# Chapter 1

# Gaussian States

## 1.1 Canonical commutation relations

The canonical commutation relations (CCR) are central to almost all standard approaches to the quantization of continuous systems, be they motional degrees of freedom of non-relativistic particles ("first" quantization) or bosonic quantum fields ("second" quantization). Given a finite set of degrees of freedom represented by pairs of self-adjoint canonical operators $\hat{x}_j$ and $\hat{p}_j$, for $j = 1, \ldots, n$, the CCR read

$$[\hat{x}_j, \hat{p}_k] = i\delta_{jk}\hbar \; . \tag{1.1}$$

where $\Omega$ is a real, canonical anti-symmetric form (also known as the 'symplectic form', for reasons that will become clear in the following), given by the direct sum of identical $2 \times 2$ blocks:

$$\Omega = \bigoplus_{j=1}^{n} \omega \; , \quad \text{with} \quad \omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \; . \tag{1.2}$$

Note that the identity operator should be understood on the RHS of Eq. (1.1): the commutators of pairs of canonical operators are proportional to $c$-numbers, and can hence be represented by a complex-valued, rather than operator valued, matrix $i\Omega$. Also, we shall set $\hbar = 1$ and only reinstate it in dealing with practical cases. By defining the vector of canonical operators $\hat{\mathbf{r}} = (\hat{x}_1, \hat{p}_1 \ldots \hat{x}_n, \hat{p}_n)^{\mathsf{T}}$, Eq. (1.1) can be expediently recast as the following geometric, label-free, expression

$$[\hat{\mathbf{r}}, \hat{\mathbf{r}}^{\mathsf{T}}] = i\Omega \; , \tag{1.3}$$

where the commutator of row and column vectors of operators should be taken as an outer product. Borrowing from the optical and field theoretical terminologies, canonical degrees of freedom are also referred to as 'modes'.

Note that $\Omega = -\Omega^{\mathsf{T}}$ and $\Omega^2 = -\mathbb{1}_{2n}$, where $\mathbb{1}_{2n}$ is the $2n \times 2n$ identity matrix. Also, $\Omega$ is a real orthogonal transformation: $\Omega^{\mathsf{T}}\Omega = -\Omega^2 = \mathbb{1}_{2n}$.

Re-ordering the canonical operators as $\hat{\mathbf{r}'} = (\hat{x}_1, \ldots \hat{x}_n, \hat{p}_1, \ldots, \hat{p}_n)^{\mathsf{T}}$ yields the following equivalent expression of the CCR:

$$[\hat{\mathbf{r}'}, \hat{\mathbf{r}'}^{\mathsf{T}}] = i\Omega' \, , \quad \text{with} \quad \Omega' = \left( \begin{array}{cc} 0_n & \mathbb{1}_n \\ -\mathbb{1}_n & 0_n \end{array} \right) \tag{1.4}$$

where $\mathbb{1}_n$ and $0_n$ are, respectively, the $n \times n$ identity and null matrices.

Another relevant, equivalent form to express the CCR is given by considering bosonic annihilation and creation operators $a_j$ and $a_j^\dagger$, defined as

$$a_j = \frac{\hat{x}_j + i\hat{p}_j}{\sqrt{2}} \, . \tag{1.5}$$

It is easy to see that the vector of annihilation and creation operators $\boldsymbol{\alpha} = (a_1, a_1^\dagger, \ldots, a_n, a_n^\dagger)^{\mathsf{T}}$ is related to $\hat{\mathbf{r}}$ by the unitary transformation $\bar{U}_n$, given by

$$\bar{U} = \bigoplus_{j=1}^{n} \bar{u} \, , \quad \text{with} \quad \bar{u} = \frac{1}{\sqrt{2}} \left( \begin{array}{cc} 1 & i \\ 1 & -i \end{array} \right) \, , \tag{1.6}$$

so that the CCR may be equivalently recast as

$$[\boldsymbol{a}, \boldsymbol{a}^\dagger] = [\bar{U}\hat{\mathbf{r}}, \hat{\mathbf{r}}^\dagger \bar{U}^\dagger] = \bar{U}[\hat{\mathbf{r}}, \hat{\mathbf{r}}^\dagger]\bar{U}^\dagger = i\bar{U}\Omega\bar{U}^\dagger = \Sigma = \bigoplus_{j=1}^{n} \sigma_z \, , \tag{1.7}$$

where $\sigma_z$ is defined as the standard $z$ Pauli matrix:

$$\sigma_z = \left( \begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right) \tag{1.8}$$

Note that the adjoint of a vector of operators has been implicitly defined as the vector obtained by transposing the original one and conjugating each of its operator entries, e.g. $\boldsymbol{a}^\dagger = (a_1^\dagger, a_1, \ldots, a_n^\dagger, a_n)$. Also, $\hat{\mathbf{r}}^{\mathsf{T}} = \hat{\mathbf{r}}^\dagger$, since all of its entries are hermitian operators.

Often, and especially in the mathematical physics literature, the CCR are expressed by exponentiating the canonical operators, which has the advantage of making the operators involved bounded:[1]

$$\mathrm{e}^{i(\hat{x}_j - \hat{p}_k)} = \mathrm{e}^{i\hat{x}_j}\mathrm{e}^{-i\hat{p}_k}\mathrm{e}^{-\frac{i}{2}\delta_{jk}} = \mathrm{e}^{-i\hat{p}_k}\mathrm{e}^{i\hat{x}_j}\mathrm{e}^{\frac{i}{2}\delta_{jk}} \, . \tag{1.9}$$

The final phase factors in the previous equation imply the non-commutativity of position and momentum shifts, and are a typical signature of quantum mechanics. Eq. (1.9) may be generalised to consider arbitrary shift operators, also

[1] The equivalence between this expression and Eq. (1.1) is a straightforward consequence of the following well known corollary of the Baker-Campbell-Hausdorff formula:

$$\mathrm{e}^{A+B} = \mathrm{e}^{A}\mathrm{e}^{B}\mathrm{e}^{-[A,B]/2} \, ,$$

which holds whenever $[A, B]$ is *central*, that is commutes with both $A$ and $B$. In this case, which is clearly the CCR one, $A$, $B$ and their commutator form a closed algebra.

known as Weyl operators in the case of the CCR algebra:

$$
\begin{aligned}
\mathrm{e}^{i(\mathbf{r}_1+\mathbf{r}_2)^{\mathsf{T}}\Omega\hat{\mathbf{r}}} &= \mathrm{e}^{i\mathbf{r}_1^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\mathrm{e}^{i\mathbf{r}_2^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\mathrm{e}^{[\mathbf{r}_1^{\mathsf{T}}\Omega\hat{\mathbf{r}},\mathbf{r}_2^{\mathsf{T}}\Omega\hat{\mathbf{r}}]/2} = \mathrm{e}^{i\mathbf{r}_1^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\mathrm{e}^{i\mathbf{r}_2^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\mathrm{e}^{-[\mathbf{r}_1^{\mathsf{T}}\Omega\hat{\mathbf{r}},\hat{\mathbf{r}}^{\mathsf{T}}\Omega\mathbf{r}_2]/2} \\
&= \mathrm{e}^{i\mathbf{r}_1^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\mathrm{e}^{i\mathbf{r}_2^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\mathrm{e}^{-\mathbf{r}_1^{\mathsf{T}}\Omega[\hat{\mathbf{r}},\hat{\mathbf{r}}^{\mathsf{T}}]\Omega\mathbf{r}_2/2} = \mathrm{e}^{i\mathbf{r}_1^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\mathrm{e}^{i\mathbf{r}_2^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\mathrm{e}^{-i\mathbf{r}_1^{\mathsf{T}}\Omega^3\mathbf{r}_2/2} \qquad (1.10) \\
&= \mathrm{e}^{i\mathbf{r}_1^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\mathrm{e}^{i\mathbf{r}_2^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\mathrm{e}^{i\mathbf{r}_1^{\mathsf{T}}\Omega\mathbf{r}_2/2} = \mathrm{e}^{i\mathbf{r}_2^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\mathrm{e}^{i\mathbf{r}_1^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\mathrm{e}^{-i\mathbf{r}_1^{\mathsf{T}}\Omega\mathbf{r}_2/2}\,, \ \forall\, \mathbf{r}_1,\mathbf{r}_2\in\mathbb{R}^{2n}\,.
\end{aligned}
$$

So that, in terms of the Weyl operators $\hat{D}_{\mathbf{r}} = \mathrm{e}^{i\mathbf{r}^{\mathsf{T}}\Omega\hat{\mathbf{r}}}$, one has

$$\hat{D}_{\mathbf{r}_1+\mathbf{r}_2} = \hat{D}_{\mathbf{r}_1}\hat{D}_{\mathbf{r}_2}\mathrm{e}^{i\mathbf{r}_1^{\mathsf{T}}\Omega\mathbf{r}_2/2}\,. \qquad (1.11)$$

Inspection reveals that the CCR algebra does not allow for a representation through finite dimensional matrices. For instance, by taking the trace of the left and right hand side of equation $[\hat{x}_1,\hat{p}_1] = i\mathbb{1}$ and assuming that the trace of a commutator vanishes, as is always the case in finite dimension, one would get $\mathrm{tr}\,\mathbb{1} = 0$, which is clearly impossible to satisfy. However, infinite dimensional representations of the CCR algebra do exist. As well known from basic quantum mechanics, one can consider the space of square-integrable functions on the real line $L^2(\mathbb{R}^n)$, and define:

$$
\begin{aligned}
\hat{x}_j|f\rangle &= x_j f(\mathbf{x})\,, && (1.12) \\
\hat{p}_j|f\rangle &= -i\frac{\mathrm{d}}{\mathrm{d}x_j}f(\mathbf{x})\,, \quad \forall\,|f\rangle \equiv f(\mathbf{x}) \in L^2(\mathbb{R}^n)\,, && (1.13)
\end{aligned}
$$

with $\mathbf{x} = (x_1,\ldots,x_n)$. By virtue of the Stone-von Neumann theorem, all representations of the CCR algebra on a finite set of degrees of freedom are unitarily equivalent to the representation given by Eqs. (1.12) and (1.13). In this book, we shall not venture to consider continua of degrees of freedom, as typically necessary in quantum field theory, and will thus be content with this representation of the CCR algebra.

