Title: Continuous-variable entanglement distillation and non-commutative central limit theorems

Date: Apr 15, 2013 04:00 PM

URL: http://pirsa.org/13040122

Abstract: Entanglement distillation
transforms weakly entangled noisy states into highly entangled states, a
primitive to be used in quantum repeater schemes and other protocols designed
for quantum communication and key distribution. In this work, we present a comprehensive
framework for continuous-variable entanglement distillation schemes that
convert noisy non-Gaussian states into Gaussian ones in many iterations of the
protocol. Instances of these protocols include the recursive Gaussifier
protocol and the pumping Gaussifier protocol. The flexibility of these
protocols give rise to several beneficial trade-offs related to success
probabilities or memory requirements that can be adjusted to reflect
experimental specifics. Despite these protocols involving measurements, we
relate the convergence in this protocols to new instances of non-commutative
central limit theorems. Implications of the findings for quantum repeater
schemes are discussed.

Freie Universität Berlin

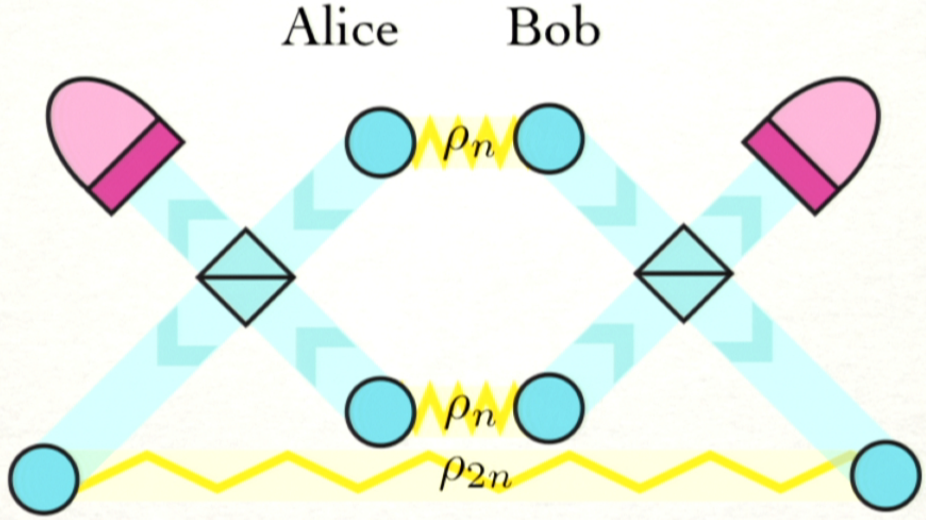
Continuous-variable entanglement distillation and non-commutative central limit theorems

Earl T. Campbell
Marco Genoni
Jens Eisert

[1] Phys. Rev. Lett 108, 020501 (2012)

[2] arXiv:1211.5483 (2012)

Overview 1/3
Setting



Inputs: non-Gaussian, weakly entangled;
Outputs: more Gaussian, often more entangled;
Using: local linear optics.

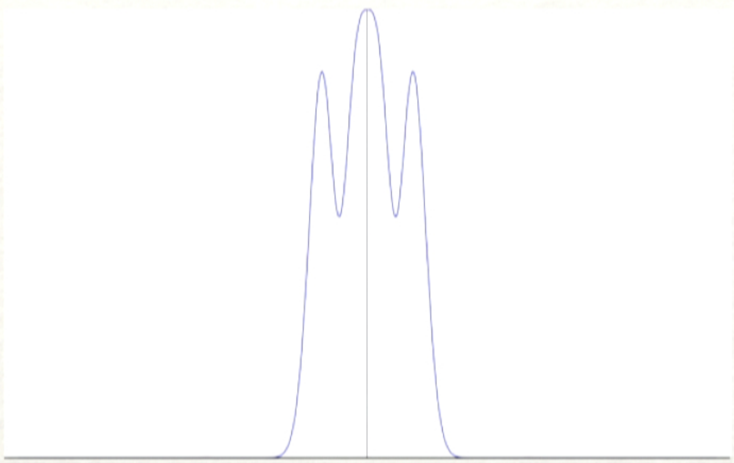
OVERVIEW 2/3
CENTRAL LIMITS

We use non-commutative variants of the following:

consider $S_n = \sum_{j=1}^{N} X_j/\sqrt{N}$

and the characteristic function $\chi_{S_n}(t) = E[\exp(itS_n)]$

then $\chi_{S_n} \to \exp(-\Gamma r^2/4)$



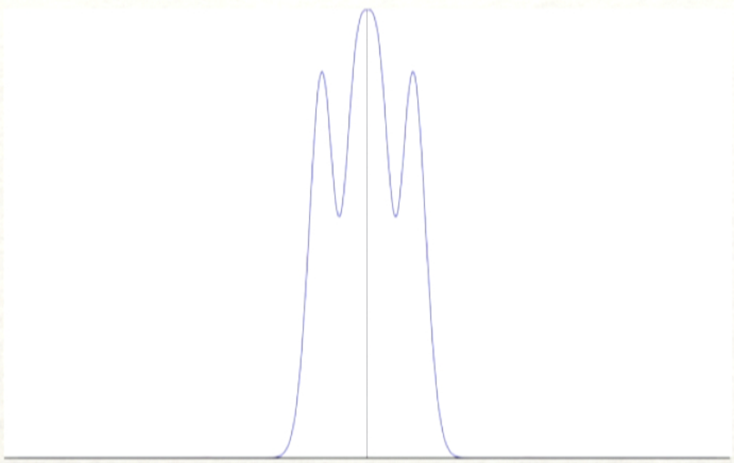
Overview 2/3 Central Limits

We use non-commutative variants of the following:

consider $S_n = \sum_{j=1}^{N} X_j/\sqrt{N}$

and the characteristic function $\chi_{S_n}(t) = E[\exp(itS_n)]$

then $\chi_{S_n} \to \exp(-\Gamma r^2/4)$



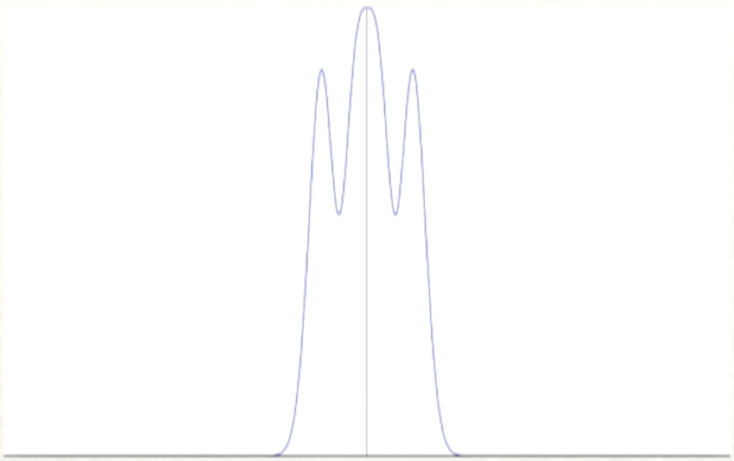
Overview 2/3
Central Limits

We use non-commutative variants of the following:

consider $S_n = \sum_{j=1}^{N} X_j/\sqrt{N}$

and the characteristic function $\chi_{S_n}(t) = E[\exp(itS_n)]$

then $\chi_{S_n} \to \exp(-\Gamma r^2/4)$



CV Notation

The Fock basis of a continuous variable mode is

$$a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$$

Different modes, can have different spatial wavepackets, frequencies or polarizations.

