Distinguishing unitaries with finite energy and a Gaussian Solovay-Kitaev theorem

arXiv 2006.06659

Cambyse Rouzé, Technische Universität München, MCQST

Joint work with Simon Becker (Cambridge) Nilanjana Datta (Cambridge) and Ludovico Lami (Ulm)

February 2021, QIP

Quantum continuous variable (CV) systems

- **Quantum CV systems** are candidates for many protocols of **quantum computation** and **communication**

- CV systems can be hard to analyse (infinite dimensional objects, unboundedness, etc…)

- Important class of CV operations are **Gaussian states**, **channels** and **measurements**

- Advantage: characterized by **covariance matrices**, i.e. admit a **finite dimensional reduction**

How can one construct a theory of approximation of quantum Gaussian circuits?

Outline and motivation

- **From QIT/Resource theory:** Can one quantify the amount of entanglement/energy needed to distinguish quantum channels over arbitrary (separable) Hilbert spaces

  -> Restriction over input states required: **finite energy states**.

Outline and motivation

- **From QIT/Resource theory:** Can one quantify the amount of entanglement/energy needed to distinguish quantum channels over arbitrary (separable) Hilbert spaces

  -> Restriction over input states required: **finite energy states**.

- **From quantum optics:** Given two Gaussian channels, how well can one distinguish them in terms of their defining properties?

Outline and motivation

- **From QIT/Resource theory:** Can one quantify the amount of entanglement/energy needed to distinguish quantum channels over arbitrary (separable) Hilbert spaces

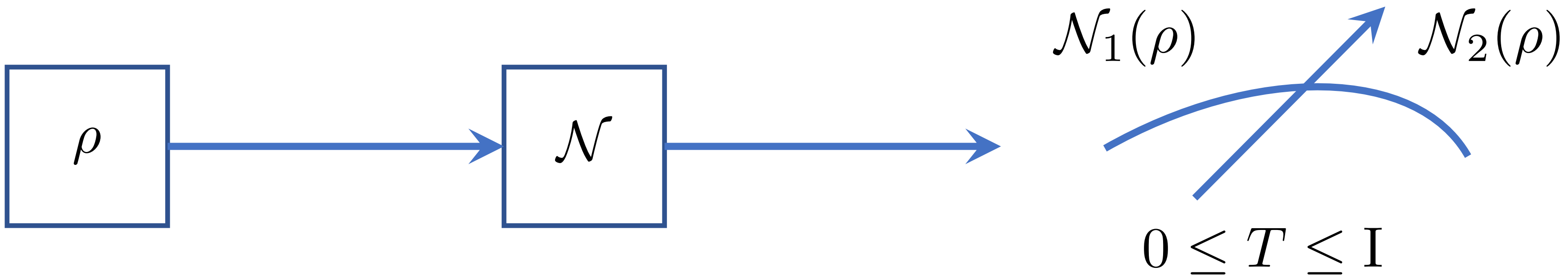
  -> Restriction over input states required: **finite energy states**.

- **From quantum optics:** Given two Gaussian channels, how well can one distinguish them in terms of their defining properties?

  -> Restriction over input states required: **finite energy states**.

- **From CV quantum computing:** How can one efficiently approximate the action of a Gaussian circuit **on low energy states** with precision from a given set of primitive gates?

