathbf{u}\in\mathbb{C}^n, t\in\mathbb{R}.$$

Writing $\mathbf{e}_j = (0,\ldots,0,1,0,\ldots,0)^T$ for $1\leq j\leq n$, where 1 occurs in the jth position and putting

$$p_j = 2^{-\frac{1}{2}}\,p(e_j),\; q_j = -2^{-\frac{1}{2}}p(ie_j)$$

we obtain selfadjoint operators obeying CCR on the linear manifold $\mathscr{E}$ generated by the exponential vectors. Then $W(\mathbf{u})$ can be expressed as

$$W(\mathbf{u}) = \exp -i\sqrt{2}\sum_{j=1}^{n}(x_jp_j - y_jq_j)$$

with $x_j = \mathrm{Re}\, u_j$, $y_j = \mathscr{I}m\, u_j$ for every j and $\sum_{j=1}^n (x_j p_j - y_j q_j)$ being the selfadjoint closure from $\mathscr{E}$. From the definition of quantum Fourier transform and (11) it follows that each observable $p(\mathbf{u})$ has a normal distribution in the Gaussian state ρ with characteristic function

$$\exp -it\sqrt{2}\sum_{j=1}^{n}(\ell_j x_j - m_j y_j) - t^2 \xi^T S \xi, \quad t \in \mathbb{R}$$

where $\xi^T = (x_1, y_1, x_2, y_2, \ldots, x_n, y_n)$. Thus

$$\ell_j = \mathrm{Tr}\,\rho\, p_j, \quad m_j = \mathrm{Tr}\,\rho\, q_j$$

and the covariance matrix of $(p_1, -q_1, \ldots, p_n, -q_n)$ is S. When (11) holds we write

$$\rho = \rho_g(\ell, \mathbf{m}, S) \tag{12}$$

in order to indicate that ρ is a Gaussian state with *mean* momentum and position vectors $\ell, \mathbf{m}$ respectively and *covariance matrix* S. If we write

$$(Z_1, Z_2, \ldots, Z_{2n}) = (p_1, -q_1, \ldots, p_n, -q_n)$$

then

$$\mathrm{Cov}(Z_r, Z_s) = \mathrm{Tr}\,\frac{Z_r Z_s + Z_s Z_r}{2}\rho - (\mathrm{Tr}\, Z_r \rho)(\mathrm{Tr}\, Z_s \rho)$$

is the rs-th entry of S. With this convention the inequality (10) encapsulates the uncertainty principle for all momentum - position pairs (P, Q) where

$$Q = \sum_{r=1}^{n} (x_r p_r - y_r q_r)$$
$$P = \sum_{r=1}^{n} \left(x'_r p_r - y'_r q_r\right)$$

and $\sum_{r=1}^{n} (x_r y'_r - x'_r y_r) = 1$, x_r, y_r, x'_r, y'_r being real scalars.

We now enumerate some of the basic properties of Gaussian states, parametrized as in (12). They are essentially corollaries of Theorem 2 and the basic properties of quantum Fourier transform mentioned earlier.

(i) Tensor products and marginals of Gaussian states are Gaussian.
(ii) (Tranformation property) For any $\mathbf{u} = \mathbf{s} + i\mathbf{t}, \mathbf{s}, \mathbf{t} \in \mathbb{R}^n$,

$$W(\mathbf{u})\rho_g(\ell, \mathbf{m}, S)W(\mathbf{u})^{-1} = \rho_g(\ell + \sqrt{2}\mathbf{t}, \mathbf{m} + \sqrt{2}\mathbf{s}, S),$$

and for any $L \in Sp(2n)$,

$$\Gamma(L)\rho_g(\ell, \mathbf{m}, S)\Gamma(L)^{-1} = \rho_g(\ell', \mathbf{m}', S')$$

where

$$\begin{bmatrix} \ell_1' \\ -m_1' \\ \vdots \\ \ell_n' \\ -m_n' \end{bmatrix} = (L^{-1})^T \begin{bmatrix} \ell_1 \\ -m_1 \\ \vdots \\ \ell_n \\ -m_n \end{bmatrix},$$

$$S' = (L^{-1})^T S L^{-1}$$

(iii) If Γ is any unitary operator in $L^2(\mathbb{R}^n)$ satisfying the property that $\Gamma\rho\Gamma^{-1}$ is a Gaussian state whenever ρ is a Gaussian state in $L^2(\mathbb{R}^n)$ then Γ is given by