The eigenstates of $\hat{x}_j$ (and $\hat{p}_j$) are not part of $L^2(\mathbb{R}^n)$, although we shall still indicate them in the Dirac notation as $|x_j\rangle$ and $|p_j\rangle$, by which we shall denote linear forms on $L^2(\mathbb{R}^n)$ such that

$$\langle x_j'|f\rangle = \langle f|x_j'\rangle^* = f(x_1\ldots,x_{j-1},x_j',x_{j+1},\ldots,x_n) \in L^2(\mathbb{R}^{n-1})\,, \qquad (1.14)$$

$\forall\,|f\rangle \equiv f(\mathbf{x}) \in L^2(\mathbb{R}^n)$. For a trace-class operator $\hat{O}$, one can then write

$$\mathrm{Tr}\left[\hat{O}\right] = \int_{-\infty}^{+\infty}\langle x|\hat{O}|x\rangle\,\mathrm{d}x\,. \qquad (1.15)$$

## 1.2 Quadratic Hamiltonians and Gaussian states

Throughout this book we will refer, somewhat loosely, to a quadratic Hamiltonian as a Hamiltonian which can be expressed as a polynomial of order two in the canonical operators. In terms of the vector of operators $\hat{\mathbf{r}}$ defined above, the most general quadratic Hamiltonian operator $\hat{H}$ reads, up to an irrelevant additive constant:

$$\hat{H} = \frac{1}{2}\hat{\mathbf{r}}^{\mathsf{T}} H \hat{\mathbf{r}} + \hat{\mathbf{r}}^{\mathsf{T}} \mathbf{r} \, , \tag{1.16}$$

where $\mathbf{r}$ is a $2n$-dimensional real vector and $H$ a symmetric matrix, known as the Hamiltonian matrix and not to be confused with the Hamiltonian operator $\hat{H}$. The matrix $H$ can be assumed to be symmetric because any anti-symmetric component in it would just add a term proportional to the identity operator, because of the CCR, and would thus amount to adding a constant to the Hamiltonian.

The modelling of quantum dynamics through quadratic Hamiltonians is very common when higher order terms are inconspicuous and negligible, as is often the case for quantum light fields. Besides, quadratic Hamiltonians represent a consistent approximation in other situations of great interest for experiments, such as ion traps, opto-mechanical systems, nano-mechanical oscillators, and several other systems which will be reviewed in chapter **??**. Up to interactions, the 'free', local Hamiltonian of a quantum oscillator, $\hat{x}^2 + \hat{p}^2$ in rescaled units, is obviously quadratic.

The diagonalisation of any quadratic Hamiltonian is a rather straightforward mathematical routine. Because, as we shall see, such a diagonalisation rests on identifying degrees of freedom that are decoupled from each other, systems governed by quadratic Hamiltonians are referred to as "quasi-free" in the quantum field theory literature. Notwithstanding the ease with which their dynamics is solved, such systems still offer a very rich scenario for quantum information theory, where the standard methods used for the analysis of quadratic Hamiltonians become powerful allies.

### 1.2.1 Gaussian states

Let us define the set of Gaussian states as *all the the ground and thermal states of quadratic Hamiltonians with positive definite Hamiltonian matrix* $H > 0$. The restriction to positive definite Hamiltonian matrices corresponds to considering 'stable' systems – i.e., Hamiltonian operators bounded from below – and make the definition above consistent.

Any Gaussian state $\varrho_G$ may hence be written as

$$\varrho_G = \frac{\mathrm{e}^{-\beta\hat{H}}}{\mathrm{Tr}\left[\mathrm{e}^{-\beta\hat{H}}\right]} \, , \tag{1.17}$$

with $\beta \in \mathbb{R}^+$ and $\hat{H}$ defined by $\mathbf{r}$ and $H$ as in Eq. (1.16), including the limiting instance

$$\varrho_G = \lim_{\beta\to\infty} \frac{\mathrm{e}^{-\beta\hat{H}}}{\mathrm{Tr}\left[\mathrm{e}^{-\beta\hat{H}}\right]} \, . \tag{1.18}$$

Clearly, all states of the form (1.17) for finite $\beta$ are by construction mixed states, while all pure Gaussian states are described by Eq. (1.18).

By the definition above, Gaussian states have been parametrized through the Hamiltonian matrix $H$, the vector $\mathbf{R}$, whose meaning will become clear shortly, and the parameter $\beta$, which is intended to mimic a notation well established in thermodynamics where it would indicate the inverse temperature (up to the Boltzmann constant).

Let us now obtain the diagonal form of states (1.17) and (1.18). First off, notice that, upon redefining $\mathbf{r}' = -H^{-1}\mathbf{r}$ (always possible, as any positive definite $H$ is invertible), and up to an irrelevant constant, the Hamiltonian $\hat{H}$ is equivalent to

$$\hat{H}' = \frac{1}{2}(\hat{\mathbf{r}} - \mathbf{r}')^{\mathsf{T}} H (\hat{\mathbf{r}} - \mathbf{r}') , \tag{1.19}$$

which is an alternative form of the most general quadratic Hamiltonian with positive definite $H$, where the real vector $\mathbf{r}'$ merely shifts the vector of operators $\hat{\mathbf{r}}$. We can prove that this shift is equivalent to the action of a unitary operator by considering the action of a Weyl operator, introduced in Eq. (1.11), on the vector of operators $\hat{\mathbf{r}}$. We intend to prove that

$$\mathrm{e}^{-i\mathbf{r}'^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\hat{\mathbf{r}}\mathrm{e}^{i\mathbf{r}'^{\mathsf{T}}\Omega\hat{\mathbf{r}}} = \hat{\mathbf{r}} - \mathbf{r}' , \tag{1.20}$$

where it is understood that the same Weyl operator acts on all entries of the vector $\hat{\mathbf{r}}$. To this aim, let us define the vector of operators $\hat{\mathbf{f}}(\mathbf{r}') = \mathrm{e}^{-i\mathbf{r}'^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\hat{\mathbf{r}}\mathrm{e}^{i\mathbf{r}'^{\mathsf{T}}\Omega\hat{\mathbf{r}}}$, for which one has $\hat{\mathbf{f}}(0) = \hat{\mathbf{r}}$, as well as

$$\begin{aligned}\partial_{r'_j}\hat{f}_k\Big|_{\mathbf{r}'=0} &= \left(\partial_{r'_j}\mathrm{e}^{-i\sum_{lm} r'_l\Omega_{lm}\hat{r}_m}\hat{r}_j\mathrm{e}^{i\sum_{st} r'_s\Omega_{st}\hat{r}_t}\right)\Big|_{\mathbf{r}'=0} \\ &= -i\sum_m \Omega_{jm}[\hat{r}_m, \hat{r}_k] = \sum_m \Omega_{jm}\Omega_{mk} = -\delta_{jk} ,\end{aligned}$$

while all the higher order derivatives of $\hat{f}_j$ are obviously zero. Hence, all the derivatives in zero of the smooth operator valued function $\hat{\mathbf{f}}(\mathbf{r}')$ coincide with the derivatives of the function $\hat{\mathbf{r}} - \mathbf{r}'$, which proves Eq. (1.20).[2] Because of Eq. (1.20), the Weyl operators are also known as shift or displacement operators, typically in the quantum optics literature.

Inserting Eq. (1.20) into (1.19) yields

$$\hat{H}' = \frac{1}{2}(\hat{\mathbf{r}} - \mathbf{r}')^{\mathsf{T}} H (\hat{\mathbf{r}} - \mathbf{r}') = \frac{1}{2}\mathrm{e}^{-i\mathbf{r}'^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\hat{\mathbf{r}}^{\mathsf{T}} H\hat{\mathbf{r}}\mathrm{e}^{i\mathbf{r}'^{\mathsf{T}}\Omega\hat{\mathbf{r}}} . \tag{1.21}$$

Up to first order displacement operators, one can hence set the vector $\mathbf{r}'$ in the quadratic Hamiltonian $\hat{H}'$ to zero. The effect of the purely quadratic part $\frac{1}{2}\hat{\mathbf{r}}^{\mathsf{T}}H\hat{\mathbf{r}}$ can be understood by considering the transformations it induces on the vector of operators $\hat{\mathbf{r}}$ in the Heisenberg picture, which will be the focus of the next section.

[2] The same conclusion could have been reached by applying the well known Baker-Campbell-Hausdorff relationship

$$\mathrm{e}^{\hat{X}}\hat{Y}\mathrm{e}^{-\hat{X}} = \hat{Y} + [\hat{X}, \hat{Y}] + \frac{1}{2!}[\hat{X}, [\hat{X}, \hat{Y}]] + \frac{1}{3!}[\hat{X}, [\hat{X}, [\hat{X}, \hat{Y}]]] + \dots .$$

### 1.2.2 The symplectic group of linear canonical transformations

Let us now consider the Heisenberg evolution of the vector of operators $\hat{\mathbf{r}}$ under the dynamics governed by the Hamiltonian $\hat{H} = \frac{1}{2}\hat{\mathbf{r}}^{\mathsf{T}} H \hat{\mathbf{r}}$. One has

$$\begin{aligned} \dot{\hat{r}}_j &= \frac{i}{2}[\hat{H}, \hat{r}_j] = \frac{i}{2}\sum_{kl}[\hat{r}_k H_{kl} \hat{r}_l, \hat{r}_j] \\ &= \frac{i}{2}\sum_{kl} H_{kl}\left(\hat{r}_k[\hat{r}_l, \hat{r}_j] + [\hat{r}_k, \hat{r}_j]\hat{r}_l\right) = \sum_{kl}\Omega_{jk} H_{kl} \hat{r}_l \ , \end{aligned} \tag{1.22}$$

which can be recast in vector form as

$$\dot{\hat{\mathbf{r}}} = \Omega H \hat{\mathbf{r}} \ . \tag{1.23}$$

The solution to the differential equation (1.23) is straightforward and given by $\hat{\mathbf{r}}(t) = \mathrm{e}^{\Omega H t}\hat{\mathbf{r}}(0)$. Since it represents the action of a unitary operation, the transformation $\mathrm{e}^{\Omega H t}$ must preserve the CCR when applied to the vector $\hat{\mathbf{r}}$, that is

$$i\Omega = [\hat{\mathbf{r}}, \hat{\mathbf{r}}^{\mathsf{T}}] = [\mathrm{e}^{\Omega H t}\hat{\mathbf{r}}, \hat{\mathbf{r}}^{\mathsf{T}}(\mathrm{e}^{\Omega H t})^{\mathsf{T}}] = \mathrm{e}^{\Omega H t}[\hat{\mathbf{r}}, \hat{\mathbf{r}}^{\mathsf{T}}](\mathrm{e}^{\Omega H t})^{\mathsf{T}} = i\mathrm{e}^{\Omega H t}\Omega(\mathrm{e}^{\Omega H t})^{\mathsf{T}} \ . \tag{1.24}$$