$a_j^\dagger$ where $[a_i, a_j^\dagger] = \delta_{i,j}$

Observables on this space include:

$$\begin{aligned} X_j &= (a_j + a_j^\dagger)/\sqrt{2} \\ P_j &= i(a_j - a_j^\dagger)/\sqrt{2} \end{aligned}$$

Phase space

The "quantum" characteristic function is

$$\chi_\rho(r) = \mathrm{tr}[\exp(i\vec{R}.\vec{r})\rho]$$
$$\vec{R} = (X_1, P_1, X_2, P_2, ...)$$

its Fourier transform is the Wigner function

$$W_\rho(\vec{q}) \propto \int \exp(i\vec{r}.\vec{q})\chi_\rho(\vec{r})d\vec{r}$$

which is a quasi-probability distribution.

Moments

The first moments of a state are

$$d_j = \mathrm{tr}(R_j \rho)$$

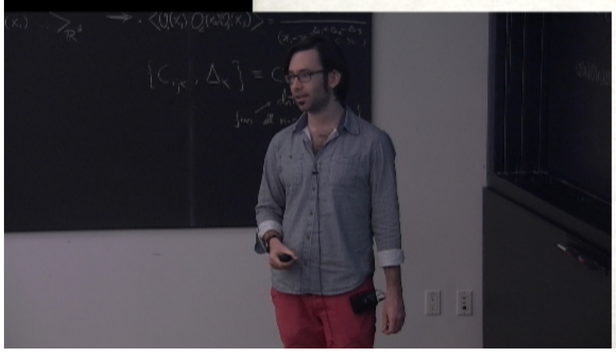
For simplicity, and w.l.o.g, we assume $d_j = 0$

Gaussian States

A state ρ is Gaussian *if and only if:*

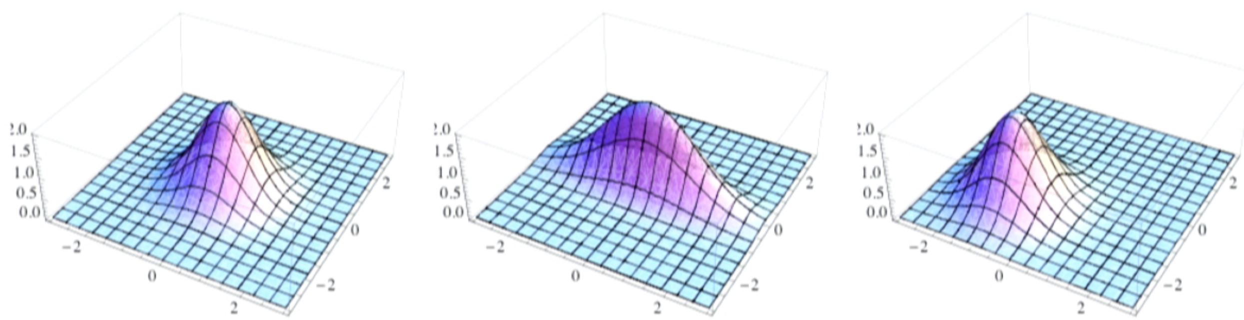
$$\begin{aligned} \chi_\rho(r) &= \mathrm{tr}[\exp(i\vec{R}.\vec{r})\rho] \\ &= \exp(-\vec{r}^T.\Gamma.\vec{r}/4) \end{aligned}$$

where Γ is the covariance matrix for ρ.



Gaussian States

Wigner function examples

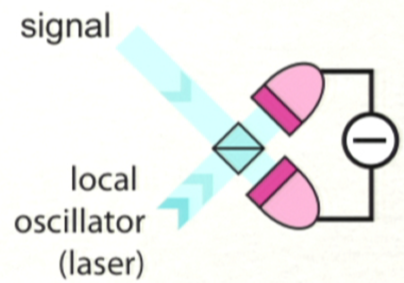


vacuum squeezed coherent

GAUSSIAN MEASUREMENTS

Homodyne

$$X_j = (a_j + a_j^\dagger)/\sqrt{2}$$
$$P_j = i(a_j - a_j^\dagger)/\sqrt{2}$$



Gaussian maps

- Gaussian unitaries and measurements have a simple effect on the covariance matrix
- More generally we can consider Gaussian maps, such that...

Gaussian maps

- Gaussian unitaries and measurements have a simple effect on the covariance matrix
- More generally we can consider Gaussian maps, such that...

$$\rho' = \mathcal{E}(\rho)/\mathrm{tr}[\mathcal{E}(\rho)]$$

If ρ is Gaussian with covariance matrix Γ then ρ' is Gaussian with covariance matrix

$$\Gamma' = \gamma_{AA} - \gamma_{AB}(\gamma_{BB} + \Gamma_\rho)^{-1}\gamma_{AB}^T$$

γ following from Choi-Jamiolkowski duality.

EXTREMALITY

For any ρ there exists a Gaussian state ρ_G with the same covariance matrix Γ

No-Go theorems

Various no-go theorems, show that entanglement cannot be distilled from Gaussian states using Gaussian maps, e.g. [3] that

[1] Fiurasek, *Phys. Rev. Lett.* **89**, 137904
[2] Eisert, Scheel, Plenio, *Phys Rev Lett.* **89**, 137903
[3] Giedke, Cirac, *Phys. Rev. A* **66**, 032316

Circumventing No-Go

A well-known protocol exists that consumes non-Gaussian states but uses Gaussian operations.

- It outputs Gaussian states (*but why?*);
- The entanglement can go up;
- It uses projects onto the vacuum.
- It is ``recursive”.

[5] Browne, Eisert, Scheel, Plenio, *Phys. Rev. A* **67**, 062320
[6] Eisert, Browne, Scheel, Plenio, *Annals of Physics* **311**, 431

Circumventing No-Go

A well-known protocol exists that consumes non-Gaussian states but uses Gaussian operations.

- It outputs Gaussian states (*but why?*);
- The entanglement can go up;
- It uses projects onto the vacuum.
- It is ``recursive''.

[5] Browne, Eisert, Scheel, Plenio, *Phys. Rev. A* **67**, 062320
[6] Eisert, Browne, Scheel, Plenio, *Annals of Physics* **311**, 431

Circumventing No-Go

A well-known protocol exists that consumes non-Gaussian states but uses Gaussian operations.