$$\Gamma = \lambda W(\mathbf{u})\Gamma(L) \tag{13}$$

for some complex scalar λ of mudulus unity, $\mathbf{u} \in \mathbb{C}^n$ and $L \in Sp(2n)$.
In view of properties (ii) and (iii) any unitary operator Γ of the form (13) is called a *Gaussian symmetry operator*. All Gaussian symmetry operators in $L^2(\mathbb{R}^n)$ constitute a group $\mathscr{G}_n$.
Suppose U is a unitary operator in $L^2(\mathbb{R}^n)$ such that for every pure Gaussian state $|\psi\rangle$ the pure state $U|\psi\rangle$ is also Gaussian. Is U a Gaussian symmetry operator? We do not know the answer.

(iv) The covariance matrix S in $\rho_g(\ell, \mathbf{m}, S)$ admits a representation

$$S = L^T(\kappa_1 I_2 \oplus \kappa_2 I_2 \oplus \cdots \oplus \kappa_n I_2)L$$

for some $L \in Sp(2n)$, $\kappa_1 \geq \kappa_2 \geq \cdots \geq \kappa_n \geq \frac{1}{2}$. In such a representation L need not be unique but $\kappa_1, \kappa_2, \ldots, \kappa_n$ are unique. The κ_j's are the *Williamson parameters* of S.

(v) The covariance matrix S of a Gaussian state in $L^2(\mathbb{R}^n)$ admits a representation

$$S = \frac{1}{4}\left(L^T L + M^T M\right)$$

for some L, M in $Sp(2n)$. Such a representation need not be unique. In the convex set $\mathscr{K}_n$ of all Gaussian covariance matrices of order $2n$, an element S is an extreme point if and only if $S = \frac{1}{2}L^T L$ for some L in $Sp(2n)$. A Gaussian state ρ in $L^2(\mathbb{R}^n)$ is pure if and only if its covariance matrix is of the form $\frac{1}{2}L^T L$ for some L in $Sp(2n)$ and in such a case its wave function $|\psi\rangle$ has the form

$$|\psi\rangle = W(\mathbf{u})\Gamma(L)\,|e(\mathbf{0})\rangle.$$

Every coherent state is Gaussian with covariance matrix $\frac{1}{2}I_{2n}$.

(vi) (Gaussian purification property) Let $\rho_g(\ell, \mathbf{m}, S)$ be a Gaussian state in $L^2(\mathbb{R}^n)$ with

$$S = \frac{1}{4}\left(L_1^T L_1 + L_2^T L_2\right)$$

as in property (v). Put

$$|\psi_j\rangle = \Gamma(L_j)^{-1}|e(\mathbf{0})\rangle, \quad j = 1,2,$$

and define the second quantization unitary operator Γ_0 in $L^2(\mathbb{R}^n)\otimes L^2(\mathbb{R}^n)$ by the relations

$$\Gamma_0 e(\mathbf{v}\oplus\mathbf{v}') = e\left(\frac{\mathbf{v}+\mathbf{v}'}{\sqrt{2}}\oplus\frac{\mathbf{v}-\mathbf{v}'}{\sqrt{2}}\right) \quad \forall \quad \mathbf{v},\mathbf{v}'\in\mathbb{C}^n.$$

Putting

$$\Gamma = \left(W\left(\frac{\mathbf{m}+i\boldsymbol{\ell}}{\sqrt{2}}\right)\otimes I\right)\Gamma_0$$

one gets a purification of $\rho_g(\boldsymbol{\ell},\mathbf{m},S)$ as

$$\rho_g(\boldsymbol{\ell},\mathbf{m},S) = \mathrm{Tr}_2\,\Gamma\left(|\psi_1\rangle\langle\psi_1|\otimes|\psi_2\rangle\langle\psi_2|\right)\Gamma^{-1}$$

where the pure state within Tr_2 is also Gaussian.