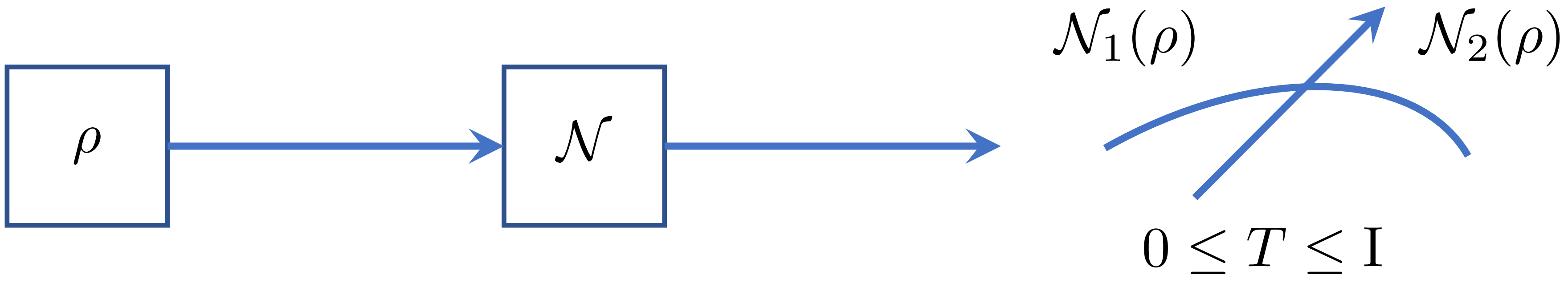
Discriminating quantum channels



$$\mathcal{N} = \begin{cases} \mathcal{N}_1 & \text{w.p. } \frac{1}{2} \\ \mathcal{N}_2 & \text{w.p. } \frac{1}{2} \end{cases}$$

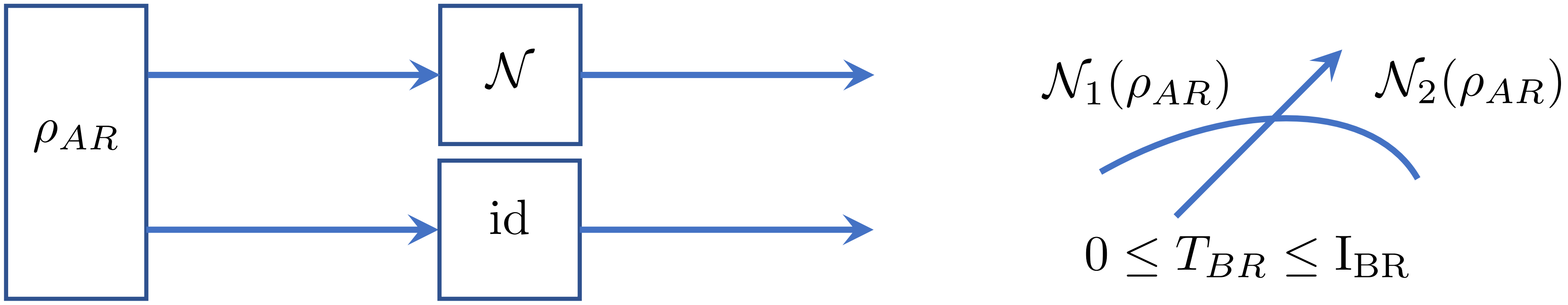
$$\mathbb{P}^{(1)}_{\mathrm{succ}}(\mathcal{N}_1, \mathcal{N}_2) = \sup_{\rho} \mathbb{P}_{\mathrm{succ}}(\mathcal{N}_1(\rho), \mathcal{N}_2(\rho)) = \frac{1 + \frac{1}{2}\|\mathcal{N}_1 - \mathcal{N}_2\|_{1\to 1}}{2}$$

Discriminating quantum channels



$$\mathcal{N} = \begin{cases} \mathcal{N}_1 & \text{w.p. } \frac{1}{2} \\ \mathcal{N}_2 & \text{w.p. } \frac{1}{2} \end{cases}$$

$$\mathbb{P}^{(1)}_{\mathrm{succ}}(\mathcal{N}_1, \mathcal{N}_2) = \sup_{\rho} \mathbb{P}_{\mathrm{succ}}(\mathcal{N}_1(\rho), \mathcal{N}_2(\rho)) = \frac{1 + \frac{1}{2}\|\mathcal{N}_1 - \mathcal{N}_2\|_{1\to 1}}{2}$$



$$\mathbb{P}^{(\mathrm{e.a.})}_{\mathrm{succ}}(\mathcal{N}_1, \mathcal{N}_2) = \sup_{R} \sup_{\rho_{AR}} \mathbb{P}_{\mathrm{succ}}(\mathcal{N}_1(\rho_{AR}), \mathcal{N}_2(\rho_{AR})) = \frac{1 + \frac{1}{2}\|\mathcal{N}_1 - \mathcal{N}_2\|_{\diamond}}{2}$$

The diamond norm and its flaws

$\Lambda : \mathcal{T}_1(\mathcal{H}) \to \mathcal{T}_1(\mathcal{H})$ Hermitian preserving[1] $\|\Lambda\|_\diamond := \sup_R \sup_{|\psi\rangle \in \mathcal{H}_{AR}} \|(\Lambda \otimes \mathrm{id})(|\psi\rangle\langle\psi|)\|_1$

(≤ 2 for channel differences)