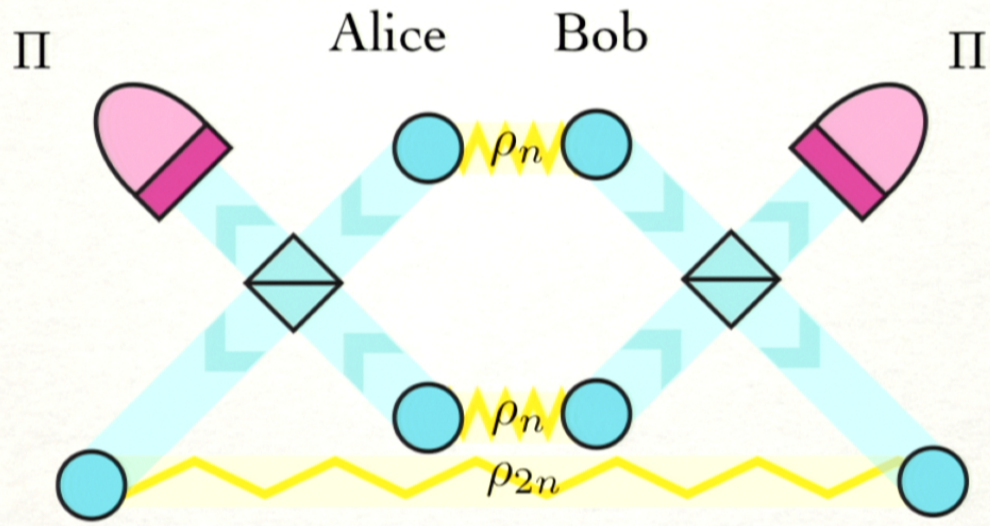
- It outputs Gaussian states (*but why?*);
- The entanglement can go up;
- It uses projects onto the vacuum.
- It is ``recursive".

We extend to a familiy of Gaussifer protocols

- Many different postselection strategies
- Many non-recursive variants.

[5] Browne, Eisert, Scheel, Plenio, *Phys. Rev. A* **67**, 062320
[6] Eisert, Browne, Scheel, Plenio, *Annals of Physics* **311**, 431

Recursive Protocols



Require POVM Π is a Gaussian operator, $\Pi \propto \rho_G$

Here, all beam-splitters 50/50

Requirement on Π

- The POVM element just be Gaussian: $\Pi \propto \rho_G$
- Our proof uses that it must be invertible.
- All Gaussians except projectors are invertible.
- It must have vanishing first moments.

Analysis

Key "trick", instead of studying ρ_n

we follow $\tau_n = \frac{\sqrt{\Pi}\rho_n\sqrt{\Pi}}{\mathrm{tr}(\sqrt{\Pi}\rho_n\sqrt{\Pi})}$

After a little algebra we find

$$\chi_{\tau_n}(\vec{r}) = \chi_{\tau_1}\left(\frac{\vec{r}}{\sqrt{n}}\right)^n$$

whereas the formulae for χ_{ρ_n} is quite involved!

NON-COMMUTATIVE CENTRAL LIMIT THMS

By a non-commutative central limit theorem:

$$\chi_{\tau_n}(r) \to \exp(-r^T \Gamma_\tau r/4)$$

pointwise in $\vec{r}$

Γ_{τ_n} is equal for all n

Also,... $\lim_{n\to\infty} ||\tau_G - \tau_n||_1 = 0$

And so clearly....

$$\lim_{n\to\infty} \langle\psi|\tau_G - \tau_n|\psi'\rangle = 0$$

[4] Wolf, Geidke, Cirac *Phys. Rev. Lett*. **96**, 080502
[7] Campbell, Eisert, *Phys. Rev. Lett*. **108**, 020501 (2012)
[8] Cushen, Hudson, *J. App. Prob*. **8**, 454 (1971)

Inheriting convergence

So $\tau_n \to \tau_G$ but does that really entail $\rho_n \to \rho_G$?

remember:

$$\tau_n = \frac{\sqrt{\Pi}\rho_n\sqrt{\Pi}}{\mathrm{tr}(\sqrt{\Pi}\rho_n\sqrt{\Pi})}$$

Inheriting convergence

So $\tau_n \to \tau_G$ but does that really entail $\rho_n \to \rho_G$?

remember:
$$\tau_n = \frac{\sqrt{\Pi}\rho_n\sqrt{\Pi}}{\mathrm{tr}(\sqrt{\Pi}\rho_n\sqrt{\Pi})}$$

Recall $\lim_{n\to\infty} \langle\psi|\tau_G - \tau_n|\psi'\rangle = 0$

For a basis $\sqrt{\Pi}|\psi_j\rangle = \lambda_j|\psi_j\rangle$

Assuming $\mathrm{tr}(\Pi\rho_n) \to \mathrm{tr}(\Pi\rho_\mathrm{G})$

$$\lim_{n\to\infty}\langle\psi_j|\rho_G - \rho_n|\psi_k\rangle = 0$$

Everything boils down to...

$$? \ \mathrm{tr}(\Pi\rho_n) \to \mathrm{tr}(\Pi\rho_{\mathrm{G}}) \ ?$$

Without much work we can *always* show

$$\mathrm{tr}(\Pi\rho_n) - \mathrm{tr}(\Pi\rho_{\mathrm{G}}) < \delta_n \quad \text{with} \quad \lim_n \delta_n \to 0$$

Recap so far

- Reviewed CV formalism;
- Outlined recursive and pumping Gaussifiers;
- Showed role of non-commutative central limit in proof techniques.

Rest of talk....

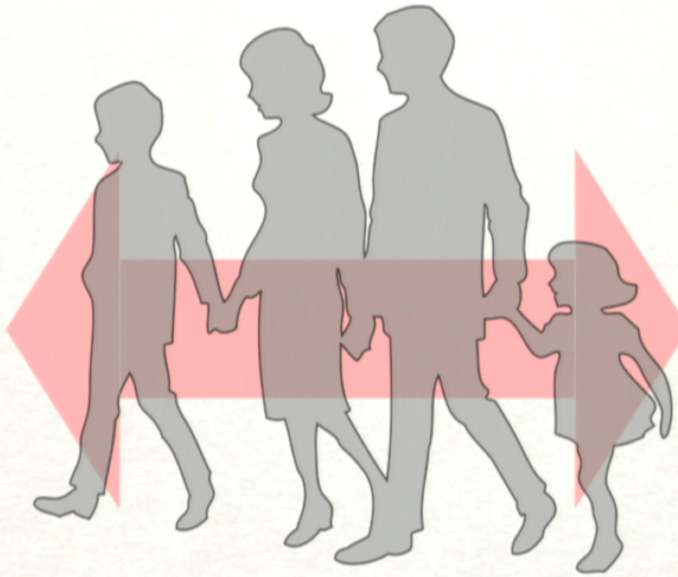
- Choosing the POVM and entanglement distillation
- Quantum repeater networks, and other applications