(vii) (von Neumann entropy of $\rho_g(\boldsymbol{\ell},\mathbf{m},S)$)

First write

$$\rho_g(\boldsymbol{\ell},\mathbf{m},S) = W\left(\frac{\mathbf{m}+i\boldsymbol{\ell}}{\sqrt{2}}\right)\rho_g(0,0,S)W\left(\frac{\mathbf{m}+i\boldsymbol{\ell}}{\sqrt{2}}\right)^{-1}$$

using transformaton property (ii). Using property (iv) and the Williamson parameters $\kappa_1\geq\kappa_2\geq\cdots\geq\kappa_n\geq\frac{1}{2}$ we express

$$\rho_g(\boldsymbol{\ell},\mathbf{m},S) = W\left(\frac{\mathbf{m}+i\boldsymbol{\ell}}{\sqrt{2}}\right)\Gamma(L)^{-1}\bigotimes_{j=1}^{r}\rho_g(\mathbf{0},\mathbf{0},\kappa_j I_2)\bigotimes\rho_g(0,0,\frac{1}{2}I_2)^{\otimes n-r}\,\Gamma(L)W\left(\frac{\mathbf{m}+i\boldsymbol{\ell}}{\sqrt{2}}\right)$$

where we assume

$$\begin{aligned}\kappa_j &> \frac{1}{2} \quad \text{if} \quad 1\leq j\leq r,\\ &= \frac{1}{2} \quad \text{if} \quad r+1\leq j\leq n.\end{aligned}$$

In $L^2(\mathbb{R})$ denote the momentum and position operators by p and q respectively and note that

$$\rho_g(\mathbf{0},\mathbf{0},\kappa I_2) = \begin{cases}|e(\mathbf{0})\rangle\langle e(\mathbf{0}| & \text{if} \quad \kappa=\frac{1}{2},\\ (1-e^{-s}e^{-\frac{1}{2}s(p^2+q^2-1)}) & \text{if} \quad \kappa>\frac{1}{2}\end{cases} \tag{14}$$

where s is given by $\kappa=\frac{1}{2}\coth\frac{1}{2}s$ with $s>0$. Writing $\kappa_j=\frac{1}{2}\coth\frac{1}{2}s_j, \quad s_j>0, \quad 1\leq j\leq r$ we see that $\rho_g(\boldsymbol{\ell},\mathbf{m},S)$ is unitarily equivalent to the tensor product state

$$\bigotimes_{j=1}^{r}\left(1-e^{-s_j}\right)e^{-\frac{1}{2}s_j(p_j^2+q_j^2-1)}\otimes\left(|e(0)\rangle\langle e(0)|\right)^{\otimes n-r}.$$

In particular, every Gaussian state is conjugate by a Gaussian symmetry operator to a product of r thermal states and $(n-r)$ vaccuum states in $L^2(\mathbb{R})$ where $0 \leq r \leq n$.

The von Neumann *entropy* of a state ρ denoted by $S(\rho)$ is defined as the quantity $-\mathrm{Tr}\,\rho\,\log\,\rho$. If ρ has eigenvalues $\lambda_1, \lambda_2, \ldots$ inclusive of multiplicity then $S(\rho) = -\sum_j \lambda_j \log \lambda_j$. Thus $S(U\rho U^{-1}) = S(\rho)$ for any unitary operator U and $S(\rho_1 \otimes \rho_2) = S(\rho_1) + S(\rho_2)$ for any product state $\rho_1 \otimes \rho_2$. Thus

$$S(\rho_g(\ell, \mathbf{m}, S)) = \sum_{j=1}^{r} S(\rho_g(0,0,\kappa_j I_2)).$$

Since the number operator $\frac{1}{2}(p^2+q^2-1)$ has eigenvalues $0,1,2,\ldots$ with multiplicity 1 each, it follows from (14) that

$$S(\rho_g(0,0,\kappa I_2)) = \begin{cases} 0 \quad \text{if} \quad \kappa = \frac{1}{2}, \\ \frac{2}{2\kappa+1} H\left(\frac{2\kappa-1}{2\kappa+1}\right) \quad \text{if} \quad \kappa > \frac{1}{2} \end{cases}$$

where H is the Shannon entropy function given by $H(t) = -t\log t - (1-t)\log(1-t)$, $0 \leq t \leq 1$ with $H(0) = H(1) = 0$. Thus

$$S(\rho_g(\ell, \mathbf{m}, S)) = \sum_{j=1}^{n} \frac{2}{2\kappa_j + 1} H\left(\frac{2\kappa_j - 1}{2\kappa_j + 1}\right)$$

where $\kappa_1 \geq \kappa_2 \geq \cdots \geq \kappa_n \geq \frac{1}{2}$ are the Williamson parameters of S.