The transformation $\mathrm{e}^{\Omega H t}$ must preserve the canonical anti-symmetric form $\Omega$ when acting by congruence.[3] This can be restated by claiming that $\mathrm{e}^{\Omega H t}$ belongs to the group of linear canonical transformations, well known from classical Hamiltonian mechanics. This group is also known as the real symplectic group in dimension $2n$, denoted by $Sp_{2n,\mathbb{R}}$ (let us remind the reader that H and $\Omega$ are $2n \times 2n$ matrices). The quadratic form $\Omega$, which encodes the commutation relations in our formalism, is also known as the symplectic form, and the symplectic group is defined as the set of transformations that preserve $\Omega$ under congruence:

$$S \in Sp_{2n,\mathbb{R}} \quad \Leftrightarrow \quad S\Omega S^{\mathsf{T}} = \Omega \ . \tag{1.25}$$

the group character of such a set is ascertained by noting that its elements must be invertible because their determinant cannot be zero by Binet's theorem, and that $S^{-1}\Omega S^{-1\mathsf{T}} = \Omega$ (the inclusion of the identity matrix and of any product of two elements are obvious).

In point of fact, the set $\mathrm{e}^{\Omega H t}$ for all $t \in \mathbb{R}$ and symmetric $H$ form the whole symplectic group. This can be seen by setting $S = \mathrm{e}^{\Omega J t}$ and taking the first derivative with respect to $t$ of $S\Omega S^{\mathsf{T}} = \Omega$, which defines the group. Thus, one obtains

$$\frac{\mathrm{d}}{\mathrm{d}t}\left(\mathrm{e}^{\Omega J t}\Omega \mathrm{e}^{-J^{\mathsf{T}}\Omega t}\right)\Big|_{t=0} = \Omega J \Omega - \Omega J^{\mathsf{T}}\Omega = 0 \quad \Rightarrow \quad J = J^{\mathsf{T}} \ , \tag{1.26}$$

[3] We will refer to the matrix $A$ acting "by congruence" on the quadratic form $B$ to indicate the transformation $B \mapsto ABA^{\mathsf{T}}$. The invertible matrix $A$ will instead be said to act "by similarity" on $B$ when it transforms it according to $B \mapsto ABA^{-1}$.

which shows that all generators of the symplectic group must be of the form $\Omega H$, with symmetric $H$. Notice that, to obtain the whole symplectic group, one cannot restrict to definite positive hamiltonian matrices. Such a restriction was only imposed in defining Gaussian states.

Our approach implicitly shows that the transformations $\mathrm{e}^{i\hat{\mathbf{r}}^{\mathsf{T}}H\hat{\mathbf{r}}}$ form a representation of the symplectic group $Sp_{2n,\mathbb{R}}$ when acting by similarity on the linear space of operators on $L^2(\mathbb{R}^{2n})$.

It is expedient to introduce the shorthand notation $\hat{S}_H$ for operators with purely quadratic generators:

$$\hat{S}_H = \mathrm{e}^{i\hat{\mathbf{r}}^{\mathsf{T}}H\hat{\mathbf{r}}} \, , \tag{1.27}$$

such that our argument above allows one to write

$$\hat{S}_H \hat{\mathbf{r}} \hat{S}_H^{\dagger} = S_H \hat{\mathbf{r}} \, , \tag{1.28}$$

where $S_H = \mathrm{e}^{\Omega H} \in Sp_{2n,\mathbb{R}}$.[4] Notice that, with respect to the treatment above, the time variable $t$ has been absorbed in the symmetric matrix $H$. The relationship (1.28) will be used extensively throughout the book.

### 1.2.3 Some facts about the symplectic group

In this appendix, we shall prove useful notions concerning the real symplectic group $\{S \in \mathcal{M}(2n,\mathbb{R}) \,|\, S\Omega' S^{\mathsf{T}} = \Omega'\}$, with

$$\Omega' = \begin{pmatrix} 0_n & \mathbb{1}_n \\ -\mathbb{1}_n & 0_n \end{pmatrix} \tag{1.29}$$

[throughout this appendix, it will be convenient to adopt the convention introduced in (1.4) by rearranging the vector of operators as an array of $\hat{x}$'s followed by an array of $\hat{p}$'s].

First off, let us list a few basic statements about the group:

$$\Omega' = \in Sp_{2n,\mathbb{R}} \, , \tag{1.30}$$

$$\Omega'^{\mathsf{T}} = -\Omega' \in Sp_{2n,\mathbb{R}} \, , \tag{1.31}$$

$$S^T = \Omega'^{\mathsf{T}} S^{-1} \Omega' \in Sp_{2n,\mathbb{R}} \, . \tag{1.32}$$

Next, let us consider the intersection $K(n)$ between the real symplectic group and the orthogonal group: $K(n) = Sp_{2n,\mathbb{R}} \cap O(2n)$. As we shall see, the subgroup $K(n)$ constitutes the maximal compact subgroup of $Sp_{2n,\mathbb{R}}$. We will

[4]This equation may be seen as a consequence of the fact that the correspondence between symplectic transformations and unitary operators generated by purely quadratic Hamiltonians constitutes a projective representation of $Sp_{2n,\mathbb{R}}$, that is a representation up to transformations-dependent phase factors. It turns out that a mapping can be defined where such phase factors are always either $-1$ or $+1$: Technically, one thus achieves a faithful representation of the *metaplectic* group, a double cover of the symplectic group whose exact definition would go beyond the scope of this book. It may however be useful to add that this construction is, somewhat loosely, also referred to as the “metaplectic” representation in the literature.

prove now that $K(n)$ is isomorphic to $U(n)$, and derive a particularly simple form for any element of $K(n)$ in the process.

Write a generic $2n \times 2n$ real matrix $S$ in terms of $n \times n$ blocks:

$$S = \begin{pmatrix} X & Y \\ W & Z \end{pmatrix} . \tag{1.33}$$

The equivalent conditions $S\Omega' S^{\mathsf{T}} = \Omega'$ and $S^{\mathsf{T}}\Omega' S = \Omega'$ read

$$XY^{\mathsf{T}} - YX^{\mathsf{T}} = WZ^{\mathsf{T}} - ZW^{\mathsf{T}} = 0_n \, , \tag{1.34}$$
$$XZ^{\mathsf{T}} - YW^{\mathsf{T}} = \mathbb{1}_n \, , \tag{1.35}$$
$$X^{\mathsf{T}}W - W^{\mathsf{T}}X = Y^{\mathsf{T}}Z - Z^{\mathsf{T}}Y = 0_n \, , \tag{1.36}$$
$$X^{\mathsf{T}}Z - W^{\mathsf{T}}Y = \mathbb{1}_n \, , \tag{1.37}$$

while orthogonality ($S^{\mathsf{T}}S = S^{\mathsf{T}}S = \mathbb{1}_{2n}$) implies

$$XX^{\mathsf{T}} + YY^{\mathsf{T}} = WW^{\mathsf{T}} + ZZ^{\mathsf{T}} = \mathbb{1}_n \, , \tag{1.38}$$
$$XW^{\mathsf{T}} + YZ^{\mathsf{T}} = 0_n \, , \tag{1.39}$$
$$X^{\mathsf{T}}X + W^{\mathsf{T}}W = Y^{\mathsf{T}}Y + Z^{\mathsf{T}}Z = \mathbb{1}_n \, , \tag{1.40}$$
$$X^{\mathsf{T}}Y + W^{\mathsf{T}}Z = 0_n \, . \tag{1.41}$$

Multiplying Eq. (1.37) by $X$ on the left, and then inserting, in order, Eqs. (1.39), (1.38) and (1.36), one obtains

$$\begin{aligned} &XX^{\mathsf{T}}Z - XW^{\mathsf{T}}Y = X \quad \Rightarrow \quad XX^{\mathsf{T}}Z + YZ^{\mathsf{T}}Y = X \\ &\Rightarrow \quad Z - YY^{\mathsf{T}}Z + YZ^{\mathsf{T}}Y = X \quad \Rightarrow \quad Z = X \, , \end{aligned} \tag{1.42}$$

Inserting $X = Z$ and Eq. (1.40) into Eq. (1.37) yields $W^{\mathsf{T}}Y + W^{\mathsf{T}}W = 0$, which can be multiplied by $W$ on the left and then simplified by using Eqs. (1.38), (1.41) and (1.36) to obtain

$$\begin{aligned} 0 &= WW^{\mathsf{T}}(Y+W) = (Y+W) - (XX^{\mathsf{T}}Y + XX^{\mathsf{T}}W) \\ &= (Y+W) - (-XW^{\mathsf{T}}X + XX^{\mathsf{T}}W) \\ &= (Y+W) - (-XW^{\mathsf{T}}X + XW^{\mathsf{T}}X) = Y + W \, . \end{aligned} \tag{1.43}$$

Hence the most general $2n \times 2n$ orthogonal symplectic matrix can be written as

$$S = \begin{pmatrix} X & Y \\ -Y & X \end{pmatrix} \quad \text{with} \quad \begin{aligned} XY^{\mathsf{T}} - YX^{\mathsf{T}} &= 0_n \, , \\ XX^{\mathsf{T}} + YY^{\mathsf{T}} &= \mathbb{1}_n \, . \end{aligned} \tag{1.44}$$

Note that the condition for simplecticity and orthogonality coincide for block matrices in this form.

