Generating Random Gaussian States

References

- arXiv:2401.12435
- Quantum Continuous Variables, Alessio Serafini
- Semidefinite Programming in Q. Information Science, Paul Skrzypczyk · Daniel Cavalcanti
- arXiv:1908.08125, Lecture notes on Free Probability Theory, Roland Speicher

A Quick Review on Gaussian State

- Gaussian states are fully characterized by it's Covariance Matrix (CM); i.e. expectations on position $\hat{x}$ and momentum $\hat{p}$ follow a gaussian distribution. Namely, given the density matrix ρ and the expectation $\langle \cdot \rangle := tr(\rho \, \cdot)$, we define the CM as:

$$S_\rho := \frac{1}{2} \langle \{ \delta x_i , \delta x_j^\dagger \} \rangle , \text{ with}$$

$$x = (x_1, x_2, \dots, x_{2n})$$
$$= (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \dots, \hat{q}_n, \hat{p}_n),$$

w/ $\hat{q}_i, \hat{p}_i$ being the quadratures of the i-th bosonic mode.

The canonical commutation relations can be expressed very concisely as:

$$[x_i, x_j] = i (J)_{ij} , \text{ with}$$

$$J_{2n} := \bigoplus_{i=1}^{N} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$ being called the symplectic form. This is central in the algebraic structure of

Gaussian states.

—1—

▷ why do we care about this stuff?

ⓐ Physicality of states:
Valid quantum states obey:

$$\left\{ S_\rho + i J_{2n} \geq 0 \right\}$$

(This is why we can't just sample from GOE to get random states).

This is basically an way to express the uncertainty principle.

ⓑ Simple computation of relevant physical quantities entirely from the CM.
For instance, the purity is:

$$\left\{ tr(\rho^2) = \frac{1}{\sqrt{\det S_\rho}} \right\}$$

④ A very convenient diagonalization following the underlying algebra. This is Williamson's Theorem. One can write

$$S_\rho = M \, \mathrm{diag}(\nu_1, \nu_1, \nu_2, \nu_2, \dots, \nu_N, \nu_N) M^T$$

Here:

- M is a symplectic transformation, it obeys $M^T J M = J$, i.e. it leaves the symplectic form invariant

- $\{\nu_i\}$ are the symplectic eigenvalues, defined as:

$$\boxed{\nu_i = \mathrm{eig}(i J_{2n} S_\rho)} \quad (\text{s.t. } \nu_i > 0)$$

Note: these eigenvalues come in positive negative pairs $\{\nu_1, -\nu_1, -\nu_2, \nu_2, \dots\}$.

Generating the Random States

Previous technique: by Fukuda & König, and Serafini.

Challenge:

The group

$Sp(2n, \mathbb{R}) = \{ M \in 2n \times 2n$ real sym. matrices : $M J_{2n} M^T = J_{2n} \}$

is not compact, sampling is hard! (Energy is unbounded for Gaussian States)

They perform some random (subset) of symplectic rotations on a pure diagonal matrix after imposing an upper bound on energies.

What do we do?

Strategy: start with arbitrary GOE matrix G.

This likely won't satisfy $G + iJ_{2n} \geq 0$! Solution: transform it as $G \to G + \lambda I$, i.e. shift it by a multiple of the identity in such a way that we satisfy this bona fide relation.

How?. This can be cast as a semi-definite programming problem.

$$\min \|G - H\| \qquad \text{real } 2n\times 2n$$

(*) $$\text{s.t. } H \in \mathcal{M}^{sa}_{2n}(\mathbb{R}) \quad \text{sym. matrices}$$

$$H \geq iJ_{2n}$$

The norm here is, in principle, arbitrary. We'll choose the operator norm, with $\|A\|_{op} = \max_i |\lambda_i|$

Interlude: using the notion of Rayleigh coefficients, finding the minimum/maximum eigenvalue can also be cast as a SDP problem:

$R(M,x) := \frac{x^* M x}{x^* x}$ is maximum for $x = v_{max}$, and $R = \lambda_{max}$

Maximize $\operatorname{tr}(MZ)$

subject to $\langle I, Z\rangle = 1$

$Z \geq 0$

Or, its dual:

Minimize y

subject to $y\mathbb{1} - M \geq 0$

SDP for operator norm $\|A\|_\infty$, chapter 2 of the SDP book.

Thus, one minimizes the scalar $t = \|G-H\|_\infty$, ~~[illegible]~~ choosing the operator $\|\cdot\|_\infty$!