3 Gaussian Channels

A *quantum channel* is a completely positive, trace preserving and linear map on the algebra $\mathscr{B}(\mathscr{H})$ of all bounded operators on a complex Hilbert space $\mathscr{H}$. If T is such a channel and $\rho_{\text{in}} = \rho$ is an input state the channel gives an output state$\rho_{\text{out}} = T(\rho)$. Such a channel is treated as a communication resource. If $\mathscr{H} = L^2(\mathbb{R}^n)$ we say that a channel T is *Gaussian* if, for every Gaussian state ρ, the output state $T(\rho)$ is also Gaussian. The set of all channels in $L^2(\mathbb{R}^n)$ is a semigroup under composition and also a convex set under mixture. The set of all Gaussian channels is a subsemigroup of the semigroup of all channels in $L^2(\mathbb{R}^n)$. We shall present some examples of Gaussian channels and conclude with some open problems.

Example 1 (Reversible Gaussian Channels). If U is a Gaussian symmetry operator as defined at the end of property (iii) of Gaussian states in Section 2, then $T(\rho) = U\rho U^{-1}$ defines a Gaussian channel. $T^{-1}(\rho) = U^{-1}\rho U$ is the reverse of such a Gaussian channel with $T^{-1} \circ T =$ identity. These are the only reversible Gaussian channels.

Example 2 (Bosonic Gaussian channels [2], [5]). Let ξ_j, η_j, $1 \leq j \leq n$ be real-valued mean zero random variables with a joint normal distribution and let $\zeta_j =$

$\xi_j + i\eta_j$. Write $\zeta^T = (\zeta_1, \zeta_2, \ldots, \zeta_n)$ and put

$$T(\rho) = \mathbb{E}W(\zeta)\ \rho\ W(\zeta)^{-1} \tag{15}$$

where $\mathbb{E}$ denotes expectation with respect to the probability distribution of ζ and $W(\zeta)$ is the Weyl operator at ζ. If $\rho = \rho_g(\ell, \mathbf{m}, S)$ in $L^2(\mathbb{R}^n)$ as defined in (12), then (8) implies that the quantum Fourier transform of $T(\rho)$ is given by

$$\begin{aligned} T(\rho)^\wedge(\mathbf{u}) &= \mathrm{Tr}\,\mathbb{E}W(\zeta)\rho_g(\ell, \mathbf{m}, S)W(\zeta)^{-1}W(\mathbf{u}) \\ &= \rho_g(\ell, \mathbf{m}, S)^\wedge(\mathbf{u})\,\mathbb{E}\,e^{2i\mathscr{I}m\langle\zeta|\mathbf{u}\rangle}. \end{aligned}$$

If $\mathbf{u} = \mathbf{s} + i\mathbf{t}$ where $\mathbf{s}$ and $\mathbf{t}$ are in $\mathbb{R}^n$ and the covariance matrix of the Gaussian random vector $\sqrt{2}(-\eta^T, \xi^T)$ is C then it follows that

$$T(\rho_g(\ell, \mathbf{m}, S)) = \rho_g(\ell, \mathbf{m}, S + C).$$

Thus T is a Gaussian channel which changes the covariance matrix S of the input Gaussian state to the covariance matrix $S+C$ of the output Gaussian state but leaves the mean momentum-position vector unchanged.

If P is the probability distribution of the Gaussian random vector ζ in (15) and $\{H_\mathbf{k}, \mathbf{k} = (k_1, k_2, \ldots, k_{2n})\}$ is the Hermite basis of orthonormal polynomials in $L^2(P)$, define the operators

$$L_\mathbf{k} = \mathbb{E}\, H_\mathbf{k}(\xi, \eta)W(\zeta).$$

Then the channel T in (15) can also be written as

$$T(\rho) = \sum_\mathbf{k} L_\mathbf{k}\ \rho\ L_\mathbf{k}^\dagger$$

in the Kraus or operator sum form.

Example 3 (Symplectic Gaussian channels). Choose and fix a mean $\mathbf{0}$ Gaussian state ρ_0 in$L^2(\mathbb{R}^m)$ and fix a symplectic matrix $L \in Sp(2(n+m))$. For any state ρ in $L^2(\mathbb{R}^n)$ define

$$T(\rho) = \mathrm{Tr}_2\ \Gamma(L)(\rho \otimes \rho_0)\Gamma(L)^\dagger \tag{16}$$

where $\Gamma(L)$ is the Gaussian symmetry operator associated with L and Tr_2 is the relative trace over the component $L^2(\mathbb{R}^m)$ in $L^2(\mathbb{R}^n) \otimes L^2(\mathbb{R}^m) = L^2(\mathbb{R}^{n+m})$. Since conjugation by a unitary operator and relative trace are completely positive and trace preseving, it follows that T as defined in (16) is a channel. If ρ is Gaussian it follows from Example 1 and property (i) of Gaussian states in Section 2 that T is Gaussian. We call T in (16) a *symplectic Gaussian channel*.