Problem: The diamond norm is trivial in simple infinite dimensional situations

Example: Bosonic quantum limited attenuator: $\forall |\alpha\rangle \in L^2(\mathbb{R})$ coherent state, $\mathcal{A}_\eta(|\alpha\rangle\langle\alpha|) := |\eta\alpha\rangle\langle\eta\alpha|$

$\eta \leq 1$

Lemma [Winter 2017] $\|\mathcal{A}_\eta - \mathcal{A}_{\eta'}\|_\diamond = 2\,, \forall \eta \neq \eta'$ $\Rightarrow \mathbb{P}^{(\text{e.a.})}_{\text{succ}}(\mathcal{A}_\eta, \mathcal{A}_{\eta'}) = 1$

Proof: $\| |\eta\alpha\rangle\langle\eta\alpha| - |\eta'\alpha\rangle\langle\eta'\alpha| \|_1 = 2\sqrt{1 - e^{-|(\eta-\eta')\alpha|^2}} \to 2\,, |\alpha| \to \infty$

Physical interpretation: $N := a^\dagger a$ $\quad \langle\alpha|a^\dagger a|\alpha\rangle = |\alpha|^2$

$$\mathbb{P}^{(\text{e.a.})}_{\text{succ}}(\mathcal{N}_1, \mathcal{N}_2) = \frac{1 + \frac{1}{2}\|\mathcal{N}_1 - \mathcal{N}_2\|_\diamond}{2}$$

$\Rightarrow$ Perfect discrimination requires **infinite average energy!**

1 Aharonov et al 1998

Energy constrained diamond (ECD) norm

Fix a Hamiltonian H_A which we assume grounded ($\min \mathrm{Sp}(H_A) = 0$) and average energy $E \geq 0$

Definition (ECD norm) [Shirokov 2017, Winter 2017, Pirandola et. Al. 2017]

$$\|\Lambda\|_{\diamond}^{H,E} := \sup_{R} \sup_{\substack{\rho_{AR} \\ \mathrm{Tr}[\rho_A H_A] \leq E}} \|(\Lambda \otimes \mathrm{id})(\rho_{AR})\|_1$$

$$\leq \sup_{R} \sup_{|\psi\rangle \in \mathcal{H}_{AR}} \|(\Lambda \otimes \mathrm{id})(|\psi\rangle\langle\psi|)\|_1 \equiv \|\Lambda\|_{\diamond}$$

(i) Energy constrained discrimination of unitaries

The ECD distance of unitaries is achieved on product states

[Aharonov, Kitaev, Nisan 1998] No entanglement needed to achieve EC distance between unitaries:

$$2\sqrt{1-\inf_{\rho}|\operatorname{Tr}[\rho U^\dagger V]|^2} = \|\mathcal{U}-\mathcal{V}\|_\diamond = \|\mathcal{U}-\mathcal{V}\|_{1\to 1} = 2\sqrt{1-\inf_{|\psi\rangle}|\langle\psi|U^\dagger V|\psi\rangle|^2}$$

$$\mathcal{U} := U(.)U^\dagger$$
$$\mathcal{V} := V(.)V^\dagger$$

The result extends to the ECD norm:

Theorem: Let U, V be two unitaries, $E \geq 0$, $H \geq 0$

$$\Rightarrow \quad \|\mathcal{U}-\mathcal{V}\|_\diamond^{H,E} = 2\sqrt{1-\inf_{\langle\psi|H|\psi\rangle\leq E}|\langle\psi|U^\dagger V|\psi\rangle|^2}$$

$$\forall E \geq 0,\ \mathbb{P}_{\mathrm{succ}}^{(1),E}(\mathcal{U},\mathcal{V}) = \mathbb{P}_{\mathrm{succ}}^{(\mathrm{e.a.}),E}(\mathcal{U},\mathcal{V})$$

Perfect discrimination with EC and multiple queries

$$2\sqrt{1-\inf_{\rho}|\operatorname{Tr}[\rho U^\dagger V]|^2} = \|\mathcal{U}-\mathcal{V}\|_\diamond = \|\mathcal{U}-\mathcal{V}\|_{1\to 1} = 2\sqrt{1-\inf_{|\psi\rangle}|\langle\psi|U^\dagger V|\psi\rangle|^2}$$

[Acín 2001] Given two unitaries $U \neq V$, there exists $n \in \mathbb{N}$ such that $\|\mathcal{U}^{\otimes n}-\mathcal{V}^{\otimes n}\|_\diamond = 2$

