Can we Prove that Vacuum is a Global Majorizing State in a Quantum Amplifier ?

**Raul Garcia-Patron, Carlos Navarrete,
Seth Lloyd, Jeff H. Shapiro, and Nicolas J. Cerf**

9th Continuous-Variable Quantum Information Processing Workshop – CV-QIP '12

Frederiksdal (Copenhagen), Denmark, 27-30 April 2012

Outline of this talk

- Classical capacity of Gaussian bosonic channels
  Gaussian minimum (output) entropy conjecture

- Link with entanglement of a 2-mode squeezer
  Gaussian minimum (output) entanglement conjecture

- Approach building on majorization theory
  Gaussian majorization conjecture
  Incomplete proof of the conjecture (Fock state inputs)

- Conclusions — importance in physics !
  … new path to the ultimate proof ?

Context

We wish to calculate the **ultimate** information capacity of optical communication channels

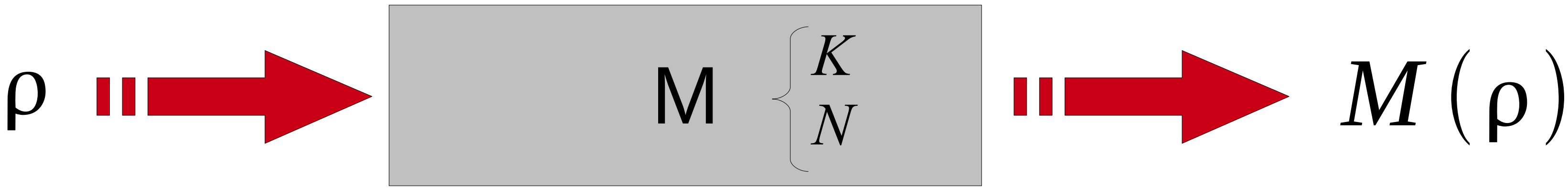
Since communication channels are **"physical devices" ...**

and since physics itself is **"quantum mechanical" ...**

... we need to use the tools of **"quantum information theory"**

Optical links are often modeled by Gaussian bosonic channels
…. we need to use the tools of **"continuous-variable QIP"**

Gaussian (quantum) Bosonic Channels



- Corresponds to linear CP maps $\rho \to M[\rho]$

  s.t. $M[\rho]$ Gaussian if ρ Gaussian

- M fully characterized by two matrices K, N

  $\vec{r} \to K\vec{r}$ — $\vec{r}$ = coherent vector

  $\gamma \to K\gamma K^T + N$ — γ = covariance matrix

  K: real; N: real & symmetric

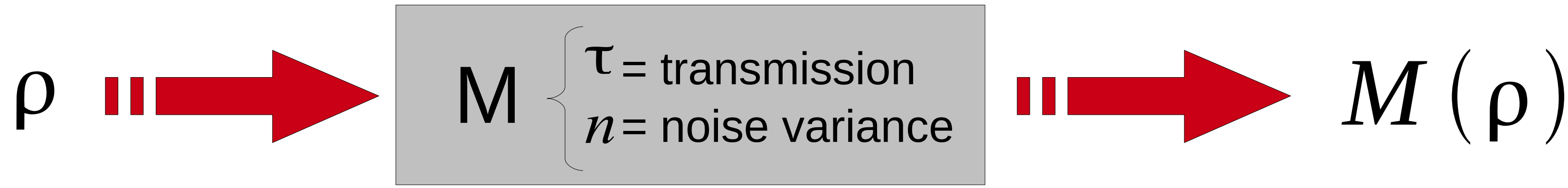
one-mode case

- M completely positive ⟺ $N \geq 0 \quad det\, N \geq (det\, K - 1)^2$

uncertainty principle

Phase-insensitive Gaussian Channels

$$\begin{cases} K = diag(\sqrt{\tau}, \sqrt{\tau}) \\ N = diag(n, n) \end{cases}$$