We shall now examine how a *symplectic Gaussian channel* changes the mean and covariance parameters of a Gaussian state. By the Gaussian purificaton property (vi) of a Gaussian state in Section 2, $L^2(\mathbb{R}^m)$ can be replaced by $L^2(\mathbb{R}^m) \otimes L^2(\mathbb{R}^m)$ and ρ_0 in (16) by a pure Gaussian state which is determined by a unit vector of the form $\Gamma(M)\ |e(\mathbf{0})\rangle$ in $L^2(\mathbb{R}^{2m})$ with $M \in Sp(2m)$. Put $k = 2m$ and note that T in (16) can

as well be replaced by

$$T(\rho) = \mathrm{Tr}_2\, \Gamma(L)\, \rho \otimes |e(\mathbf{0})\rangle\langle e(\mathbf{0})|\, \Gamma(L)^\dagger \tag{17}$$

with a different L in $Sp(2(n+k))$. Note that

$$|e(\mathbf{0})\rangle\langle e(\mathbf{0})| = \rho_g(\mathbf{0},\mathbf{0},\frac{1}{2}I_{2k}),$$
$$\rho_g(\ell,\mathbf{m},S)\otimes\rho_g(\mathbf{0},\mathbf{0},\frac{1}{2}I_{2k}) = \rho_g(\ell\oplus\mathbf{0},\mathbf{m}\oplus\mathbf{0},S\oplus\frac{1}{2}I_{2k}).$$

By the transformation property of Gaussian states we have from (7)

$$T(\rho_g(\ell,\mathbf{m},S)) = \rho_g(\ell'\oplus\mathbf{a},\mathbf{m}'\oplus\mathbf{b},S')$$

where

$$S' = (L^{-1})^T \begin{bmatrix} S & 0 \\ 0 & \frac{1}{2}I_{2k} \end{bmatrix} L^{-1}$$

and ℓ', $\mathbf{m}'$, $\mathbf{a}$, $\mathbf{b}$ are obtained as follows. Define μ,μ' by $\mu^T = (\ell_1,-m_1,\ldots,\ell_n,-m_n,0,0,\ldots,0)$, $(\mu')^T = (\ell'_1,-m'_1,\ldots,\ell'_n,-m'_n,a_1,-b_1,\ldots,a_k,-b_k)$. Then

$$\mu' = (L^{-1})^T\,\mu \quad \text{in} \quad \mathbb{R}^{2(n+k)}.$$

Writing

$$L^{-1} = M = \begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix}, \quad S' = \begin{bmatrix} S'_{11} & S'_{12} \\ S'_{21} & S'_{22} \end{bmatrix}$$

in block notation where 11 and 22 blocks are of order $2n\times 2n$ and $2k\times 2k$ respectively we see that, for T as in (17),

$$T(\rho_g(\ell,\mathbf{m},S)) = \rho_g((\ell',\mathbf{m}',S'_{11})$$

where

$$S'_{11} = M_{11}^T S M_{11} + \frac{1}{2}M_{21}^T M_{21},$$
$$\begin{bmatrix} \ell'_1 \\ -m'_1 \\ \vdots \\ \ell'_n \\ -m'_n \end{bmatrix} = M_{11}^T \begin{bmatrix} \ell_1 \\ -m_1 \\ \vdots \\ \ell_n \\ -m_n \end{bmatrix}.$$

We summarize our algebra in the form of a theorem.