Again, the result extends to the ECD norm: denoting $H^{(n)} := \sum_{j=1}^{n} H_j$ on $\mathcal{H}^{\otimes n}$,

Theorem: Let $U \neq V$ be two unitaries on $H \geq 0$,

$$\exists E < \infty,\ n \in \mathbb{N} \text{ s.t. } \|\mathcal{U}^{\otimes n}-\mathcal{V}^{\otimes n}\|_\diamond^{H^{(n)},E} = 2$$

(ii) Discriminating Gaussian unitaries

Phase space formalism, quick recap

$\mathcal{H} = L^2(\mathbb{R}^m),\ m \in \mathbb{N}$: number of modes

$[a_j, a_k^\dagger] = \delta_{jk}\,\mathrm{I}, [a_j, a_k] = 0$: creation and annihilation operators,

$a_j = \dfrac{x_j + ip_j}{\sqrt{2}}$, x_j, p_j position/momentum operators, $\mathbf{a} = (a_1, ..., a_m)$

$\mathbf{R} = (x_1, p_1, ..., x_m, p_m)$, $[R_j, R_k] = i\,\Omega_{jk}$, $\Omega := \bigoplus_{s=1}^{m} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$: symplectic form

$N := \sum_{j=1}^{m} a_j^\dagger a_j$: number operator

Gaussian unitary channels

Phase space representation: $\mathbb{R}^{2m} \ni \mathbf{z} \mapsto \mathcal{D}(\mathbf{z}) \equiv e^{i\mathbf{z}^T.\Omega\mathbf{R}}$ **displacement operators**

Gaussian unitary channel: characterized by their induced action on the phase space:

$$\mathrm{Sp}_{2m}(\mathbb{R}) := \{S \in \mathbb{M}_{2m}(\mathbb{R}) | \ \ S\,\Omega\,S^T = \Omega\}$$

$$\forall S \in \mathrm{Sp}_{2m}(\mathbb{R}),\ \mathbf{z} \mapsto S\mathbf{z} \quad \Rightarrow \quad U_S^\dagger \mathcal{D}(\mathbf{z}) U_S = \mathcal{D}(S\mathbf{z})$$

symplectic unitaries

Problem: How well can we distinguish S from S' ?

Toolbox: Quantum speed limits

Quantum speed limits: How long does it take for $|\psi_t\rangle = e^{itH}|\psi_0\rangle$ to satisfy $\langle\psi_t|\psi_0\rangle = 0$?

$$\begin{cases} U_t := e^{-itH} \\ V_t := e^{-itH'} \end{cases}$$

Conditions (relative boundedness):

$$\langle\psi||H||\psi\rangle \le \alpha\,\langle\psi|H_0|\psi\rangle + \beta\||\psi\rangle\|^2\,, \qquad \forall|\psi\rangle \in \mathrm{dom}(\sqrt{H_0})$$
$$\|(H - H')|\psi\rangle\| \le \gamma\,\|H|\psi\rangle\| + \delta\||\psi\rangle\|\,, \qquad \forall|\psi\rangle \in \mathrm{dom}(H_0)$$

Theorem: $$\|\mathcal{U}_t - \mathcal{V}_t\|_\diamond^{H_0,E} \le 2\sqrt{2}\,\sqrt{\alpha E + \beta}\,\sqrt{\gamma\, t} + \delta\, t$$

Recall:

$$\|\mathcal{U} - \mathcal{V}\|_\diamond^{H,E} = 2\sqrt{1 - \inf_{\langle\psi|H|\psi\rangle \le E} |\langle\psi|U^\dagger V|\psi\rangle|^2}$$

Back to symplectic unitaries

Quantum speed limits can certainly be used to distinguish symplectic unitaries $U_S, U_{S'}$ for $S \sim S'$

$$S \sim I \quad \Rightarrow U_S = \mathrm{e}^{iP_2(\mathbf{R})}$$

Problem: $\mathrm{Sp}_{2m}(\mathbb{R})$ non-compact $\Rightarrow$ $\exp : \mathrm{sp}_{2m}(\mathbb{R}) \to \mathrm{Sp}_{2m}(\mathbb{R})$ non-surjective