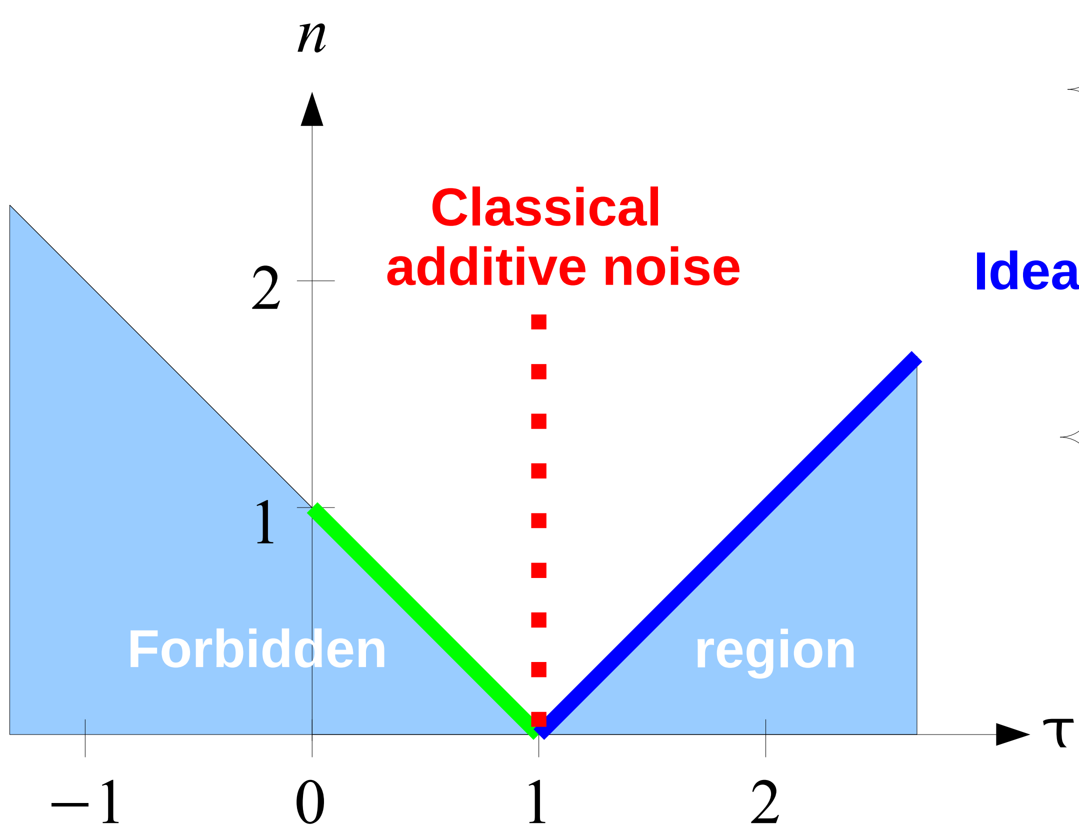


Purely lossy channel

$$\begin{cases} K = diag(\sqrt{T}, \sqrt{T}) \\ N = diag(1-T, 1-T) \end{cases} \qquad (T \leq 1)$$

Ideal (quantum-limited) amplifier

$$\begin{cases} K = diag(\sqrt{G}, \sqrt{G}) \\ N = diag(G-1, G-1) \end{cases} \qquad (G \geq 1)$$