CHOOSING Π

The family of protocols with $\Pi \propto \rho_G$

Eisert, Browne, Scheel and Plenio, Ann. Phys. **311**, 431 (2004);

$$\Pi = |0,0\rangle\langle 0,0|$$



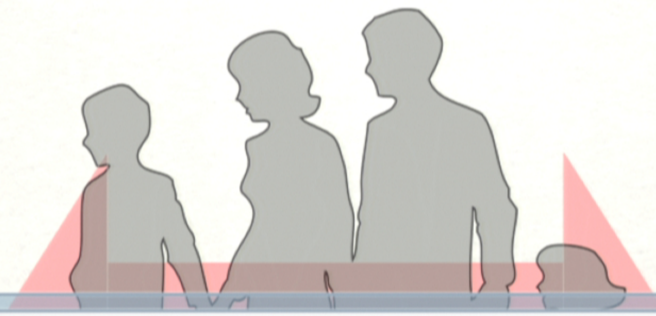
Wolf, Giedke, and Cirac, Phys. Rev. Lett. **96**, 080502 (2006)

$$\Pi = \mathbb{1}$$

CHOOSING Π

The family of protocols with $\Pi \propto \rho_G$

Eisert, Browne, Scheel and Plenio, Ann. Phys. **311**, 431 (2004);



Wolf, Giedke, and Cirac, Phys. Rev. Lett. **96**, 080502 (2006)

Π

*Rarely means:
with zero probability when implemented with reliable 8-port homodyne detectors, non-zero with photon detectors.

1.
2.
3. Rarely* succeeds

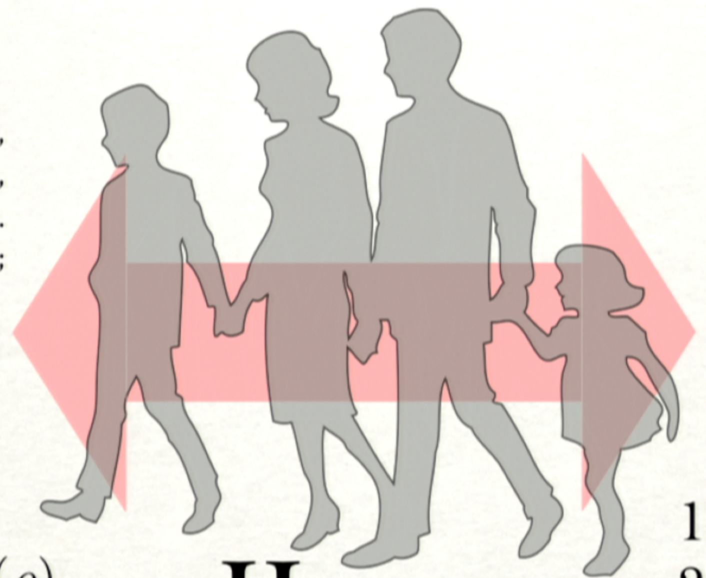
CHOOSING Π

The family of protocols with $\Pi \propto \rho_G$

Eisert, Browne, Scheel and Plenio, Ann. Phys. **311**, 431 (2004);