On the other hand, splitting an $n \times n$ unitary $U$ in real and imaginary parts as per $U = X + iY$, with $X$ and $Y$ real, implies the following conditions on $X$ and $Y$:

$$UU^{\dagger} = XX^{\mathsf{T}} + YY^{\mathsf{T}} + i(YX^{\mathsf{T}} - XY^{\mathsf{T}}) = \mathbb{1}_n \, , \tag{1.45}$$

which are identical to the conditions of Eq. (1.44), thus proving the isomorphism relating $K(n)$ to $U(n)$.

Furthermore, notice that any $S \in K(n)$ can be block-diagonalised by applying the unitary $\bar{U}'$ that describes the passage from canonical to annihilation and creation operators:

$$\bar{U}' \begin{pmatrix} X & Y \\ -Y & X \end{pmatrix} \bar{U}'^{\dagger} = \begin{pmatrix} X - iY & 0_n \\ 0_n & X + iY \end{pmatrix} = \begin{pmatrix} U^* & 0_n \\ 0_n & U \end{pmatrix} , \qquad (1.46)$$

for

$$\bar{U}' = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbb{1}_n & i\mathbb{1}_n \\ \mathbb{1}_n & -i\mathbb{1}_n \end{pmatrix} . \qquad (1.47)$$

Besides providing a very compact way of expressing an orthogonal symplectic matrix, Eq. (1.46) also shows that the determinant of any $S \in K(n)$ is equal to $+1$.

We are now in a position to introduce and prove a useful decomposition of a symplectic operation, which goes under the name of Euler decomposition in analogy with the Euler decomposition of orthogonal operations:
Any symplectic matrix $S \in Sp_{2n,\mathbb{R}}$ can be decomposed as

$$S = O_1 Z O_2 \, , \qquad (1.48)$$

with $O_1$, $O_2 \in K(n)$ and

$$Z = \bigoplus_{j=1}^{n} \begin{pmatrix} z_j & 0 \\ 0 & z_j^{-1} \end{pmatrix} . \qquad (1.49)$$

Let us notice that any matrix $S$ allows for a singular value decomposition where $S = O_1 Z O_2$ for some $O_1, O_2 \in K(n)$ and $Z$ diagonal and positive semidefinite. We just need to prove that the singular value decomposition of a symplectic operation may always be given in terms of *symplectic* orthogonal $O_1$ and $O_2$ and of $Z$ of the form above.

As for $Z$ note that, by Eq. (1.32), the inverse of any symplectic $S^{-1}$ is orthogonally equivalent to its transpose $S^{\mathsf{T}}$. Since the set of singular values is preserved by orthogonal transformations and transposition, there follows that the set of singular values of $S$ must be the same as the set of singular values of $S^{-1}$, which are obviously just the inverse of the singular values of $S$. Hence, the set of $2n$ singular values of $S$ must be invariant under element-wise inversion, i.e. it must be made up of pairs $z_j$ and $z_j^{-1}$. This is consistent with the statement (1.48). Also note that the singular value decomposition is determined up to the ordering of the singular values, which may be varied by redefining $O_1$ and $O_2$ and inserting (orthogonal) permutations acting on the central diagonal matrix. For ease of notation, we will adopt here the ordering with singular value matrix $Z'$ written as

$$Z' = \begin{pmatrix} D & 0 \\ 0 & D^{-1} \end{pmatrix} , \qquad (1.50)$$

with $D = \mathrm{diag}(z_1, \dots, z_n)$ and $z_j \geq 0 \ \forall \ j$. This is equivalent to the statement given above under the choice $\Omega'$ for the symplectic form. This choice ensures that the matrix $Z'$ is symplectic, as can be straightforwardly verified. Note that the singular value decomposition of $S$ is determined up to an orthogonal transformation $R \in O(2n)$:

$$S = O_1 R Z' R^{\mathsf{T}} O_2 \ , \tag{1.51}$$

, where

$$R = \begin{pmatrix} R_1 & 0_n \\ 0_n & R_2 \end{pmatrix} \tag{1.52}$$

and $R_1$ and $R_2$ are any two $n \times n$ orthogonal transformation that act on the subspaces pertaining to degenerate singular values of $S$ (that is, $R_1$ and $R_2$ act as the identity on basis vectors corresponding to non-degenerate singular value and are block diagonal orthogonal on any degenerate subspace). Also note that $R_1$ may be picked different from $R_2$. No further ambiguity is allowed by the singular value decomposition, other than the trivial ordering of the $z_j$, which we shall disregard.

Now, we set to prove that a choice of $R_1$ and $R_2$ exist such that $O_1 R$ and $RO_2$ are symplectic. Notice that

$$SS^{\mathsf{T}} \in Sp_{2n,\mathbb{R}} \quad \Rightarrow \quad O_1 R Z'^2 R^{\mathsf{T}} O_1^{\mathsf{T}} \Omega' O_1 R Z'^2 R^{\mathsf{T}} O_1^{\mathsf{T}} = \Omega' \ , \tag{1.53}$$

which implies

$$Z'^2 \Omega'' Z'^2 = \Omega'' \tag{1.54}$$

for the anti-symmetric form

$$\Omega'' = R^{\mathsf{T}} O_1^{\mathsf{T}} \Omega' O_1 R = \begin{pmatrix} A & B \\ -B^{\mathsf{T}} & C \end{pmatrix} \ , \tag{1.55}$$

where the $n \times n$ blocks $A$, $B$ and $C$ are implicitly defined, with $A = -A^{\mathsf{T}}$, $C = -C^{\mathsf{T}}$ and $B$ arbitrary. We will now show that Eq. (1.54) allows one to choose $R$ such that $\Omega'' = \Omega'$. Then, Eq. (1.55) is equivalent to stating that $RO_1$ is symplectic. In components, Eq. (1.54) reads

$$A_{jk} z_j z_k = A_{jk} \quad \forall \quad j,k \in [1, \dots, n] \ , \tag{1.56}$$

$$C_{jk} z_j^{-1} z_k^{-1} = C_{jk} \quad \forall \quad j,k \in [1, \dots, n] \ , \tag{1.57}$$

$$B_{jk} z_j z_k^{-1} = B_{jk} \quad \forall \quad j,k \in [1, \dots, n] \ . \tag{1.58}$$

Since $A$ and $C$ are anti-symmetric and $z_j \geq 1 \ \forall \ j$, the first two equations above show that, unless $z_j = z_k = 1$ for $j \neq k$, then $A_{jk} = C_{jk} = 0$. Moreover, $B_{jk} = 0$ for $j \neq k$, unless $z_j = z_k$. Now, the subspace described by the vectors corresponding to $z_j = 1$, can be handled by choosing the arbitrary $R$ to put the antisymmetric form defined on it in canonical form, as detailed in footnote 5. This will render $A_{jk} = C_{jk} = 0$, and $B_{jk} = 0$ for $j \neq k$. Finally, the matrix $B_{jk}$ may be diagonalised on the subspaces with degenerate $z_j \neq 1$ too, by choosing

$R_1$ and $R_2$ that enact the singular value decomposition of the restriction of $B$ on such subspaces. Note in fact that

$$R\Omega'' R^{\mathsf{T}} = \begin{pmatrix} R_1 A R_1^{\mathsf{T}} & R_1 B R_2^{\mathsf{T}} \\ -R_2 B R_1^{\mathsf{T}} & R_2 C R_2^{\mathsf{T}} \end{pmatrix} , \tag{1.59}$$

so that the freedom of $R_1$ and $R_2$ is enough to singular value decompose on the degenerate subspaces. We have hence shown that a choice of $R$ exists that puts the anti-symmetric form of Eq. (1.55) in canonical form, with $A = B = 0$ and $B$ diagonal and and positive semi-definite. Inspection of the reduction to canonical form (see footnote 5), reveals that the diagonal entries of $B$ are determined as the square root of the eigenvalues of $-\Omega''^2$ and therefore do not depend on the orthogonal transformation acting on the anti-symmetric form. But, by its definition given in Eq. (1.55), $\Omega''^2 = \mathbb{1}_{2n}$, so that the diagonal entries of $B$ in canonical form must be all equal to 1. This shows that $R$ may always be chosen such that $\Omega'' = \Omega'$, and hence that $O_1 R$ is symplectic. Since $S$, $Z'$ and $O_1 R$ are all symplectic, then $R^{\mathsf{T}} O_2$ must also be symplectic, which proves the existence of the Euler decomposition.

Note that, since any matrix in the compact subgroup $K(n)$ has determinant 1, the Euler decomposition implies that any symplectic matrix has determinant 1. Moreover, it shows that $K(n) = Sp_{2n,\mathbb{R}} \cap O(2n)$ is the maximal compact subgroup of $Sp_{2n,\mathbb{R}}$ (as any element of $Sp_{2n,\mathbb{R}}$ with any singular value different from 1 may not belong to a compact subgroup).

Compact symplectic operations are also known as 'passive' operations, in the sense they preserve the number of excitations of the system, or equivalently the free Hamiltonian $\hat{\mathbf{r}}^t \hat{\mathbf{r}}$. In the quantum optics laboratory, they model passive elements, essentially beam splitters (semi-reflectant mirrors that mix two modes up) and phase shifters (dielectric plates that rotate the polarisation of a travelling electromagnetic wave with respect to a given reference). More precisely, a beam splitter is described by an orthogonal on two modes mixing $x$'s and $p$'s in the same way:

$$S_{BS} = \begin{pmatrix} \cos\theta & 0 & \sin\theta & 0 \\ 0 & \cos\theta & 0 & \sin\theta \\ -\sin\theta & 0 & \cos\theta & 0 \\ 0 & -\sin\theta & 0 & \cos\theta \end{pmatrix} , \tag{1.60}$$

where $\cos^2\theta$ is the transmittivity of the semi-reflectant mirror, while a phase shifter is simply a local rotation:

$$S_{PS} = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} , \tag{1.61}$$

where $\varphi$ represents the phase shift of the polarisation vector.