Classical Capacity of Quantum Channels

Holevo, Schumacher, Westmoreland, 1998

- encoding $\{p_a, \rho_a\}_{a=1,\ldots d}$ such that $\sum_a p_a \rho_a = \rho$

- Holevo bound $\chi(\{p_a, \rho_a\}, M) = S(M(\rho)) - \sum_a p_a S(M(\rho_a))$

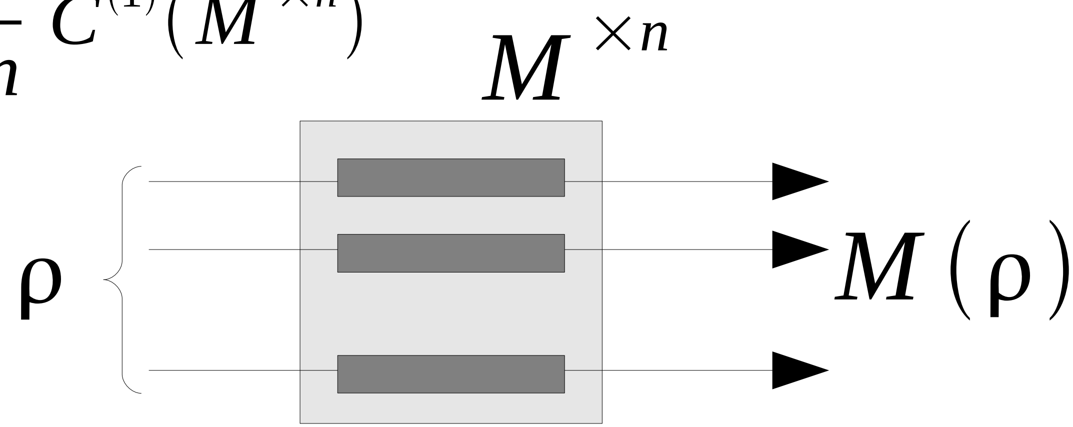
- Single-shot capacity $C^{(1)}(M) = max_{\{p_a, \rho_a\}} \chi(\{p_a, \rho_a\}, M)$

- Capacity $C(M) = \lim_{n\to\infty} \frac{1}{n} C^{(1)}(M^{\times n})$

... in general, <u>not</u> additive !

(Hastings, 2009)

... cfr. Raul Garcia's talk



Role of Minimum Output Entropy

- encoding $\{p_a, \rho_a\}_{a=1,\ldots d}$ such that $\sum_a p_a \rho_a = \rho$

$$C^{(1)}(M) = max_\rho \, \tilde{\chi}(\rho, M)$$

... maximization in 2 steps

with $$\tilde{\chi}(\rho, M) \equiv S\big(M(\rho)\big) - min_{\substack{\{p_a,\rho_a\} \\ \sum_a p_a \rho_a = \rho}} \underbrace{\sum_a p_a S\big(M(\rho_a)\big)}_{\geq S(M(\Phi_0))}$$

$$\leq S\big(M(\rho)\big) - S\big(M(\Phi_0)\big)$$

Upper bound on $C^{(1)}$ relying on <u>pure state</u> Φ_0 <u>minimizing the output entropy</u>

$$min_\sigma S\big(M(\sigma)\big) \equiv S\big(M(\Phi_0)\big)$$

Capacity of Gaussian Quantum Channels

Yuen and Ozawa, 1993

Holevo and Werner, 1998

ρ_α → M $\begin{cases} \tau = \text{transmission} \\ n = \text{noise variance} \end{cases}$ → $M(\rho_\alpha)$

- continuous encoding $\{p(\alpha), \rho_\alpha\}$ such that $\int d^2\alpha \; p(\alpha)\rho_\alpha = \rho$
- energy constraint

$$C^{(1)}(M) = \max_\rho \tilde{\chi}(\rho, M)$$

$$\leq \max_\rho S\big(M(\rho)\big) - \min_\sigma S\big(M(\sigma)\big)$$

for fixed energy, achieved by a thermal state

$$S\big(M(\rho_{therm})\big)$$

$$S\big(M(\Phi_0)\big)$$

with $\Phi_0 =$ minimum output entropy state ???

Gaussian minimum output entropy conjecture: $\Phi_0 = |0\rangle\langle 0|$

Conjectured Single-shot Capacity

ρ_α → M { τ = transmission, n = noise variance } → $M(\rho_a)$

continuous encoding $\{p(\alpha), \rho_\alpha\}$ such that $\int d^2\alpha \; p(\alpha)\,\rho_\alpha = \rho$

$$C^{(1)}(M) \leq S\big(M(\rho_{therm})\big) - S\big(M(|0\rangle\langle 0|)\big)$$

use Gaussian encoding $\rho_\alpha = |\alpha\rangle\langle\alpha|$ $\qquad p(\alpha) = \frac{1}{\pi\nu}\exp\left(\frac{-|\alpha|^2}{\nu}\right)$

with ν = mean thermal photon number

$$C^{(1)}(M) = g[\tau\nu + n] - g[n] \qquad \text{where} \quad g[x] = (x+1)\log(x+1) - x\log(x)$$

→ coherent states modulated with a Gaussian bivariate distribution do achieve the capacity (it is the *optimal encoding*)

... provided the Gaussian minimum entropy conjecture holds !