Polar decomposition:

$$S = PO\,, P \in \mathrm{Pos}_{2m}(\mathbb{R}) \cap \exp(\mathrm{sp}_{2m}(\mathbb{R})),\; O \in O_{2m}(\mathbb{R}) \cap \exp(\mathrm{sp}_{2m}(\mathbb{R}))$$

Theorem: For any two symplectic unitaries $U_S, U_{S'}$, $\|S\|_\infty, \|S'\|_\infty \leq r$

$$\|\mathcal{U}_S - \mathcal{U}_{S'}\|_\diamond^{N,E} \leq c\sqrt{m\,E}\,r\,\sqrt{\|(S')^{-1}S - I\|_2}$$

Back to symplectic unitaries

Quantum speed limits can certainly be used to distinguish symplectic unitaries U_S, $U_{S'}$ for $S \sim S'$

$$S \sim I \quad \Rightarrow U_S = \mathrm{e}^{iP_2(\mathbf{R})}$$

Problem: $\mathrm{Sp}_{2m}(\mathbb{R})$ non-compact $\Rightarrow$ $\exp : \mathrm{sp}_{2m}(\mathbb{R}) \to \mathrm{Sp}_{2m}(\mathbb{R})$ non-surjective

Polar decomposition:

$$S = PO\,,\, P \in \mathrm{Pos}_{2m}(\mathbb{R}) \cap \exp(\mathrm{sp}_{2m}(\mathbb{R})),\; O \in O_{2m}(\mathbb{R}) \cap \exp(\mathrm{sp}_{2m}(\mathbb{R}))$$

Theorem: For any two symplectic unitaries $U_S, U_{S'}$, $\|S\|_\infty, \|S'\|_\infty \leq r$

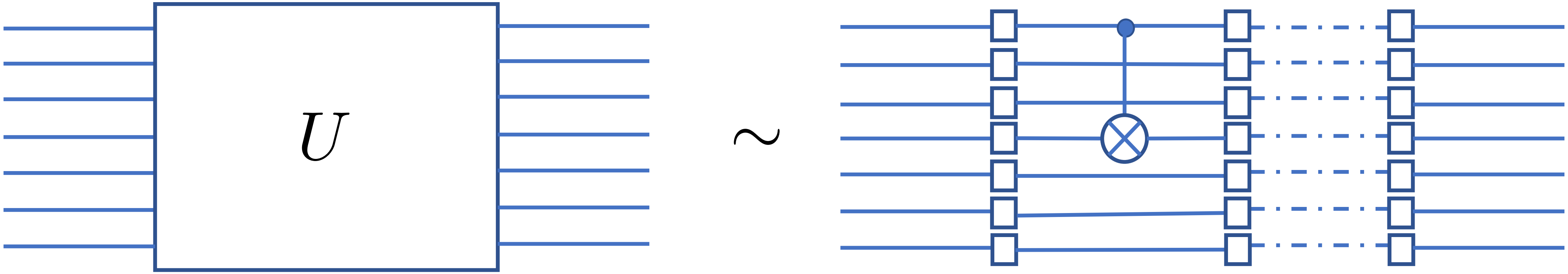
$$\|\mathcal{U}_S - \mathcal{U}_{S'}\|_\diamond^{N,E} \leq c\sqrt{m\,E}\,r\,\sqrt{\|(S')^{-1}S - I\|_2}$$

Maximum squeezing

(iii) A Gaussian Solovay-Kitaev theorem

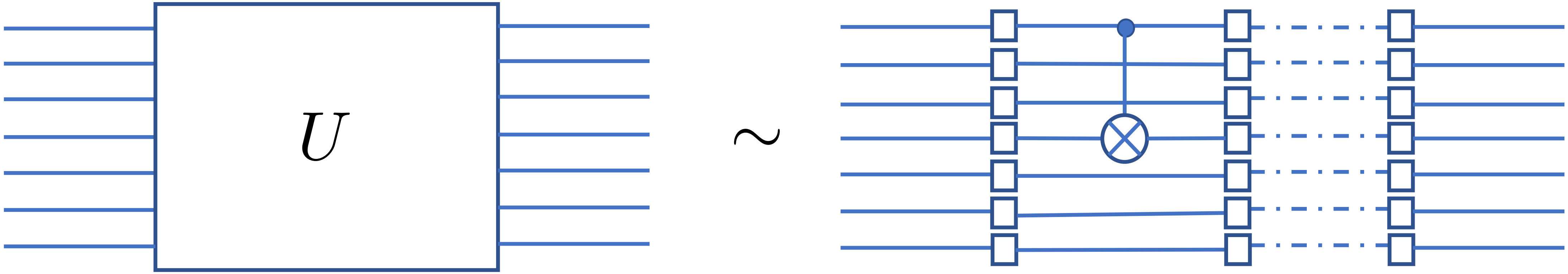
Quantum computing with qubits

Universal gate set: ex: $\mathcal{G}$ = {H, π/8, CNOT} [Boykin et. Al 1999]