Theorem 3. *The most general symplectic Gaussian channel T has the property that for all Gaussian states $\rho_g(\ell,\mathbf{m},S)$ in $L^2(\mathbb{R}^n)$,*

$$T(\rho_g(\ell,\mathbf{m},S)) = \rho_g((\ell',\mathbf{m}',S')$$

where

$$S' = M_{11}^T\, S\, M_{11} + \frac{1}{2}\, M_{21}^T\, M_{21} \tag{18}$$

for some $M \in Sp(2(n+k))$ for some k with

$$M = \begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix} \tag{19}$$

where the blocks with labels 11 *and* 22 *are matrices of order $2n \times 2n$ and $2k \times 2k$ respectively and the vectors μ, μ' defined by*

$$\mu^T = (\ell_1, -m_1, \ldots, \ell_n, -m_n), \tag{20}$$

$$\mu'^T = (\ell'_1, -m'_1, \ldots, \ell'_n, -m'_n), \tag{21}$$

where

$$\mu' = M_{11}^T\, \mu. \tag{22}$$

We shall denote by T_M any symplectic Gaussian channel in $L^2(\mathbb{R}^n)$ satisfying Theorem 3 for some k, some $M \in Sp(2(n+k))$ and equations (18)-(22) for all Gaussian states $\rho_g(\ell, \mathbf{m}, S)$.

Theorem 4. *Let T_L, T_M be symplectic Gaussian channels in $L^2(\mathbb{R}^n)$ where $L \in Sp(2(n+\ell))$, $M \in Sp(2(n+m))$. Then there exists a symplectic Gaussian channel T_N in $L^2(\mathbb{R}^n)$ for some $N \in Sp(2(n+\ell+m))$ such that for every Gaussian state ρ in $L^2(\mathbb{R}^n)$*

$$T_N(\rho) = T_L(T_M(\rho)).$$

Proof. Express the matrices L and M in block notation

$$L = \begin{bmatrix} L_{00} & L_{01} \\ L_{10} & L_{11} \end{bmatrix}, \quad M = \begin{bmatrix} M_{00} & M_{02} \\ M_{20} & M_{22} \end{bmatrix}$$

where L_{00} and M_{00} are of order $2n \times 2n$, L_{11} is of order $2\ell \times 2\ell$ and M_{22} is of order $2m \times 2m$. Define

$$\widetilde{L} = \begin{bmatrix} L_{00} & L_{01} & 0 \\ L_{10} & L_{11} & 0 \\ 0 & 0 & I_{2m} \end{bmatrix}, \quad \widetilde{M} = \begin{bmatrix} M_{00} & 0 & M_{02} \\ 0 & I_{2\ell} & 0 \\ M_{20} & 0 & M_{22} \end{bmatrix},$$

$$N = \widetilde{M}\widetilde{L} = \begin{bmatrix} M_{00}L_{00} & M_{00}L_{01} & M_{02} \\ L_{10} & L_{11} & 0 \\ M_{20}L_{00} & M_{20}L_{01} & M_{22} \end{bmatrix}.$$

Then $\widetilde{M}, \widetilde{L}$ and N are all elements of $Sp(2(n+\ell+m))$. Consider the symplectic Gaussian channel T_N as described in Theorem 3. Then

$$T_N(\rho_g(\ell, \mathbf{m}, S)) = \rho_g(\ell', \mathbf{m}', S') \tag{23}$$

where

$$\begin{aligned} S' &= (M_{00}L_{00})^T S\, M_{00}L_{00} + \frac{1}{2}(L_{10}^T L_{10} + (M_{20}L_{00})^T M_{20}L_{00}) \\ &= L_{00}^T \left\{ M_{00}^T S M_{00} + \frac{1}{2} M_{20}^T M_{20} \right\} L_{00} + \frac{1}{2} L_{10}^T L_{10} \end{aligned}$$

which is also the covariance matrix of the Gaussian state $T_L(T_M(\rho_g(\ell, \mathbf{m}, S)))$. Since N is a symplectic dilation of $M_{00}L_{00}$, equations (20)-(22) in Theorem 3 imply that the momentum and position means $\ell', \mathbf{m}'$ in (23) agree with the momentum and position means of $T_L(T_M(\rho_g(\ell, \mathbf{m}, S)))$. □

Corollary 1. *Let A, B be real $2n \times 2n$ matrices admitting symplectic dilations of order $2(n+\ell), 2(n+m)$ respectively. Then AB admits a symplectic dilation of order $2(n+\ell+m)$.*

Proof. This is seen immediately from the proof of Theorem 4 if we write $A = M_{00}$, $B = L_{00}$. □