Note that, if one switches to complex variables $\alpha$, a phase shifter just multiplies $\alpha$ by a phase $\mathrm{e}^{i\varphi}$, while a beam splitter rotates $\alpha_1$ and $\alpha_2$. Hence, recalling the simple expression (1.46) for any orthogonal symplectic in terms of a unitary matrix, and observing that any unitary can be decomposed into a product of diagonal local phase multiplication and $2 \times 2$ real rotations, one is led to conclude that *any passive symplectic operation is the product of beam splitter and phase shifters*, given above.

Going back to the Euler decomposition, it is clear that it can be interpreted to state that any symplectic operation, and hence any purely quadratic operation at the Hilbert space level, can be decomposed as the product of passive operations and local squeezing operations, where by a local squeezing $S_{SQ}$ we intend a symplectic acting on a single mode by contracting a canonical variable and expanding the conjugate one:

$$S_{SQ} = \begin{pmatrix} z_j & 0 \\ 0 & z_j^{-1} \end{pmatrix} . \tag{1.62}$$

In quantum optics, a squeezing operation is obtained by employing nonlinear crystals pumped by an accessory laser field, in set-ups which are referred to as parametric oscillators or parametric amplifiers (depending on whether the light field is in a cavity, or a travelling wave). Such operations require energy, in the sense that they do not commute with the free Hamiltonian $\hat{\mathbf{r}}^{\mathsf{T}}\hat{\mathbf{r}}$. These symplectic operations are not generated by strictly positive Hamiltonians.

We have established the notable result that any symplectic operation can be obtained as the product of single-mode squeezers and phase shifters and two-mode beam splitters.

**Problem.** Show that the Hamiltonian matrix generating a local squeezing operation is not positive.

**Problem.** Let us define a purely non-compact symplectic operation $S = \mathrm{e}^{\Omega H}$ as one where the generator $\Omega H$ is symmetric, and thus has real eigenvalues. Show that any Hamiltonian matrix generating a purely non-compact symplectic operation is not positive.

*Solution.* If $\Omega H = F$, with $F^{\mathsf{T}} = F$, then $H = -\Omega F$. From $H = H^{\mathsf{T}}$ (all symplectic transformations are generated by $\Omega$ times a symmetric matrix), one has $-\Omega F = F\Omega$, which implies $F = \Omega F \Omega$. Now, assume $\mathbf{v}^{\mathsf{T}} H \mathbf{v} > 0$ for some real vector $\mathbf{v}$, then one has

$$\mathbf{v}^{\mathsf{T}}\Omega^{\mathsf{T}} H \Omega \mathbf{v} = -\mathbf{v}^{\mathsf{T}}\Omega H \Omega \mathbf{v} = \mathbf{v}^{\mathsf{T}}\Omega^2 F \Omega \mathbf{v} = \mathbf{v}^{\mathsf{T}}\Omega F \mathbf{v} = -\mathbf{v}^{\mathsf{T}} H \mathbf{v} < 0$$

by hypothesis. Thus, $H$ is not definite positive nor negative, since it has a positive and a negative eigenspace of dimension $n$ (as for any vector on which the quadratic form $H$ is positive one can identify an orthogonal vector on which it is negative).

### 1.2.4 Normal modes

The normal mode decomposition, whereby a positive definite quadratic form is split into 'decoupled' degrees of freedom, is instrumental in diagonalising quadratic Hamiltonians, and will represent one of the methodological cornerstones of the material covered in this book. This technique, well established since the early days of classical mechanics, can be summarised in the following statement:

Given a $2n \times 2n$ positive definite real matrix $M$, there exists a symplectic transformation $S \in Sp_{2n,\mathbb{R}}$ such that

$$SMS^{\mathsf{T}} = D \quad \text{with} \quad D = \mathrm{diag}(d_1, d_1, \ldots, d_n, d_n)\,, \tag{1.63}$$

with $d_j \in \mathbb{R}^+ \;\forall\; j \in [1, \ldots, n]$.

Since $M$ is invertible and with strictly positive eigenvalues, a set of real matrices $S$ satisfying Eq. (1.63) may be constructed as $S = D^{1/2}OM^{-1/2}$, for all $O \in O(2n)$. We have to show that a choice of the orthogonal transformation $O$ exists such that this matrix is symplectic, which is equivalent to

$$D^{1/2}OM^{-1/2}\Omega M^{-1/2}O^{\mathsf{T}}D^{1/2} = \Omega\,, \tag{1.64}$$

where we have made use of the symmetry of $M$ and $D$. Now, the matrix $\Omega' = M^{-1/2}\Omega M^{-1/2}$ is clearly anti-symmetric, and for any $2n \times 2n$ real anti-symmetric matrix there exists an orthogonal transformation $O \in O(2n)$ which puts it in a decoupled canonical form, as per:

$$O\Omega' O^{\mathsf{T}} = \bigoplus_{j=1}^{n} d_j^{-1}\omega\,, \tag{1.65}$$

where $\omega$ is the $2 \times 2$ antisymmetric block defined in Eq. (1.2) and $d_j \in \mathbb{R}\;\forall\; j \in [1, \ldots, n]$.[5] Hence, one has:

$$D^{1/2}OM^{-1/2}\Omega M^{-1/2}O^{\mathsf{T}}D^{1/2} = D^{1/2}O\Omega' O^{\mathsf{T}}D^{1/2} = \bigoplus_{j=1}^{n} d_j d_j^{-1}\omega = \Omega\,, \tag{1.66}$$

where $D$ has been set to $\mathrm{diag}(d_1, d_1, \ldots, d_n, d_n)$, as anticipated in Eq. (1.63), thus proving the theorem. Note that the quantities $d_j$ must be strictly positive because $M$ is strictly positive.

The symplectic transformation $S$ that turns a matrix $M$ into its normal form is determined by the linear transformation $L$ that diagonalises the matrix $i\Omega M$ (where the conventional factor $i$ is included because the eigenvalues of $\Omega M$ are

[5] The canonical decomposition of anti-symmetric matrices follows from the diagonalisability of symmetric ones: let $A$ be a real, anti-symmetric, $2n \times 2n$ matrix (even dimension is just imposed to fix ideas and because it applies to our case), then $A^2$ is symmetric and can be diagonalised as per $OA^2O^{\mathsf{T}} = B$, with $B$ diagonal and $O \in O(2n)$. Consider then a generic eigenvector $\mathbf{e}_1$ of $A^2$, with eigenvalue $d_1 \in \mathbb{R}$. The vector $\mathbf{e}'_1 = A\mathbf{e}_1$ is clearly orthogonal to $\mathbf{e}_1$, because $A$ is antisymmetric: $\mathbf{e}_1^{\mathsf{T}}A\mathbf{e}_1 = 0$. Let $\mathbf{v}$ be a generic vector in the linear subspace orthogonal to the space spanned by $\mathbf{e}_1$ and $\mathbf{e}'_1$, then one has

$$\mathbf{v}^{\mathsf{T}}A\mathbf{e_1} = \mathbf{v}^{\mathsf{T}}\mathbf{e}'_\mathbf{1} = 0 \quad \text{and} \quad \mathbf{v}^{\mathsf{T}}A\mathbf{e}'_\mathbf{1} = \mathbf{v}^{\mathsf{T}}A^2\mathbf{e_1} = 0\,,$$

as $\mathbf{e_1}$ is an eigenvalue of $A^2$ by hypothesis. The equation above shows that any choice of orthogonal basis including $\mathbf{e}_1$ and $\mathbf{e}'_1$ would result in $A$ acting as a diagonal block $d_1\omega$ in the subspace spanned by $\mathbf{e}_1$ and $\mathbf{e}'_1$. Iterating this argument leads to the canonical decomposition of Eq. (1.65).

purely imaginary). This can be seen by taking the converse of the normal mode decomposition (1.63): $M = S^{-1}DS^{\mathsf{T}-1}$, and noticing that

$$i\Omega M = i\Omega S^{-1}DS^{\mathsf{T}-1} = iS^{\mathsf{T}}\Omega DS^{\mathsf{T}-1} = iS^{\mathsf{T}}\bar{U}\left(\bigoplus_{j=1}^{n} d_j\sigma_z\right)\bar{U}^{\dagger}S^{\mathsf{T}-1} \, , \quad (1.67)$$

where $\bar{U} = \bigoplus_{j=1}^{n} \bar{u}$, and

$$\bar{u} = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \quad (1.68)$$

is the transformation that diagonalises $\omega$: $\bar{u}\omega\bar{u}^{\dagger} = \sigma_z$ (note that this is the very same unitary transformation that appeared in Eq. (1.7) to relate ladder and canonical operators). Eq. (1.67) shows that $i\Omega M$ is always diagonalisable for positive definite $M$ and that, if $L$ is the matrix that diagonalises $i\Omega M$ by similarity (such that $L\Omega ML^{-1}$ is diagonal), then one has $S = \bar{U}L^{\dagger}$ (where we accounted for the fact that transposing a real matrix is the same as conjugating it) for the symplectic transformation $S$ that decomposes $M$ in normal modes by congruence.

Eq. (1.67) also implies that the $n$ quantities $\{d_j, j \in [1, \ldots, n]\}$ are the absolute values of the eigenvalues of $i\Omega M$ (which come in pairs of equal modulus and opposite sign). The $d_j$'s are referred to as the symplectic eigenvalues of the positive definite matrix $M$, while the normal mode decomposition is also known as "symplectic diagonalisation".

Note that, since it preserves the CCR, a symplectic transformation acting on the vector of canonical operators corresponds to defining new canonical degrees of freedom which are linearly related to the original ones. As we shall see in detail in the next section, the normal mode decomposition of a $2n \times 2n$ positive definite quadratic Hamiltonian defines a new set of degrees of freedom which are dynamically decoupled under such a Hamiltonian, and oscillate like free harmonic oscillators. In this instance, the $n$ symplectic eigenvalues correspond to the frequencies of the normal modes (also known as "eigenfrequencies" or "normal" frequencies). Let us emphasise that the normal mode decomposition only holds for positive definite matrices, in that a real symplectic $S$ doing the job could only be constructed as above for such matrices.[6] A few considerations about non definite cases, notably including the free Hamiltonian $\hat{p}^2$, will be postponed to Appendix **??**.