Gaussian Minimum Entropy Conjecture

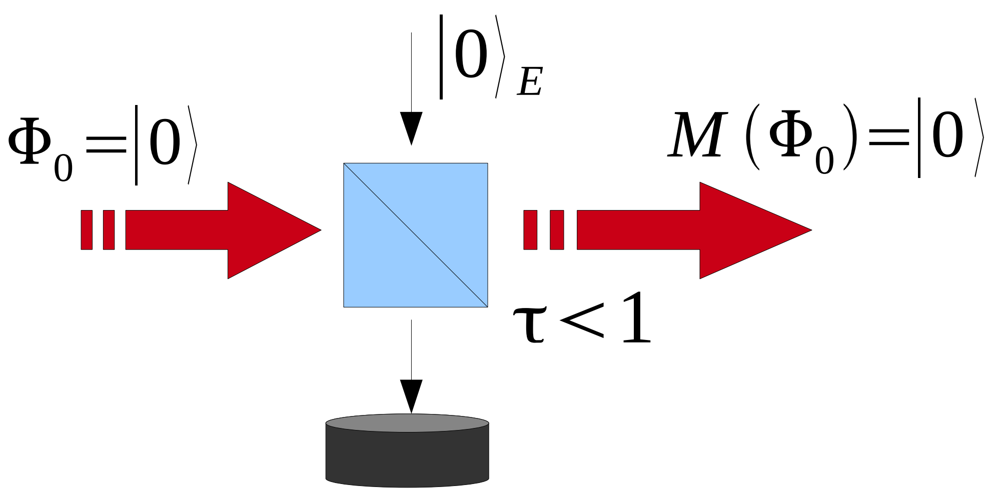
$$\min_{\sigma} S\left(M(\sigma)\right) = S\left(M\left(|0\rangle\langle 0|\right)\right)$$

- The same conjecture is made for the joint channel $M^{\times n}$

$$C(M) \equiv \lim_{n\to\infty} \frac{1}{n} C^{(1)}(M^{\times n}) = C^{(1)}(M)$$ ... cfr. Raul Garcia's talk

- All papers on Gaussian Bosonic channels
  rely on this widely admitted conjecture !!!

- Single exception: <u>pure lossy</u> channel (environment *E* in vacuum state)