Similar to largest eigenvalue problem but w/ absolute value instead.

$$
\begin{aligned}
&\min \; t \\
&\text{s.t. } H \in \mathcal{M}^{sa}_{2n}(\mathbb{R}),\; t \in \mathbb{R} \\
&\qquad H \geq iJ_{2n} \\
&\qquad -t\, I_{2n} \leq G - H \leq t\, I_{2n}
\end{aligned}
$$

with dual

$$
\begin{aligned}
&\max \; \langle Z, iJ_{2n} - G \rangle \\
&\text{s.t. } Z \in \mathcal{M}^{sa}_{2n}(\mathbb{C}) \\
&\qquad Z \geq 0 \\
&\qquad \cancel{\|Z\|_1 \ldots} \\
&\qquad \operatorname{Tr} Z \leq 1
\end{aligned}
$$

with solution

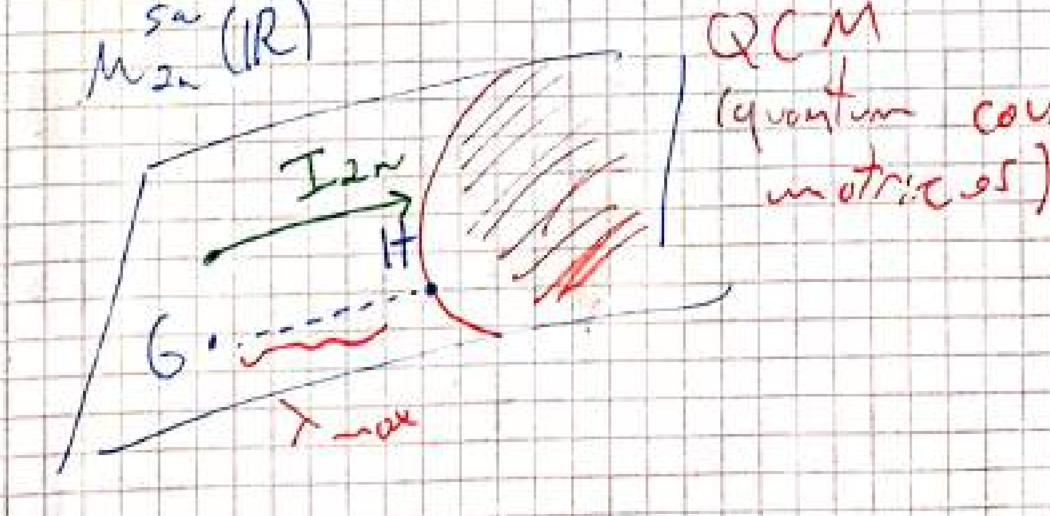
$$\boxed{\lambda(G) = \max\left(0, \lambda_{max}[iJ_{2n} - G]\right)}$$

where $\lambda_{max}[\ldots]$ denotes the largest eigenvalue of a matrix.

And $\boxed{H = G + \lambda(G)\, I_{2n}}$

Note that this last SDP is just the SDP for the matrix $iJ_{2n} - G$, with an inequality (instead of equality) on the trace.

And overall, in the solution we simply shift the (possibly non-physical) matrix G by $\lambda(G) I$, bringing it into the convex hull of valid Gaussian states.



Random Quantum Covariance Matrices (RQCM)

Let $G \in GOE(2n, \sigma)$.

we denote by $RQCM(2n, \sigma)$ the ensemble:

$$S_G := G + \lambda_{max}[iJ_{2n} - G] \cdot \mathbb{I}_{2n},$$

which are all valid CMs.

Proof:

$\lambda_{min}[S_G - iJ_{2n}]$

$= \lambda_{min}[G - iJ_{2n}] + \lambda_{max}[iJ_{2n} - G]$

$= 0$, because $\lambda_{min}[-X] = -\lambda_{max}[X]$. //

Note that those matrices in the RQCM ensemble have $K(2n) = O(2n) \cap Sp(2n)$ symmetry

orthosymplectic group

That is,

$$S_{UGU^T} = U S_G U^T$$

Proof: $S_{UGU^T} = UGU^T + \lambda_{max}[iJ_{2n} - UGU^T] I_{2n}$

$$= UGU^T + \lambda_{max}[U(iU^T J_{2n} U - G)U^T] I_{2n}$$

use orthogonality $UU^T = 1$

$$= UGU^T + \lambda_{max}[i -$$

use symplectic invariance $U^T J_{2n} U = J_{2n}$

$$= UGU^T + \lambda_{max}[iJ_{2n} - G] I_{2n}$$

orthogonality again

$$= U(G + \lambda_{max}[iJ_{2n} - G] I_{2n})U^T$$

$$= US_GU^T$$

— " —

Remarks: for the derivation of the SDP problems, check the Example 2.3 in the book, page 57, as well as examples 2.1 and 2.4.

Interlude: A positive $2n \times 2n$ matrix S_ρ has decomposition

$$S_\rho = M \operatorname{diag}(\nu_1, \nu_1, \nu_2, \nu_2, \dots, \nu_n, \nu_n) M^T,$$

as we saw.

We get these $\{\nu_i\}$ as the positive eigenvalues of $i\Omega M$,

since

$$i\Omega S = B\,(D_n \otimes -\sigma_2)\,B^{-1}, \text{ with}$$

$$B = M^{-T}(I_n \otimes U_2), \text{ w/ } U_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}.$$

That is,

$$D_n \otimes -\sigma_2 = \operatorname{diag}(-\nu_1, \nu_1, -\nu_2, \nu_2, \dots),$$

we pick the positive eigvals of $iJ_{2n}S$, and

$$B = M^{-T}(I_n \otimes U_2) = J_{2n} M J_{2n}^T (I_n \otimes U_2)$$