## 1.3 Normal mode decomposition of a Gaussian state

Let us now go back to our definition of the set of a Gaussian state given by Eqs. (1.16), (1.17) and (1.18), in terms of a positive definite Hamiltonian matrix

[6] Trivially, the decomposition extends to negative definite matrices too, which are equivalent to positive definite up to a minus sign.

$H$, a vector of displacements $\mathbf{r}$ and an inverse temperature $\beta$. We have already seen how to reduce the vector parameter $\mathbf{r}$ to the action of a unitary Weyl operator. The normal mode decomposition puts us in a position to analyse the role of $H$ as well. In fact, because of the theorem proven in the previous section, one can write

$$H = S_H^{\mathsf{T}} \left( \bigoplus_{j=1}^{n} \omega_j \mathbb{1}_2 \right) S_H \quad \text{for} \quad S_H \in Sp_{2n,\mathbb{R}} \,, \tag{1.69}$$

where $S_H$ is the transpose and inverse of the (not necessarily unique) symplectic transformation that puts $H$ in normal form acting by congruence, which always exists because $H > 0$ by hypothesis, and the $\omega_j$'s are the symplectic eigenvalues of $H$ (the frequencies of its normal modes). Eq. (1.69) leads to

$$\hat{\mathbf{r}}^{\mathsf{T}} H \hat{\mathbf{r}} = \hat{\mathbf{r}}^{\mathsf{T}} S_H^{\mathsf{T}} \left( \bigoplus_{j=1}^{n} \omega_j \mathbb{1}_2 \right) S_H \hat{\mathbf{r}} \,. \tag{1.70}$$

But our introduction of the symplectic group was based upon the equivalence between the action of a symplectic transformation on the vector of canonical operators, as in $S_H \hat{\mathbf{r}}$, and the action of a unitary operator generated by a quadratic Hamiltonian. Therefore, a symmetric matrix $J_H$ must exist such that

$$S_H \hat{\mathbf{r}} = \mathrm{e}^{i \frac{1}{2} \hat{\mathbf{r}}^{\mathsf{T}} J_H \hat{\mathbf{r}}} \hat{\mathbf{r}} \mathrm{e}^{-i \frac{1}{2} \hat{\mathbf{r}}^{\mathsf{T}} J_H \hat{\mathbf{r}}} \tag{1.71}$$

(where the operator acts by similarity on each entry of $\hat{\mathbf{r}}$). The matrix $J_H$ is not necessarily unique, and satisfies the equality $S_H = \mathrm{e}^{\Omega J_H}$. Although in practice it may not be possible to determine $J_H$ analytically, such a matrix always exists for any given Hamiltonian matrix $H$. Also note that here the parameter $t$, which we employed above in our treatment of the symplectic group, has been absorbed in $J_H$. Inserting Eq. (1.71) into (1.70) yields

$$\hat{\mathbf{r}}^{\mathsf{T}} H \hat{\mathbf{r}} = \mathrm{e}^{i \frac{1}{2} \hat{\mathbf{r}}^{\mathsf{T}} J_H \hat{\mathbf{r}}} \, \hat{\mathbf{r}}^{\mathsf{T}} \left( \bigoplus_{j=1}^{n} \omega_j \mathbb{1}_2 \right) \hat{\mathbf{r}} \, \mathrm{e}^{-i \frac{1}{2} \hat{\mathbf{r}}^{\mathsf{T}} J_H \hat{\mathbf{r}}} \tag{1.72}$$

$$= \mathrm{e}^{i \frac{1}{2} \hat{\mathbf{r}}^{\mathsf{T}} J_H \hat{\mathbf{r}}} \left( \sum_{j=1}^{n} \omega_j \left( \hat{x}_j^2 + \hat{p}_j^2 \right) \right) \mathrm{e}^{-i \frac{1}{2} \hat{\mathbf{r}}^{\mathsf{T}} J_H \hat{\mathbf{r}}} \,. \tag{1.73}$$

We have shown that every quadratic Hamiltonian with zero displacement and positive definite Hamiltonian matrix is unitarily equivalent to the Hamiltonian of a set of free, non-interacting harmonic oscillators. Clearly, the unitary transformation that enacts such an equivalence is generated by quadratic operators too. From now on, let us denote the free Hamiltonian of mode $j$ with frequency $\omega_j$ by the shorthand notation $\hat{H}_{\omega_j}$:

$$\hat{H}_{\omega_j} = \frac{\omega_j}{2} \left( \hat{x}_j^2 + \hat{p}_j^2 \right) \,. \tag{1.74}$$

Putting together Eqs. (1.21) and (1.73), the most general quadratic Hamiltonian $\hat{H}$ of Eq. (1.16) with positive definite Hamiltonian matrix $H$ may be recast in the form:

$$\hat{H} = \frac{1}{2}\hat{\mathbf{r}}^{\mathsf{T}} H \hat{\mathbf{r}} + \hat{\mathbf{r}}^{\mathsf{T}}\mathbf{r} \tag{1.75}$$

$$= \frac{1}{2}\mathrm{e}^{-i\mathbf{r}'^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\mathrm{e}^{i\frac{1}{2}\hat{\mathbf{r}}^{\mathsf{T}}J_H\hat{\mathbf{r}}}\left(\sum_{j=1}^{n}\hat{H}_{\omega_j}\right)\mathrm{e}^{-i\frac{1}{2}\hat{\mathbf{r}}^{\mathsf{T}}J_H\hat{\mathbf{r}}}\mathrm{e}^{i\mathbf{r}'^{\mathsf{T}}\Omega\hat{\mathbf{r}}}\,, \tag{1.76}$$

where $\mathbf{r}' = -H^{-1}\mathbf{r}$, $H = \mathrm{e}^{\Omega J_H}\bigoplus_{j=1}^{n}\omega_j\mathbb{1}_2\mathrm{e}^{-J_H\Omega}$, so that $\{\omega_j, j\in[1,\ldots,n]\}$ is the set of (doubly-degenerate) eigenvalues of $|i\Omega H|$.[7]

Henceforth, it will be expedient to adopt a compact notation for unitary operators with generators of order one and two. Let us define

$$\hat{D}_{\mathbf{r}} = \mathrm{e}^{i\mathbf{r}^{\mathsf{T}}\Omega\hat{\mathbf{r}}} = \hat{D}^{\dagger}_{-\mathbf{r}} \tag{1.77}$$

and

$$\hat{S}_J = \mathrm{e}^{i\frac{1}{2}\hat{\mathbf{r}}^{\mathsf{T}}J_H\hat{\mathbf{r}}}\,, \tag{1.78}$$

so that Eq. (1.76) may be rewritten as

$$\hat{H} = \hat{D}^{\dagger}_{\mathbf{r}'}\hat{S}_{J_H}\left(\sum_{j=1}^{n}\hat{H}_{\omega_j}\right)\hat{S}^{\dagger}_{J_H}\hat{D}_{\mathbf{r}'}\,. \tag{1.79}$$

The same unitary equivalence carries over to Gaussian states, whose operator form $\varrho_G$, as defined in Eqs. (1.17) and (1.18), only depends on the quadratic Hamiltonian $\hat{H}$. Hence, we have derived the most general expression for a Gaussian state $\varrho_G$ as:

$$\varrho_G = \hat{D}^{\dagger}_{\mathbf{r}'}\hat{S}_{J_H}\frac{\left(\bigotimes_{j=1}^{n}\mathrm{e}^{-\beta\hat{H}_{\omega_j}}\right)}{\prod_{j=1}^{n}\mathrm{Tr}\left[\mathrm{e}^{-\beta\hat{H}_{\omega_j}}\right]}\hat{S}^{\dagger}_{J_H}\hat{D}_{\mathbf{r}'}\,,\quad \beta>0\,. \tag{1.80}$$

One then just needs to put the free Hamiltonian $\hat{H}_{\omega_j}$ in diagonal form in order to obtain the spectrum of any Gaussian state.

Notice how the direct sum of Hamiltonians Eq. (1.72), in the 'phase space' picture set by the vector of canonical operators $\hat{\mathbf{r}}$, turned into a tensor product in the Hilbert space representation. This trait, due to the linearity of the operations acting on $\hat{\mathbf{r}}$, will be an important ingredient in much of our treatment of Gaussian states and their information properties.

[7] Note that the $2n^2+n$ real parameters contained in the $2n\times 2n$ real, positive definite matrix $H$, have been transferred into the $2n\times 2n$ symmetric matrix $J_H$ plus the set of $n$ symplectic eigenvalues $\omega_j$'s. The number of free parameters has not changed though, as the transformation performing the symplectic diagonalisation of any positive definite matrix (generated by $\Omega J_H$ in our case) is in general ambiguous due to the invariance of the Hamiltonian matrix $\mathbb{1}_2$ under local rotations, which are symplectic. Hence, the number of parameters is still $2n^2+n$ (a generic symmetric matrix) minus $n$ (due to the invariance that was just mentioned) plus $n$ (the number of symplectic eigenvalues), which is consistent with the previous counting.

## 1.4 The Fock basis

As we just saw, the diagonal form of the free oscillator's Hamiltonian $\hat{H}_{\omega_j}$ of Eq. (1.74) determines the spectrum of any Gaussian state. Obtaining such a diagonal form is one of the very first notions dealt with in most basic quantum mechanics courses. Nonetheless, it is such a cornerstone of our theoretical framework that we will take the opportunity to concisely recall it here.