Remark 3. From equation (17) we can easily write down a Kraus or operator sum representation of the symplectic Gaussian channel. Indeed, in (17) put $U = \Gamma(L)$ where $L \in Sp(2(n+k))$. Consider the particle number basis $\{|r_1, r_2, \ldots, r_k\rangle, r_j \in \{0, 1, 2, \ldots, \} \forall\, j\}$ in $L^2(\mathbb{R}^k)$ when identified with the boson Fock space over $\mathbb{C}^k$. Define the operators $U_{\mathbf{r},\mathbf{s}}$ in $L^2(\mathbb{R}^n)$ by the identity

$$\langle \psi \otimes \mathbf{r} | U | \psi' \otimes \mathbf{s} \rangle = \langle \psi | U_{\mathbf{r},\mathbf{s}} | \psi' \rangle \quad \forall\, \psi, \psi' \in L^2(\mathbb{R}^n).$$

Then

$$\begin{aligned} T(\rho) &= \mathrm{Tr}_2\, \Gamma(L)\ (\rho \otimes |\mathbf{0}\rangle\langle\mathbf{0}|)\Gamma(L)^\dagger \\ &= \mathrm{Tr}_2\, U(\rho \otimes |\mathbf{0}\rangle\langle\mathbf{0}|)U^\dagger) \\ &= \sum_r U_{\mathbf{r},\mathbf{0}}\, \rho\, U_{\mathbf{r},\mathbf{0}}^\dagger \end{aligned}$$

Example 4 (Quasifree channels[3], [8]). This example is from the construction given by Heinosaari, Holevo and Wolf [3]. To describe this we rewrite the Weyl operators $W(\mathbf{u})$ as $W(\xi)$ where $\xi^T = (\xi_1, \xi_2, \ldots, \xi_{2n}) = (\mathrm{Re}\, u_1, \mathrm{Im}\, u_1, \ldots, \mathrm{Re}\, u_n, \mathrm{Im}\, u_n)$ for $\mathbf{u} \in \mathbb{C}^n$. Then there exists a unital completely positive map T_0 on $\mathscr{B}(L^2(\mathbb{R}^n))$ satisfying

$$T_0(W(\xi)) = e^{-\frac{1}{2}\xi^T B \xi}\, W(A\xi), \quad \xi \in \mathbb{R}^{2n} \tag{24}$$

whenever A and B are $2n \times 2n$ real matrices, B is symmetric and the matrix inequality

$$B + i(A^T J_{2n} A - J_{2n}) \geq 0 \tag{25}$$

holds with J_{2n} given by (1). The left hand side of (25) is a complex hermitian matrix and (25) implies that $B \geq 0$.

Now choose and fix A, B as above and consider T_0 satisfying (24). For any state ρ in $L^2(\mathbb{R}^n)$ define the state $T(\rho)$ by

$$\begin{aligned}\mathrm{Tr}\, T(\rho)\, W(\xi) &= \mathrm{Tr}\, \rho\; T_0(W(\xi)) \\ &= \mathrm{Tr}\, \rho\; W(A\xi) e^{-\frac{1}{2}\xi^T B\xi} \quad \forall\, \xi. \end{aligned} \tag{26}$$

Then for any Gaussian state $\rho_g(\ell, \mathbf{m}, S)$ we have from (11)

$$\mathrm{Tr}\, T(\rho_g(\ell, \mathbf{m}, S)) = \rho_g(\ell', \mathbf{m}', S')$$

where

$$S' = A^T S A + \frac{1}{2} B$$

and $\ell', \mathbf{m}'$ are given by

$$A^T \begin{bmatrix} \ell_1 \\ -m_1 \\ \vdots \\ \ell_n \\ -m_n \end{bmatrix} = \begin{bmatrix} \ell'_1 \\ -m'_1 \\ \vdots \\ \ell'_n \\ -m'_n \end{bmatrix}$$

Thus T is a Gaussian channel which changes the means and the covariance matrix exactly in the same manner as for the symplectic Gaussian channel T_M of Theorem 3 by writing $M_{11} = A$ and $M_{21}^\dagger M_{21} = B$, associated with the symplectic matrix M. We call the channel defined through (24) and (25), a *quasifree Gaussian channel*.