$\Pi = |0,0\rangle\langle 0,0|$

1. Gaussifies
2. Increases $E(\rho)$
3. Rarely* succeeds

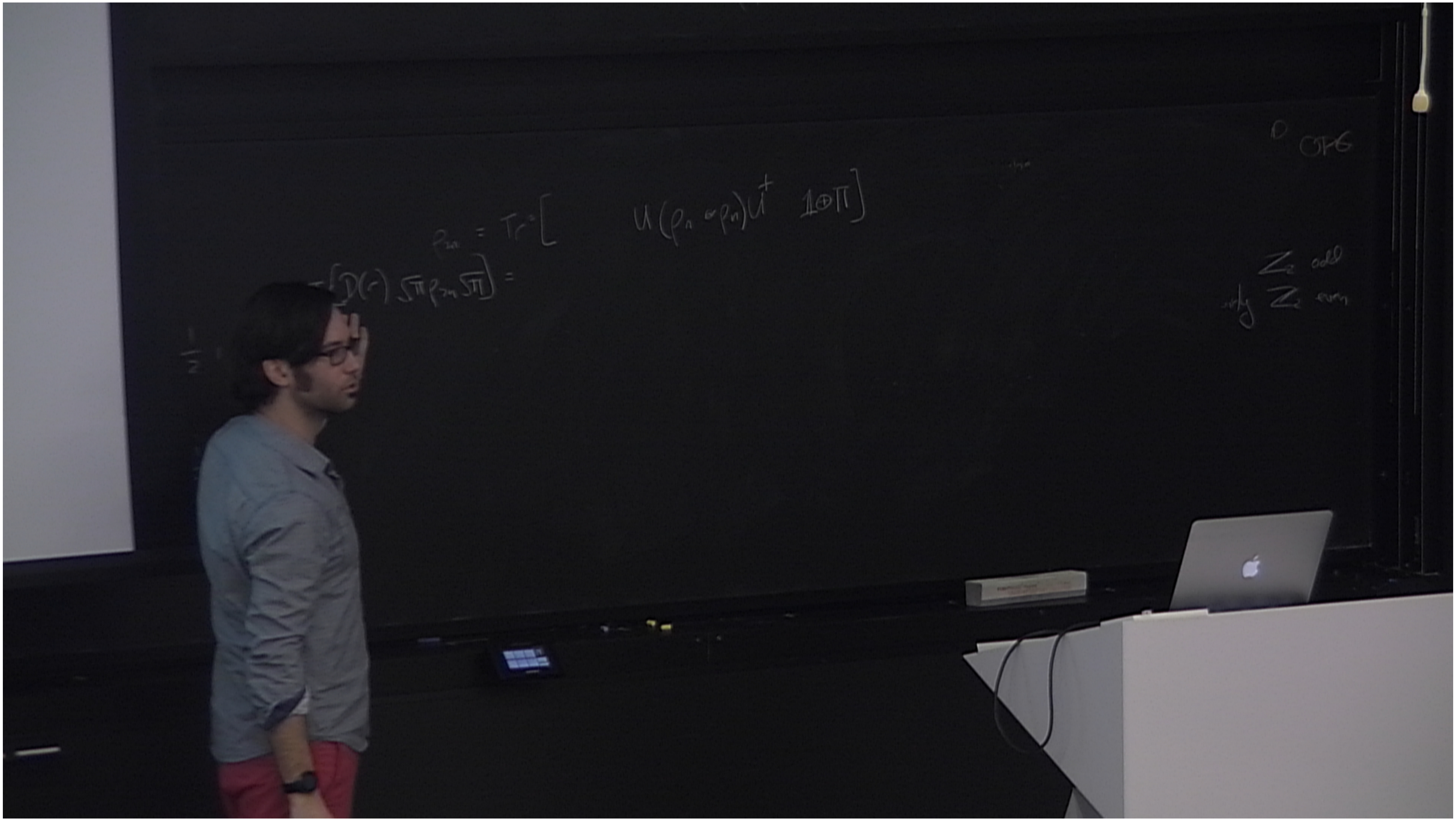


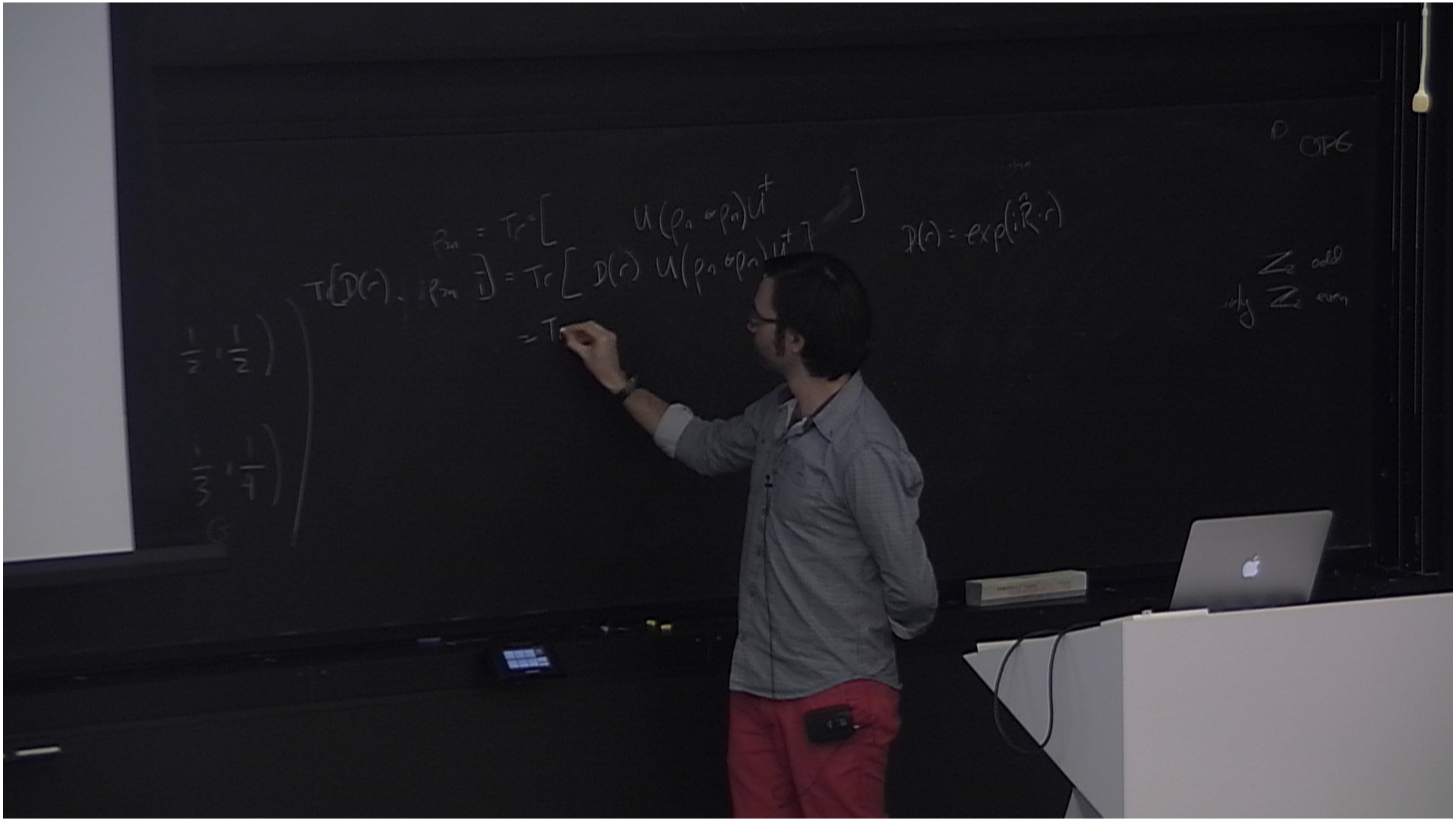
Happy medium

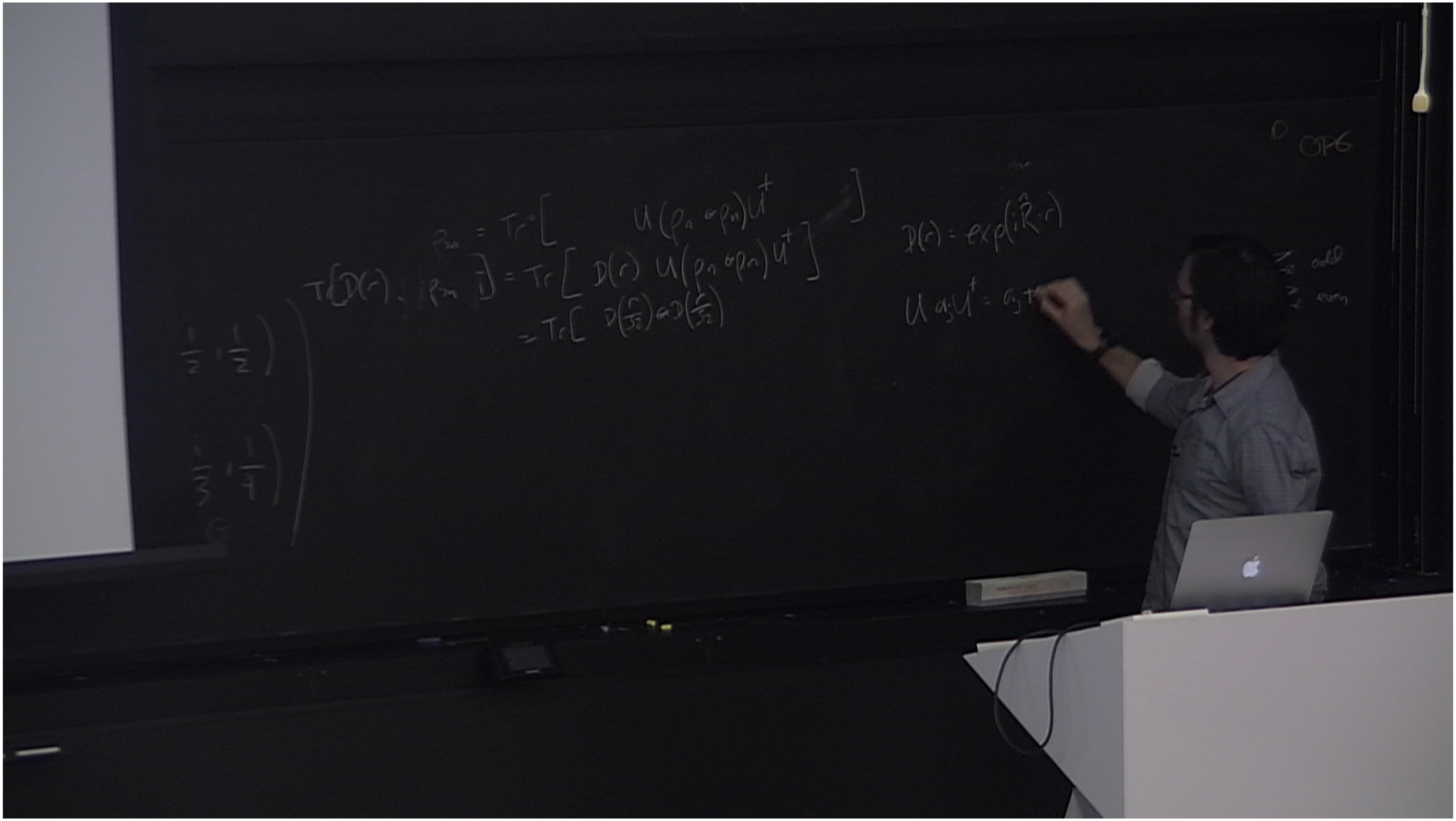
Wolf, Giedke, and Cirac, Phys. Rev. Lett. **96**, 080502 (2006)