The Hamiltonian $\hat{H}_{\omega_j}$ may be recast as $\hat{H}_{\omega_j} = \omega_j \left( a_j^\dagger a_j + \frac{1}{2} \right)$ in terms of the annihilation and creation operators defined in Eq. (1.5). Because of the CCR, it can be easily shown that, if $|\lambda\rangle_j$ is an eigenstate of $\hat{H}_{\omega_j}$ with generic eigenvalue $\omega_j \lambda$, then $a|\lambda\rangle_j$ is an eigenvector too, with eigenvalue $\omega_j(\lambda - 1)$. But since the spectrum of $\hat{H}_{\omega_j}$ must be bounded from below, this implies that a state $|0\rangle_j$ must exist such that $a|0\rangle_j = 0$. Such a state is referred to as the vacuum state, and it is the ground state of $\hat{H}_{\omega_j}$, with eigenvalue $1/2$. It is then easy to show that all other eigenvectors of $\hat{H}_{\omega_j}$ may be obtained by $m$ repeated applications of the creation operator $a_j^\dagger$ on $|0\rangle_j$, and that they have eigenvalues $\omega_j \left( m + \frac{1}{2} \right)$, with $m \in \mathbb{N}$. The normalised eigenstates of $\hat{H}_{\omega_j}$ are known as Fock, or number states, and will be denoted with $\{|m\rangle_j, m \in \mathbb{N}\}$. The operator $a_j^\dagger a_j$ is known as the number operator. Let us summarise the action of creation and annihilation operators in the Fock basis:

$$a_j|m\rangle_j = \sqrt{m}|m-1\rangle_j \ , \tag{1.81}$$

$$a_j^\dagger|m\rangle_j = \sqrt{m+1}|m+1\rangle_j \ , \tag{1.82}$$

$$a_j^\dagger a_j|m\rangle_j = m|m\rangle_j \ . \tag{1.83}$$

For a bosonic quantum field, in the second quantization picture, the number state $|m\rangle_j$ represents the presence of $m$ particles (excitations of the field) in mode $j$.

We can now make use of Eq. (1.80) to determine the spectrum of a generic Gaussian state $\varrho_G$ and express it in the Fock basis. The normalisation factor is promptly evaluated:

$$\frac{1}{\mathrm{Tr}\left[\mathrm{e}^{-\beta \hat{H}_{\omega_j}}\right]} = \frac{1}{\mathrm{e}^{-\frac{\beta\omega_j}{2}} \sum_{m=0}^{\infty} \mathrm{e}^{-\beta\omega_j m}} = \mathrm{e}^{\frac{\beta\omega_j}{2}} - \mathrm{e}^{-\frac{\beta\omega_j}{2}} \ , \tag{1.84}$$

so that

$$\varrho_G(\beta) = \left( \prod_{j=1}^{n} \left(1 - \mathrm{e}^{-\beta\omega_j}\right) \right) \hat{D}_{\mathbf{r}'}^\dagger \hat{S}_{J_H} \left( \bigotimes_{j=1}^{n} \left( \sum_{m=0}^{\infty} \mathrm{e}^{-\beta\omega_j m} |m\rangle_{jj}\langle m| \right) \right) \hat{S}_{J_H}^\dagger \hat{D}_{\mathbf{r}'} \ . \tag{1.85}$$

The limit of pure states, $\beta \mapsto \infty$, is particularly simple and instructive in this representation:

$$\lim_{\beta\to\infty} \varrho_G(\beta) = \hat{D}_{\mathbf{r}'}^\dagger \hat{S}_{J_H} |0\rangle\langle 0| \hat{S}_{J_H}^\dagger \hat{D}_{\mathbf{r}'} \ , \tag{1.86}$$

where the shorthand notation $|0\rangle = \bigotimes_{j=1}^{n} |0\rangle_j$ has been introduced to represent the vacuum of the whole field. *All pure Gaussian states are obtained by applying unitary operations generated by quadratic Hamiltonians on the vacuum state.*

Note that the positive parameter $\beta$ is technically redundant, as it might have been absorbed in the Hamiltonian matrix $H$ and, in particular, in its normal frequencies $\omega_j$, as apparent from Eq. (1.85). We have preferred to render it explicit in our treatment because it allows for a very clear definition of the set of pure Gaussian states, and because it relates our formalism to a physical interpretation: the Gaussian state with parameters $H$, $\mathbf{r}$ and $\beta$ is the equilibrium state of a system with local quadratic Hamiltonian $\hat{H}$ after thermalisation with a reservoir at rescaled temperature $1/\beta$. In the next section, we will move on to yet another equivalent parametrisation of a generic Gaussian state.

## 1.5 Statistical moments of a Gaussian state and the covariance matrix

Before proceeding, let us drop the dependence on the quadratic Hamiltonian $\hat{H}$ and assume instead the parametrisation of the most general $n$-mode Gaussian state, given by Eq. (1.85), in terms of a generic symplectic transformation $S$, represented in the Hilbert space by $\hat{S}$, of an arbitrary displacement operator $D_{\mathbf{r}}$, and of a set of $n$ strictly positive real numbers $\xi_j$ (each replacing $\beta\omega_j$ above). The limit of pure states may still be taken by sending all the $\xi_j$ to infinity. Then one has, for the most general Gaussian state $\varrho_G$:

$$\varrho_G = \left( \prod_{j=1}^{n} \left(1 - \mathrm{e}^{-\xi_j}\right) \right) \hat{D}_{\mathbf{r}}^{\dagger} \hat{S}^{\dagger} \left( \bigotimes_{j=1}^{n} \left( \sum_{m=0}^{\infty} \mathrm{e}^{-\xi_j m} |m\rangle_{jj} \langle m| \right) \right) \hat{S} \hat{D}_{\mathbf{r}} \, . \tag{1.87}$$

Also note that, by virtue of Eqs. (1.20) and (1.71), one has

$$\hat{D}_{\mathbf{r}} \hat{\mathbf{r}} \hat{D}_{\mathbf{r}}^{\dagger} = \hat{\mathbf{r}} + \mathbf{r} \, , \tag{1.88}$$

$$\hat{S} \hat{\mathbf{r}} \hat{S}^{\dagger} = S \hat{\mathbf{r}} \, , \tag{1.89}$$

which express the fact that Weyl operators and unitary operators generated by Hamiltonians of order two projectively represent, respectively, the abelian group of translations in dimension $2d$ and the real symplectic group.

Let us now evaluate the expectation value of $\hat{\mathbf{r}}$ for the Gaussian state $\varrho_G$:

$$\begin{aligned}\mathrm{Tr}\left[\varrho_G\hat{\mathbf{r}}\right] &= \prod_{j=1}^{n}\left(1-\mathrm{e}^{-\xi_j}\right)\mathrm{Tr}\left[\left(\bigotimes_{j=1}^{n}\left(\sum_{m=0}^{\infty}\mathrm{e}^{-\xi_j m}|m\rangle_{jj}\langle m|\right)\right)\hat{S}\hat{D}_{\mathbf{r}}\hat{\mathbf{r}}\hat{D}_{\mathbf{r}}^{\dagger}\hat{S}^{\dagger}\right]\\ &= \prod_{j=1}^{n}\left(1-\mathrm{e}^{-\xi_j}\right)\mathrm{Tr}\left[\bigotimes_{j=1}^{n}\left(\sum_{m=0}^{\infty}\mathrm{e}^{-\xi_j m}|m\rangle_{jj}\langle m|\right)(S\hat{\mathbf{r}}+\mathbf{r})\right]\\ &= \prod_{j=1}^{n}\left(1-\mathrm{e}^{-\xi_j}\right)\mathrm{Tr}\left[\bigotimes_{j=1}^{n}\left(\sum_{m=0}^{\infty}\mathrm{e}^{-\xi_j m}|m\rangle_{jj}\langle m|\right)\mathbf{r}\right] = \mathbf{r}\,, \end{aligned} \tag{1.90}$$

where we used the fact that the expectation value of any linear combination of canonical operators vanishes when calculated on a state which is diagonal in the Fock basis. This can be understood by inspecting Eqs. (1.81) and (1.82), and keeping in mind that a linear combination of $\hat{x}_j$'s and $\hat{p}_j$'s is a linear combination of $a_j$'s and $a_j^{\dagger}$'s. The vector parameter $\mathbf{r}$ is then just the vector of expectation values of the canonical operators on the state $\varrho_G$, which could be determined by performing measurements of positions and momenta on non-relativistic particles described by such operators. This will also be referred to as the vector of first (statistical) moments.

Let us then move on to consider second statistical moments of canonical operators on our state. In particular, let us consider the second moments in their symmetrised version, which we shall group together in the 'covariance matrix' $\boldsymbol{\sigma}$:

$$\begin{aligned}\boldsymbol{\sigma} &= \mathrm{Tr}\left[\left\{(\hat{\mathbf{r}}-\mathbf{r}),(\hat{\mathbf{r}}-\mathbf{r})^{\mathsf{T}}\right\}\varrho_G\right]\\ &= \prod_{j=1}^{n}\left(1-\mathrm{e}^{-\xi_j}\right)\mathrm{Tr}\left[\left(\bigotimes_{j=1}^{n}\left(\sum_{m=0}^{\infty}\mathrm{e}^{-\xi_j m}|m\rangle_{jj}\langle m|\right)\right)\hat{S}\hat{D}_{\mathbf{r}}\left\{(\hat{\mathbf{r}}-\mathbf{r}),(\hat{\mathbf{r}}-\mathbf{r})^{\mathsf{T}}\right\}\hat{D}_{\mathbf{r}}^{\dagger}\hat{S}^{\dagger}\right]\\ &= \prod_{j=1}^{n}\left(1-\mathrm{e}^{-\xi_j}\right)\mathrm{Tr}\left[\left(\bigotimes_{j=1}^{n}\left(\sum_{m=0}^{\infty}\mathrm{e}^{-\xi_j m}|m\rangle_{jj}\langle m|\right)\right)\hat{S}\left\{\hat{\mathbf{r}},\hat{\mathbf{r}}^{\mathsf{T}}\right\}\hat{S}^{\dagger}\right]\\ &= \prod_{j=1}^{n}\left(1-\mathrm{e}^{-\xi_j}\right)\mathrm{Tr}\left[\left(\bigotimes_{j=1}^{n}\left(\sum_{m=0}^{\infty}\mathrm{e}^{-\xi_j m}|m\rangle_{jj}\langle m|\right)\right)\left\{S\hat{\mathbf{r}},\hat{\mathbf{r}}^{\mathsf{T}}S^{\mathsf{T}}\right\}\right]\\ &= \prod_{j=1}^{n}\left(1-\mathrm{e}^{-\xi_j}\right)S\mathrm{Tr}\left[\left(\bigotimes_{j=1}^{n}\left(\sum_{m=0}^{\infty}\mathrm{e}^{-\xi_j m}|m\rangle_{jj}\langle m|\right)\right)\left\{\hat{\mathbf{r}},\hat{\mathbf{r}}^{\mathsf{T}}\right\}\right]S^{\mathsf{T}}\,. \end{aligned} \tag{1.91}$$