Quantum computing with qubits

Universal gate set: ex: $\mathcal{G}$ = {H, π/8, CNOT} [Boykin et. Al 1999]



Efficiency: Assume $\mathcal{G}$ is closed under taking inverses.

Theorem [Solovay 1995, Kitaev 1997]

For any $U \in \mathcal{SU}(2)$, and all $\delta > 0$, there exists a finite concatenation U' of polylog(δ^{-1}) elements from a universal gate set $\mathcal{G}$, which can be found in time polylog(δ^{-1}) and such that

$$\|U - U'\|_\infty < \delta$$

Quantum computing with continuous variables

Universality:

[Lloyd & Braunstein 1999] : Universality in the sense of approximations of unitaries $U = e^{i\,\mathrm{Poly}(\mathbf{R})}$ of finite degree d.

$\mathcal{G}_2$ = {translations, phase shifts, squeezers} generates all quadratic Hamiltonians
+ { Q^3 }: any higher degree achievable.

[Barlett, Sanders, Braunstein & Nemoto 2002] d=2? “Gaussian circuits are classically simulatable”

Efficiency?

The Gaussian Solovay-Kitaev theorem

Here we are interested in efficiently approximating symplectic unitaries U_S where

$$S \in \mathrm{Sp}_{2m}^r := \{S \in \mathrm{Sp}_{2m}(\mathbb{R}),\ \|S\|_\infty \leq r\}$$

Physical interpretation: $\|S\|_\infty$ measures the amount of squeezing induced by S

Fix $\mathcal{G}$ to be any finite generating subset of Sp_{2m}^r containing inverses of its elements.

In practice, any gate set generating the group of passive Gaussian unitary and an arbitrary non-passive Gaussian unitary will do.

Theorem [Becker, Datta, Lami, CR 2020]

For any $S \in \mathrm{Sp}_{2m}^r$ and all $\delta > 0$, there exists a finite concatenation S' of polylog(δ^{-1}) elements from $\mathcal{G}$, which can be found in time polylog(δ^{-1}) and such that

$$\|\mathcal{U}_S - \mathcal{U}_{S'}\|_\diamond^{N,E} \leq c\sqrt{m}\, r^{\frac{3}{2}} \sqrt{E}\sqrt{\delta}$$

Gaussian SV theorem: proof idea

Theorem [Becker, Datta, Lami, CR 2020]

For any $S \in \mathrm{Sp}_{2m}^{r}$ and all $\delta > 0$, there exists a finite concatenation S' of $\mathrm{polylog}(\delta^{-1})$ elements from $\mathcal{G}$, which can be found in time $\mathrm{polylog}(\delta^{-1})$ and such that

$$\|\mathcal{U}_S - \mathcal{U}_{S'}\|_{\diamond}^{N,E} \leq c\sqrt{m}\, r^{\frac{3}{2}} \sqrt{E}\sqrt{\delta}$$

Proof: 2 ingredients:

1) Extension of the original SV theorem to[1] $\{X \in \mathrm{Sp}_{2m}(\mathbb{R}),\ \|X\|_\infty \leq r\}$

2) Use of our bounds on energy constrained diamond norm in order to reduce to 1)

$$\|\mathcal{U}_S - \mathcal{U}_{S'}\|_{\diamond}^{N,E} \leq c\sqrt{m\,E}\, r\,\sqrt{\|(S')^{-1}S - I\|_2}$$

1. [Aharonov, Arad, Eban, Landau 2008] Extension of SV to $\{X \in \mathrm{SL}_d(\mathbb{R}),\ \|X - \mathrm{I}\|_\infty \leq r\}$

Conclusions

Summary of results:

(i) **Entanglement is not necessary** when EC discriminating between unitaries

(ii) **Perfect discrimination** between unitaries possible at finite energy and with finite number of copies

(iii) **New quantum speed limits** measuring the drift between two unitaries of unbounded Hamiltonians