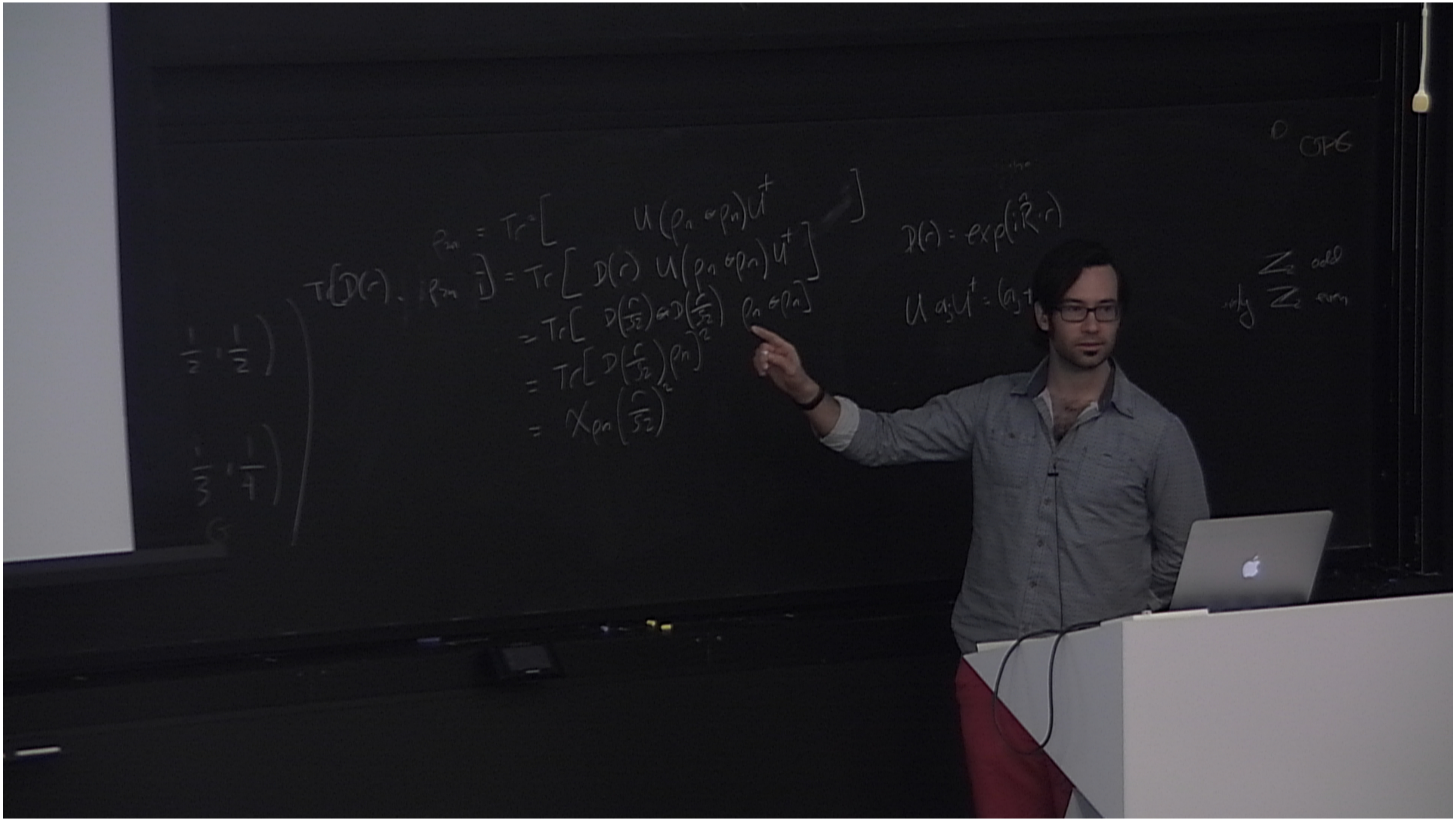
$\Pi = \mathbb{1}$

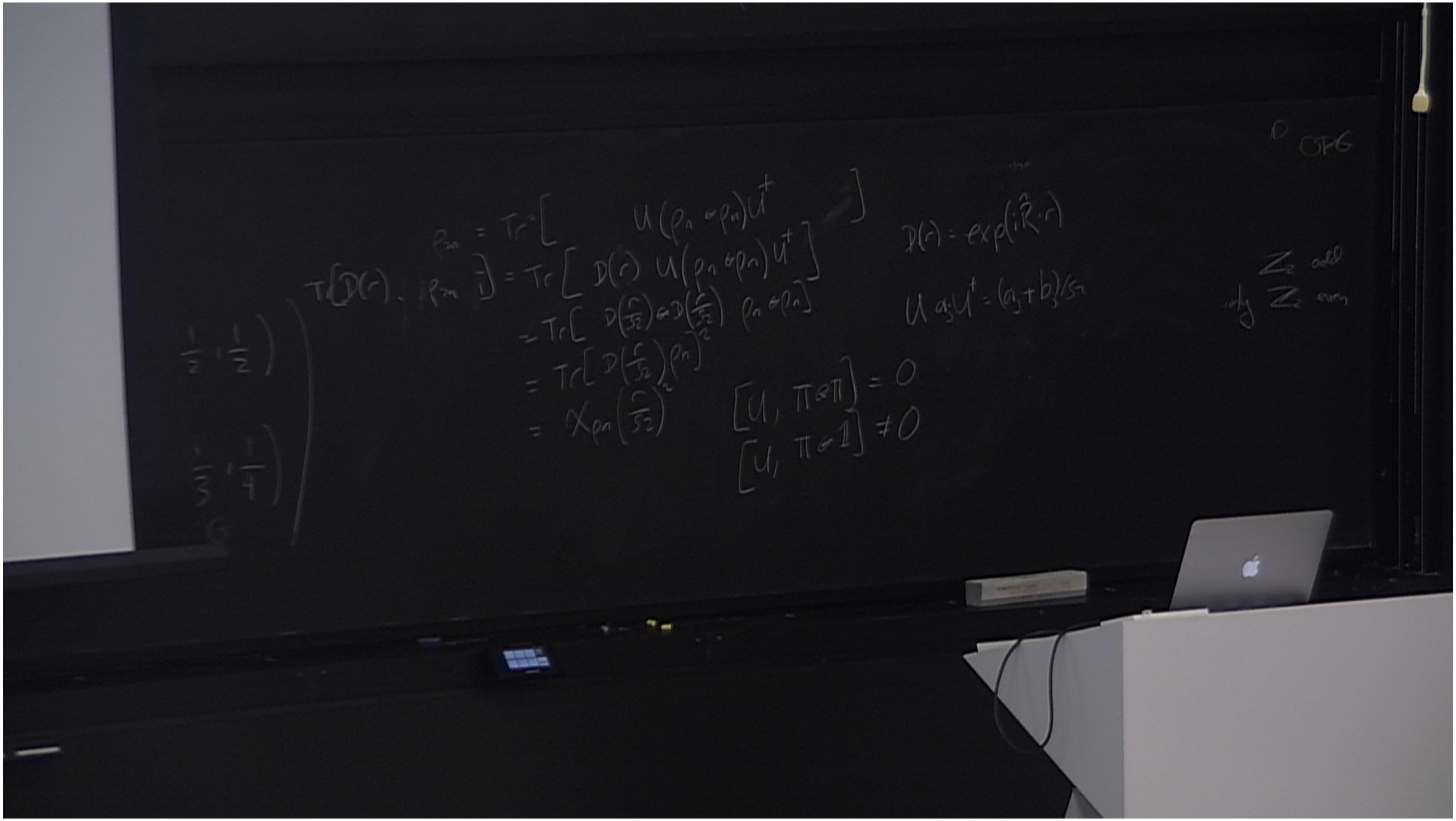
1. Gaussifies
2. Decreases $E(\rho)$
3. Always succeeds




$\mathbb{Z}_2$ odd
$\mathbb{Z}_2$ even






D(r) = exp(iR̂·r)
[U, π⊗π] = 0
[U, π⊗1] ≠ 0

Inheriting convergence

So $\tau_n \to \tau_G$ but does that really entail $\rho_n \to \rho_G$?

remember:
$$\tau_n = \frac{\sqrt{\Pi}\rho_n\sqrt{\Pi}}{\mathrm{tr}(\sqrt{\Pi}\rho_n\sqrt{\Pi})}$$

Recall $\lim_{n\to\infty} \langle\psi|\tau_G - \tau_n|\psi'\rangle = 0$

For a basis $\sqrt{\Pi}|\psi_j\rangle = \lambda_j|\psi_j\rangle$

$$\lim_{n\to\infty}\langle\psi_j|\frac{\rho_G}{\mathrm{tr}(\Pi\rho_G)} - \frac{\rho_n}{\mathrm{tr}(\Pi\rho_n)}|\psi_k\rangle = 0$$

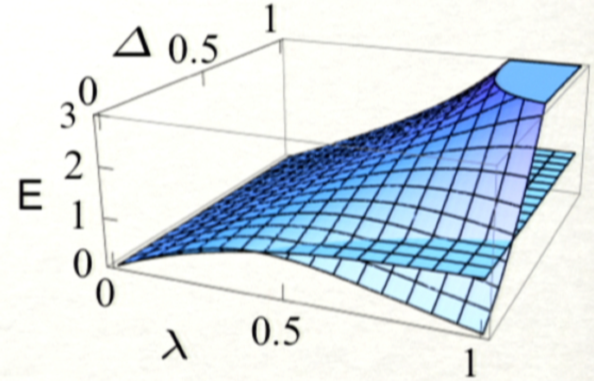
CHOOSING Π

We consider initial states
$|\psi_0\rangle \propto |0,0\rangle + \lambda|1,1\rangle$

Post-select on POVM
$$\Pi = \sum t^n |n\rangle\langle n|$$

Can be implemented using homodyne measurements, or number resolving detector with efficiency $\eta = 1 - t$

$$E = \mathrm{logNeg}(\rho_\infty)$$