Thanks to the use we made of group representations, we were able to bring the unitary operators outside the evaluation of the expectation value, which is now reduced to determining the trace in the last expression above. That is a rather straightforward task. First of all, notice that any expectation value involving two canonical operators pertaining to different modes is zero, because the state left inside the trace is diagonal in the Fock basis (this is the same argument by which we showed that the expectation values of linear functions of canonical operators are zero for such states). We are left with the task of evaluating the expectation values of the operators

$$2\hat{x}_j^2 = 2a_j^\dagger a_j + 1 + a_j^2 + a_j^{\dagger 2} \,, \tag{1.92}$$

$$2\hat{p}_j^2 = 2a_j^\dagger a_j + 1 - a_j^2 - a_j^{\dagger 2} \,, \tag{1.93}$$

$$\hat{x}_j\hat{p}_j + \hat{p}_j\hat{x}_j = i(a_j^{\dagger 2} - a_j^2) \,, \tag{1.94}$$

which have been expressed as functions of creation and annihilation operators, for the local state $\sum_{m=0}^{\infty} \mathrm{e}^{-\xi_j m} |m\rangle_{jj}\langle m|$. Only terms with the same number of $a_j$ and $a_j^\dagger$ contribute to the expectation value, because the state we are considering is diagonal in the Fock basis. The only operator that does contribute, besides the identity, is the number operator $a_j^\dagger a_j$, for which one finds

$$\langle a_j^\dagger a_j\rangle = \left(1 - \mathrm{e}^{-\xi_j}\right) \mathrm{Tr}\left[\sum_{m=0}^{\infty} \mathrm{e}^{-\xi_j m} |m\rangle_{jj}\langle m| a_j^\dagger a_j\right] \tag{1.95}$$

$$= \left(1 - \mathrm{e}^{-\xi_j}\right) \sum_{m=0}^{\infty} \mathrm{e}^{-\xi_j m} m = \frac{\mathrm{e}^{-\xi_j}}{1 - \mathrm{e}^{-\xi_j}} \,, \tag{1.96}$$

so that

$$2\langle \hat{x}_j^2\rangle = 2\langle \hat{p}_j^2\rangle = \frac{2\mathrm{e}^{-\xi_j}}{1 - \mathrm{e}^{-\xi_j}} + 1 = \frac{1 + \mathrm{e}^{-\xi_j}}{1 - \mathrm{e}^{-\xi_j}} \,. \tag{1.97}$$

Hence, for the expectation values of the anti-commutators entering Eq. (1.91), one has

$$\prod_{j=1}^{n} \left(1 - \mathrm{e}^{-\xi_j}\right) \mathrm{Tr}\left[\left(\bigotimes_{j=1}^{n}\left(\sum_{m=0}^{\infty} \mathrm{e}^{-\xi_j m} |m\rangle_{jj}\langle m|\right)\right)\left\{\hat{\mathbf{r}}, \hat{\mathbf{r}}^{\mathsf{T}}\right\}\right] = \bigoplus_{j=1}^{n} \frac{1 + \mathrm{e}^{-\xi_j}}{1 - \mathrm{e}^{-\xi_j}} \mathbb{1}_2 \,. \tag{1.98}$$

Upon defining

$$\nu_j = \frac{1 + \mathrm{e}^{-\xi_j}}{1 - \mathrm{e}^{-\xi_j}} \,, \tag{1.99}$$

the covariance matrix (CM) of the most general Gaussian state can be written as

$$\boldsymbol{\sigma} = S\left(\bigoplus_{j=1}^{n} \nu_j \mathbb{1}_2\right) S^{\mathsf{T}} \,, \tag{1.100}$$

with $\nu_j \geq 1$ [see Eq. (1.99)] and $S \in Sp_{2n,\mathbb{R}}$. Eq. (1.100), formally analogous to (1.63), is the normal mode decomposition of the CM $\boldsymbol{\sigma}$, with $\nu_j$ as its symplectic eigenvalues. The spectrum of the state $\varrho_G$ is given in terms of the symplectic eigenvalues alone, as per

$$\varrho_G = \hat{D}_{\mathbf{r}}^\dagger \hat{S}^\dagger \left(\bigotimes_{j=1}^{n}\left(\sum_{m=0}^{\infty} 2\left(\frac{\nu_j - 1}{\nu_j + 1}\right)^m |m\rangle_{jj}\langle m|\right)\right) \hat{S}\hat{D}_{\mathbf{r}} \,. \tag{1.101}$$

Eq. (1.100), along with (1.90), shows that all the parameters of a Gaussian state, $\mathbf{r}$, $S$ and $\{\nu_j\}$, are completely determined by first and second statistical moments, which can then be adopted as a way to parametrise the state. This is in obvious analogy with a Gaussian function, which is also completely determined by first and second order moments. In the following, we will let covariance matrices represent Gaussian states, when first moments will be irrelevant, as is often the case.

## 1.6 The uncertainty principle

Not all symmetric matrices belong to the set of covariances of a quantum state. The non-commutativity of the canonical operators, along with the probabilistic interpretation of the quantum state, impose specific constraints on the variances and covariances of such observables that go under the name of uncertainty principles. We will derive here a geometric uncertainty relation which turns out to be necessary and sufficient for $\boldsymbol{\sigma}$ to be a the CM of a Gaussian state.

Given a – not necessarily Gaussian – quantum state $\varrho$ on a system of $n$ modes, let us define the matrix $\boldsymbol{\tau}$ as

$$\boldsymbol{\tau} = 2\mathrm{Tr}\left[\varrho\hat{\mathbf{r}}\hat{\mathbf{r}}^{\mathsf{T}}\right] \ , \tag{1.102}$$

where $\hat{\mathbf{r}}\hat{\mathbf{r}}^{\mathsf{T}}$ is to be taken in the outer product sense. One has

$$\boldsymbol{\tau} = \mathrm{Tr}\left[\varrho\{\hat{\mathbf{r}},\hat{\mathbf{r}}^{\mathsf{T}}\} + [\hat{\mathbf{r}},\hat{\mathbf{r}}^{\mathsf{T}}]\right] = \boldsymbol{\sigma} + i\Omega\,. \tag{1.103}$$

Now, define the operator $\hat{O} = \sqrt{2}\,\mathbf{y}^{\dagger}\hat{\mathbf{r}}$ for a generic $\mathbf{y} \in \mathbb{C}^{2n}$. Because of the positivity of the density matrix $\varrho$, one has

$$0 \leq \mathrm{Tr}\left[\varrho\hat{O}\hat{O}^{\dagger}\right] = \mathbf{y}^{\dagger}\boldsymbol{\tau}\mathbf{y} = \mathbf{y}^{\dagger}(\boldsymbol{\sigma}+i\Omega)\mathbf{y}\,, \quad \forall\,\mathbf{y}\in\mathbb{C}^{2n}\,. \tag{1.104}$$

That is

$$\boldsymbol{\sigma} + i\Omega \geq 0\ . \tag{1.105}$$

This relationship is manifestly invariant under symplectic transformations, since $\Omega = S\Omega S^{\mathsf{T}}$. It can therefore be expressed in terms of the symplectic eigenvalues, which are the $n$ independent symplectic invariant quantities of a $2n$-mode covariance matrix. By writing (1.105) for the normal mode form of $\boldsymbol{\sigma}$ one gets

$$\boldsymbol{\nu} + i\Omega = \bigoplus_{j=1}^{n}\begin{pmatrix}\nu_j & 1\\ -1 & \nu_j\end{pmatrix} \geq 0\ , \tag{1.106}$$

which co-implies

$$\nu_j \geq 1\ , \quad j\in[1,\ldots,n]\ . \tag{1.107}$$

It may be shown that (1.105) directly implies that $\boldsymbol{\sigma} > 0$, and hence that any $\boldsymbol{\sigma}$ pertaining to a quantum state can be symplectically diagonalised, so that (1.107) is completely equivalent to (1.105). The positive semi-definiteness

$\boldsymbol{\sigma} \geq 0$ is obvious from (1.105) since $\mathbf{v}^{\mathsf{T}}\Omega\mathbf{v} = 0$ for all $\mathbf{v} \in \mathbb{R}^{2n}$. The more restrictive condition $\boldsymbol{\sigma} > 0$ can be established by noting that, if a vector $\mathbf{v}_0$ existed such that $\mathbf{v}_0^{\mathsf{T}}\boldsymbol{\sigma}\mathbf{v}_0 = 0$, then one could always identify a vector $\mathbf{v}_1$ such that $\mathbf{v}_0^{\mathsf{T}}\Omega\mathbf{v}_1 = b \neq 0$ and define a vector $\mathbf{w} = ix\mathbf{v}_0 + \mathbf{v}_1$ for $x \in \mathbb{R}$ for which

$$\mathbf{w}^{\dagger}(\boldsymbol{\sigma} + i\Omega)\mathbf{w} = \mathbf{v}_1^{\mathsf{T}}\boldsymbol{\sigma}\mathbf{v}_1 + 2bx \; . \tag{1.108}$$

A choice of $x$ then would always exist such that $\mathbf{w}^{\dagger}(\boldsymbol{\sigma} + i\Omega)\mathbf{w}$ is negative, thus violating the relationship (1.105).

In our constructive definition of the set of Gaussian states, the relationship (1.107) arose naturally as a sufficient condition on the symplectic eigenvalues. Hence, we can claim that the uncertainty relation (1.105), which is equivalent to (1.107), is necessary and sufficient for $\boldsymbol{\sigma}$ to represent the covariance matrix of a Gaussian state.