The inequality (26) raises some questions concerning symplectic dilations. To any $2n \times 2n$ real matrix A, associate the convex sets

$$\begin{aligned} \mathscr{K}_n &= \{S | S \geq 0, \quad 2S - iJ_{2n} \geq 0\}, \\ \mathscr{F}_n(A) &= \left\{ B | B \geq 0, A^T S A + \frac{1}{2} B \geq 0 \quad \forall\, S \in \mathscr{K}_n \right\}, \\ \mathscr{F}_n^0(A) &= \left\{ B | B \geq 0, i(A^T J_{2n} A - J_{2n}) + B \geq 0 \right\}. \end{aligned}$$

By Theorem 2, $\mathscr{K}_n$ is the set of all $2n \times 2n$ covariance matrices of Gaussian states, $B \in \mathscr{F}_n(A)$ if and only if the affine tranformaton $S \to A^T S A + \frac{1}{2} B$ leaves $\mathscr{K}_n$ invariant and $\mathscr{F}_n^0(A)$ is the set of all $2n \times 2n$ positive definite matrices such that (A, B) defines a quasifree Gaussian channel. since

$$\begin{aligned} & 2\left(A^T\ S\ A + \frac{1}{2} B\right) - i\ J_{2n} \\ & = A^T\ (2S - i\ J_{2n})\ A + i\ \left(A^T\ J_{2n} A - J_{2n}\right) +\ B \end{aligned}$$

it follows that $\mathscr{F}_n^0(A) \subset \mathscr{F}_n(A)$. Is it true for every B in $\mathscr{F}_n(A)$ there is a Gaussian channel with the property that it transforms a Gaussian state $\rho_g(\ell, \mathbf{m}, S)$ to a Gaussian state with covariance matrix $A^T S A + \frac{1}{2} B$? To any $B \in \mathscr{F}_n^0(A)$ does there exist a symplectic dilation $\widetilde{A} = \begin{bmatrix} A & P \\ Q & R \end{bmatrix}$ such that $B = Q^T Q$? If this holds we can realize the quasifree channel associated with (A, B) by a symplectic channel associated with

$\widetilde{A}$. If $\begin{bmatrix} A & P \\ Q & R \end{bmatrix}$ is a symplectic matrix does $Q^T Q \in \mathscr{F}_n^0(A)$? Finally, are there Gaussian channels not belonging to the semigroup generated by all reversible, bosonic, symplectic and quasifree Gaussian channels? It would be interesting to find answers to all the questions raised above. One would also like to have a description of the extreme points of $\mathscr{F}_n(A)$ and $\mathscr{F}_n^0(A)$.

Acknowledgement

This paper is an expanded version of a lecture delivered in the Kerala School of Mathematics, Kozhikode at a workshop and conference held in honour of Professor Kalyan B. Sinha on his 70th birthday during 7-14 February 2014. I thank the faculty and staff of KSOM for their warm hospitality in a scenic campus surrounded by hills and native trees. Part of this work was done at the Institute of Mathematical Sciences, Chennai where I enjoyed their warm hospitality and benefitted from several conversations with M. Krishna and R. Simon. I am grateful to Ajit Iqbal Singh for a careful reading of the manuscript and suggesting many improvements. I thank my colleagues at the Delhi Centre of the Indian Statistical Institute for providing me a friendly research environment.

References

[1] Arvind, Dutta B, Mukunda N and Simon R, The real symplectic group in quantum mechanics and optics, *Pramana - J. Phys.* 45 (1995) 471-497.
[2] Caruso F, Eisert J. Giovannetti V and Holevo A S, Multimode bosonic Gaussian channels, *New J. Phys.*, 10:083030 (2008).
[3] Heinosaari T, Holevo A. S. and Wolf M M, The semigroup structure of Gaussian channels, *arXiv: 0909.0408v1 [quant-ph]* 2 Sep 2009, J. Quantum Inf. Comp. 10:0619-0635 (2010).
[4] Holevo A S, Probabilistic and Statistical Aspects of Quantum Theory (1982) (Amsterdam: North Holland).
[5] Holevo A. S. and Werner R. F., Evaluating capacities of bosonic Gaussian channels, Phys. Rev. A 63:032312 (2001).
[6] Parthasarathy K. R. What is a Gaussian state? *Commun. Stoch. Anal* 4 (2010) 143-160.
[7] Parthasarathy K. R The symmetry group of Gaussian states in $L^2(\mathbb{R}^n)$, in Prokhorov and Contemporary Probability 349-369 (2013) Eds: Shiryaev A. N., Varadhan S. R. S. and Presman E. L. (Berlin, Springer Proceedings in Mathematics and Statistics 33)
[8] Vanheuverzwijn P, Generators for completely positive semigroups, *Ann. Inst. H. Poincaré Sect. A (N.S.)* 29 (1978) 123-138.
[9] Williamson J, The exponential representation of canonical matrices, *Amer. J. Math* 61 (1939) 897-911.