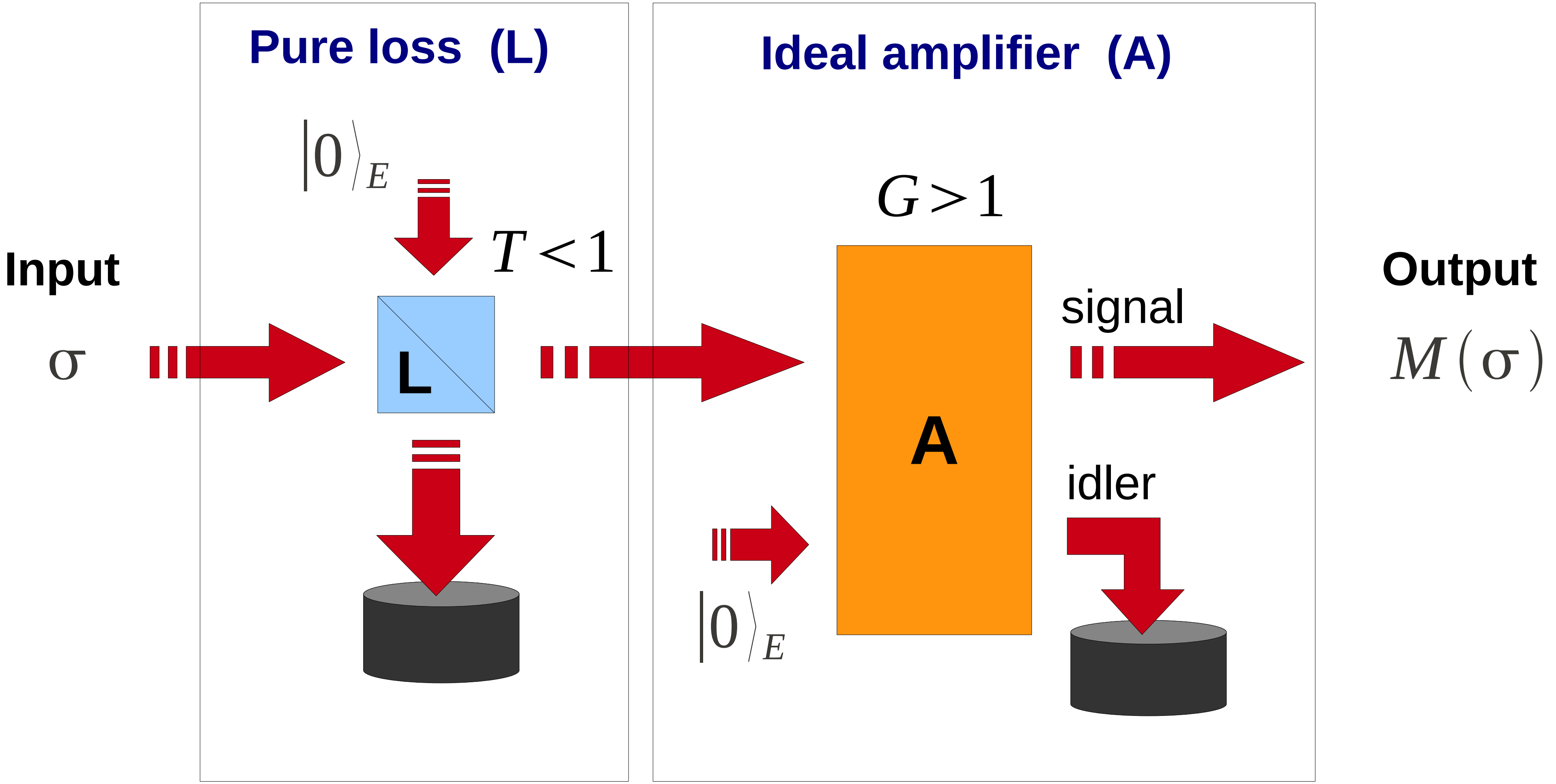


$$C^{(1)}(M) = g[\tau\nu]$$

V. Giovannetti *et al.*, PRL, 2004

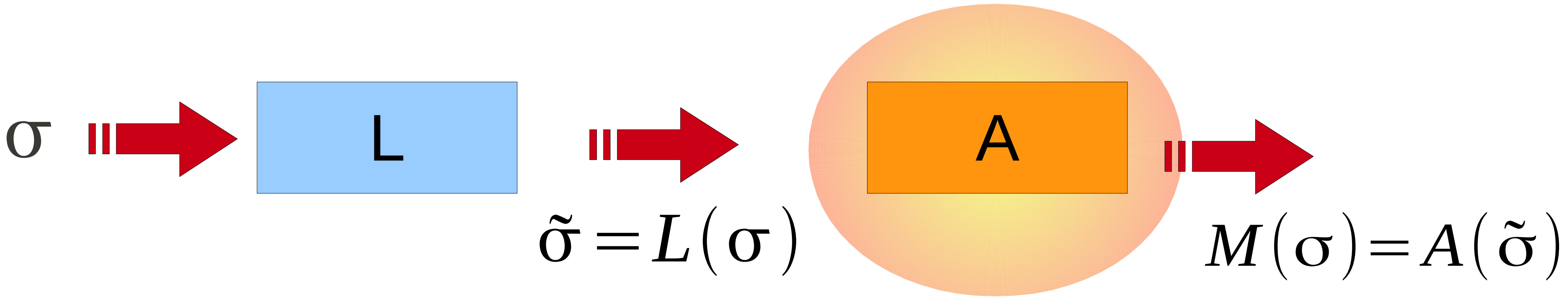
Generic Decomposition of Phase-insensitive Channels

- $\tau = TG < 1$ lossy fiber with thermal noise
- $\tau = TG = 1$ classical Gaussian additive noise
- $\tau = TG > 1$ (non-ideal) noisy amplifier