$$\Delta = \frac{1-t}{1+t}$$

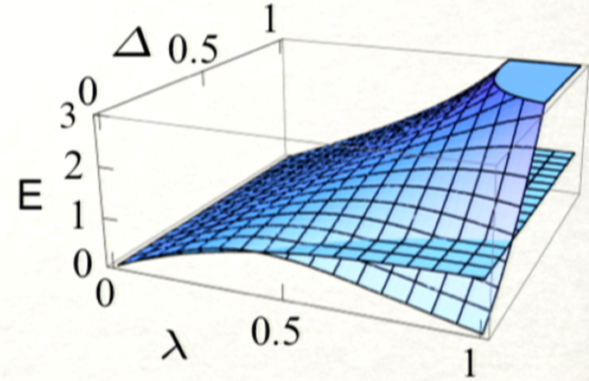
CHOOSING Π

We consider initial states
$|\psi_0\rangle \propto |0,0\rangle + \lambda|1,1\rangle$

Post-select on POVM
$$\Pi = \sum t^n |n\rangle\langle n|$$

Can be implemented using homodyne measurements, or number resolving detector with efficiency $\eta = 1 - t$

$$E = \mathrm{logNeg}(\rho_\infty)$$



$$\Delta = \frac{1-t}{1+t}$$

Quantum repeaters

Dominated by photon loss, though we also allow for a small amount of thermal noise. This gives a noisy channel

$$\Gamma \to \exp^{-l/l_{att}} \Gamma + (1 + 2n_{th})(1 - \exp^{-l/l_{att}})1$$

we take $l_{att} = 22km \qquad n_{th} = 10^-8$

Assume an initially Gaussian source of entanglement

$$\Gamma_\rho = \begin{pmatrix} C & 0 & S & 0 \\ 0 & C & 0 & -S \\ S & 0 & C & 0 \\ 0 & -S & 0 & C \end{pmatrix} \quad \text{with} \quad \begin{matrix} C = \cosh(2r) \\ S = \sinh(2r) \end{matrix}$$

Quantum repeaters

Dominated by photon loss, though we also allow for a small amount of thermal noise. This gives a noisy channel