(iv) **A Solovay-Kitaev theorem for symplectic unitaries**

Future direction:

Necessary and sufficient conditions for perfect EC discrimination of non-unitary channels?
Bounds for Gaussian non-unitary (noisy) channels?
Etc…

Thank you for your attention!

$$\mathcal{H},\ \dim(\mathcal{H}) \geq 3 \quad \Rightarrow \quad \|\mathcal{U}-\mathcal{V}\|_\diamond^{H,E} = 2\sqrt{1 - \inf_{\langle\psi|H|\psi\rangle\leq E} |\langle\psi|U^\dagger V|\psi\rangle|^2}$$

Proof: By Schmidt decomposition, $\|\mathcal{U}-\mathcal{V}\|_\diamond^{H,E} = 2\sqrt{1 - \inf_{\mathrm{Tr}[\rho H]\leq E} |\,\mathrm{Tr}[\rho U^\dagger V]|^2}$ $(*)$

Remains to prove that infimum is achieved on pure states.

Theorem (Au-Yeung, Poon 1979) For $d \geq 3$ and Z_1, Z_2, Z_3 s.a.
$F_3 := \{(\langle\psi|Z_1|\psi\rangle,\ \langle\psi|Z_2|\psi\rangle, \langle\psi|Z_3|\psi\rangle);\ |\psi\rangle \in \mathbb{C}^d\}$ is convex.

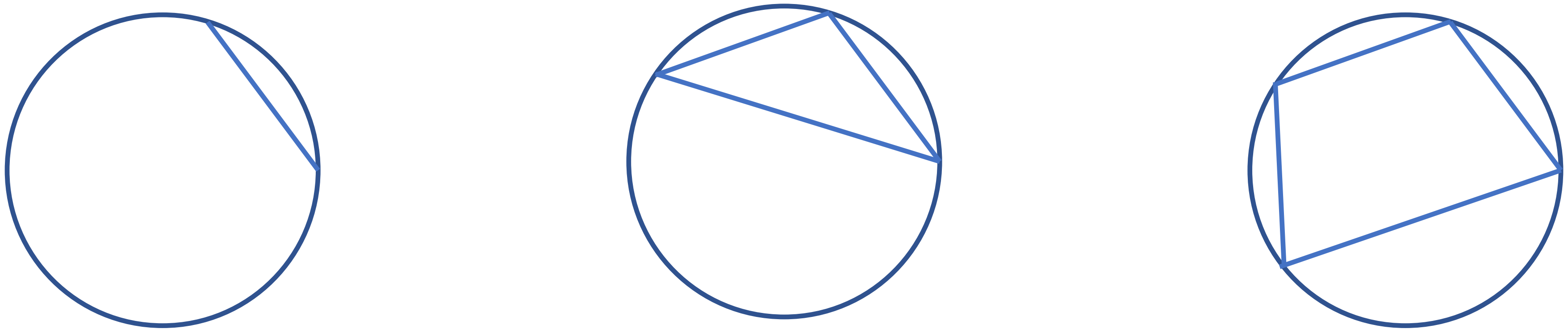
Use it for $(Z_1, Z_2, Z_3) = (\mathrm{Re}(U^\dagger V), \mathrm{Im}(U^\dagger V), H)$, and conclude by $(*)$ and

$$\inf_{\substack{(x,y,z)\in\mathrm{Conv}(R_3)\\ z\leq E}} x^2+y^2 = \inf_{\substack{(x,y,z)\in(R_3)\\ z\leq E}} x^2+y^2 \ \text{(Au-Yeung, Poon)}$$

$$\exists E < \infty,\, n \in \mathbb{N} \text{ s.t. } \|\mathcal{U}^{\otimes n} - \mathcal{V}^{\otimes n}\|_{\diamond}^{H^{(n)},E} = 2$$

Proof: By the previous theorem, we need to prove that there exists an energy such that

$$0 \in \{\langle\psi|(U^\dagger V)^{\otimes n}|\psi\rangle,\ \langle\psi|H^{(n)}|\psi\rangle \leq E\}$$



$U^\dagger V$ $(U^\dagger V)^{\otimes 2}$ $(U^\dagger V)^{\otimes 3}$

Take tensor products of three eigenvectors of $U^\dagger V$ whose eigenvalues triangularize 0, approximate them by vectors in the domain of H. Conclude by Toeplitz-Hausdorff theorem.