Reduction of the Conjecture

Conjecture I $$\min_{\sigma} S(M(\sigma)) = S(M(|0\rangle\langle 0|))$$

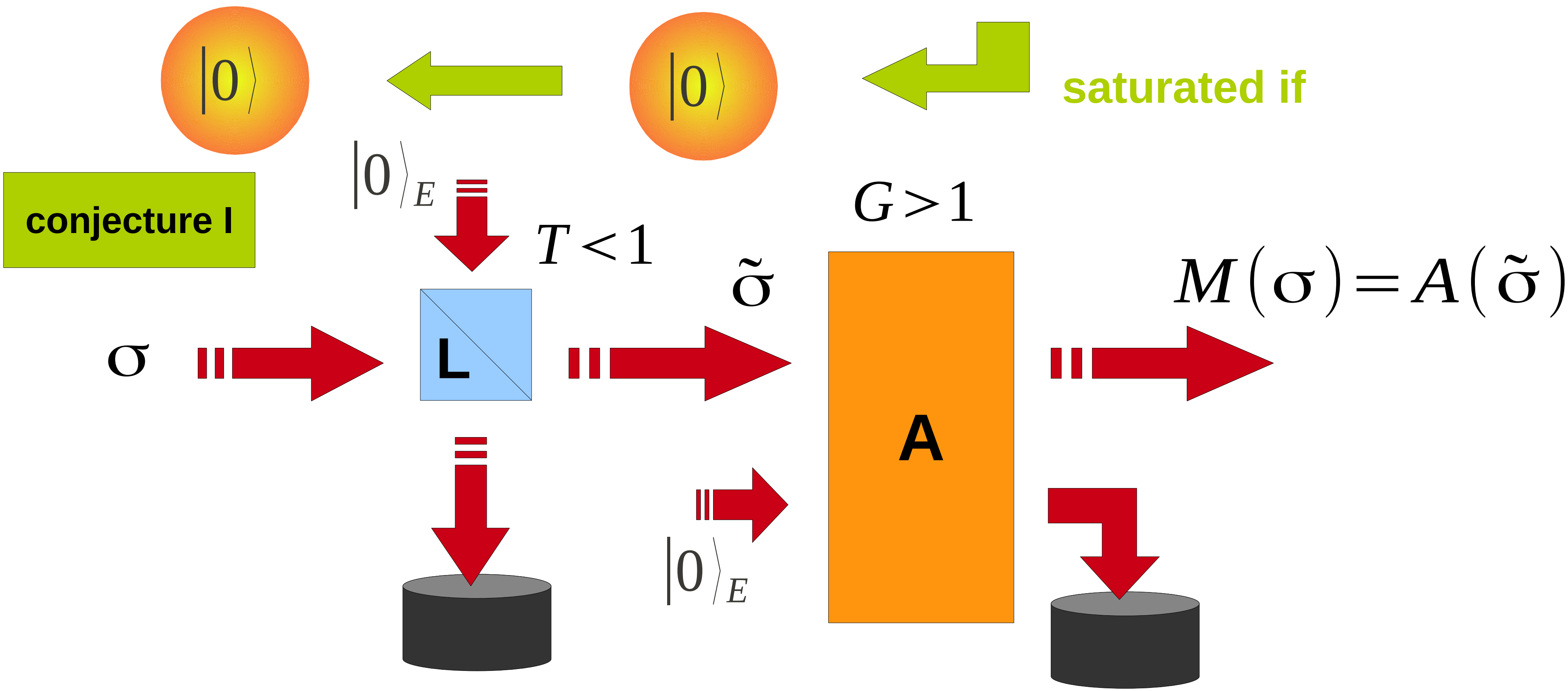


Conjecture II $$\min_{\tilde{\sigma}} S(A(\tilde{\sigma})) = S(A(|0\rangle\langle 0|))$$