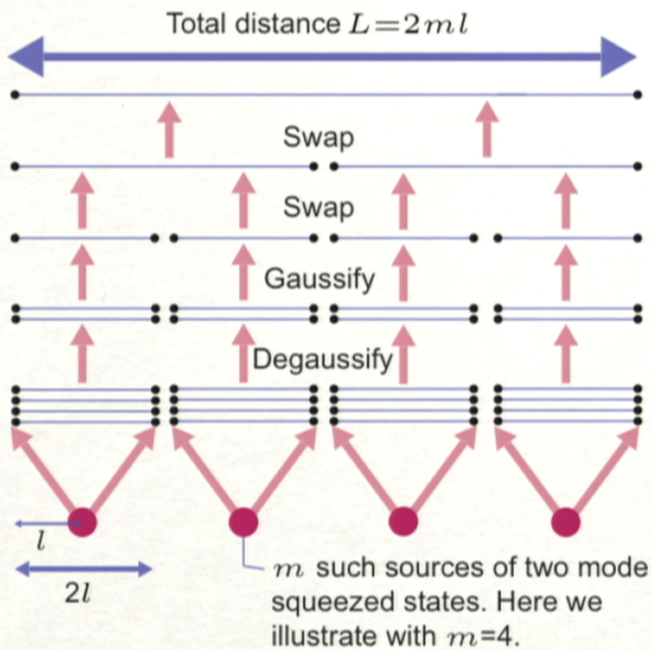
$$\Gamma \to \exp^{-l/l_{att}} \Gamma + (1 + 2n_{th})(1 - \exp^{-l/l_{att}})1$$

we take $l_{att} = 22km$ $\qquad n_{th} = 10^-8$

Assume an initially Gaussian source of entanglement

$$\Gamma_\rho = \begin{pmatrix} C & 0 & S & 0 \\ 0 & C & 0 & -S \\ S & 0 & C & 0 \\ 0 & -S & 0 & C \end{pmatrix} \quad \text{with} \quad \begin{matrix} C = \cosh(2r) \\ S = \sinh(2r) \end{matrix}$$

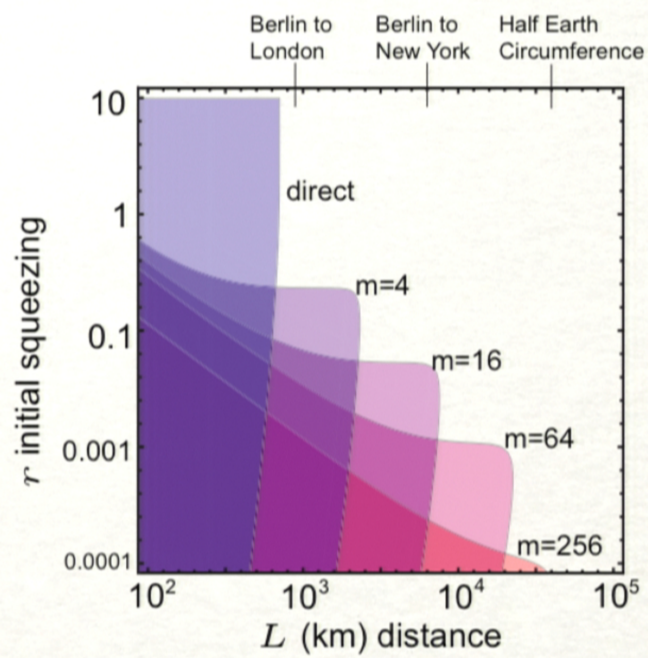
Used in CV Repeaters



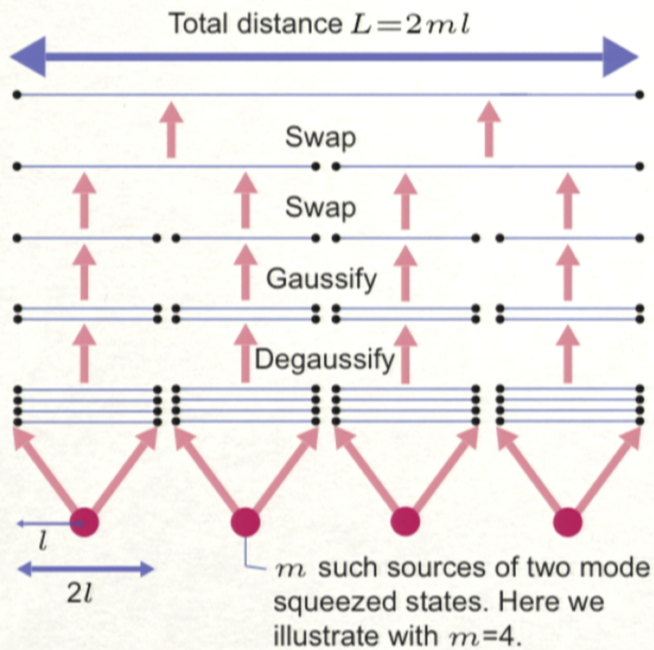
Combining various elements into quantum repeater network.

SUMMARY OF RESULTS

Colored regions indicate we can distribute entanglement over this distance with this squeezing.



Used in CV Repeaters



Combining various elements into quantum repeater network.

OTHER NUMBERS OF MODES

- Techniques can be used to distill tripartite entanglement, e.g. from

$$|\psi\rangle \sim |000\rangle + \mu(|011\rangle + |101\rangle + |110\rangle)$$

- and also increase single-mode squeezing from states like

$$|\psi\rangle \sim |0\rangle + \mu|2\rangle$$

OTHER NUMBERS OF MODES

- Techniques can be used to distill tripartite entanglement, e.g. from

$$|\psi\rangle \sim |000\rangle + \mu(|011\rangle + |101\rangle + |110\rangle)$$

- and also increase single-mode squeezing from states like

$$|\psi\rangle \sim |0\rangle + \mu|2\rangle$$

OTHER NUMBERS OF MODES

- Techniques can be used to distill tripartite entanglement, e.g. from

$$|\psi\rangle \sim |000\rangle + \mu(|011\rangle + |101\rangle + |110\rangle)$$

- and also increase single-mode squeezing from states like

$$|\psi\rangle \sim |0\rangle + \mu|2\rangle$$

Closing remarks

- Many ways to Gaussify.
- Even with measurements, central limit theorems can be leveraged.
- Working in phase space is more intuitive!
- CV rsystems could achieve long distance quantum crypto, but secret key rates are not yet known.
- Potential for clearer conditions for when we have convergence $\mathrm{tr}(\Pi\rho_n) \to \mathrm{tr}(\Pi\rho_G)$
- Rates of convergence?

Closing remarks

- Many ways to Gaussify.
- Even with measurements, central limit theorems can be leveraged.
- Working in phase space is more intuitive!
- CV rsystems could achieve long distance quantum crypto, but secret key rates are not yet known.
- Potential for clearer conditions for when we have convergence $\mathrm{tr}(\Pi\rho_n) \to \mathrm{tr}(\Pi\rho_G)$
- Rates of convergence?

Closing remarks

- Many ways to Gaussify.
- Even with measurements, central limit theorems can be leveraged.
- Working in phase space is more intuitive!
- CV rsystems could achieve long distance quantum crypto, but secret key rates are not yet known.
- Potential for clearer conditions for when we have convergence $\mathrm{tr}(\Pi\rho_n) \to \mathrm{tr}(\Pi\rho_G)$
- Rates of convergence?