Reduction to Ideal Amplifier

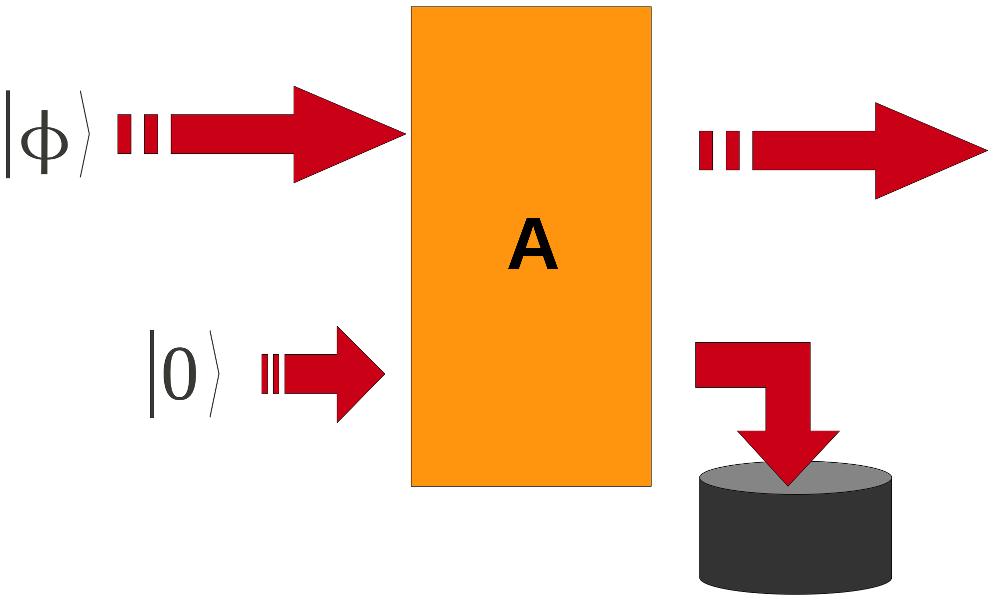
assume conjecture II holds

$$S\left(M(\sigma)\right) = S\left(A(\tilde{\sigma})\right) \geq S\left(A\left(|0\rangle\langle 0|\right)\right)$$



it is (necessary and) <u>sufficient</u> to prove the reduced conjecture II

Link with Output Entanglement of a Two-Mode Squeezer

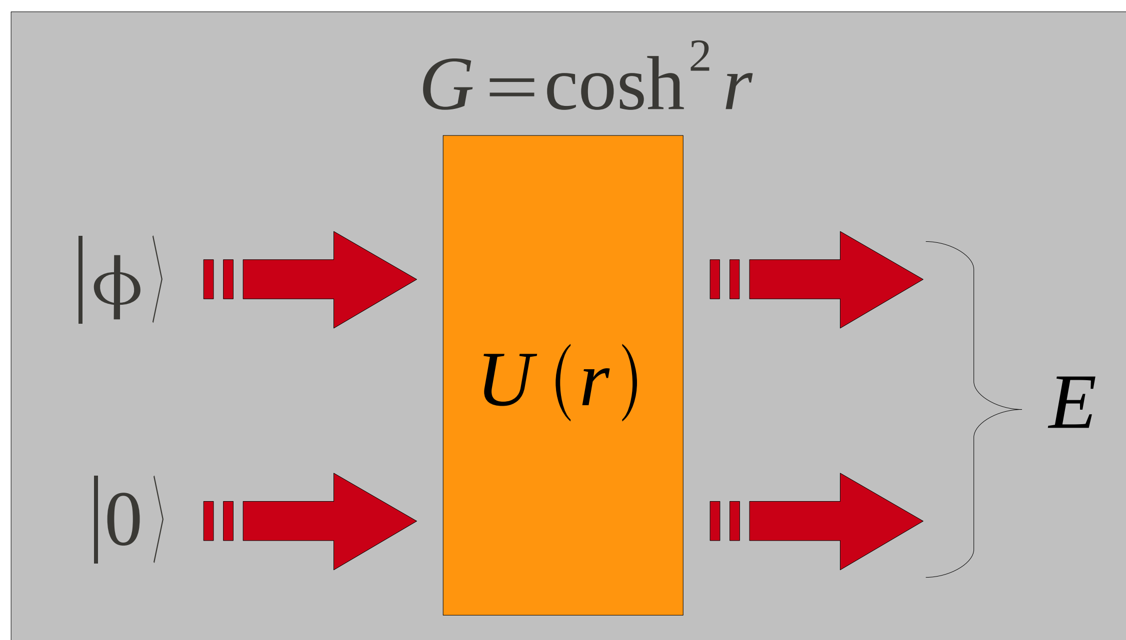


$$S\left(A\left(|\phi\rangle\langle\phi|\right)\right)=E\left(U(r)|\phi\rangle|0\rangle\right)$$

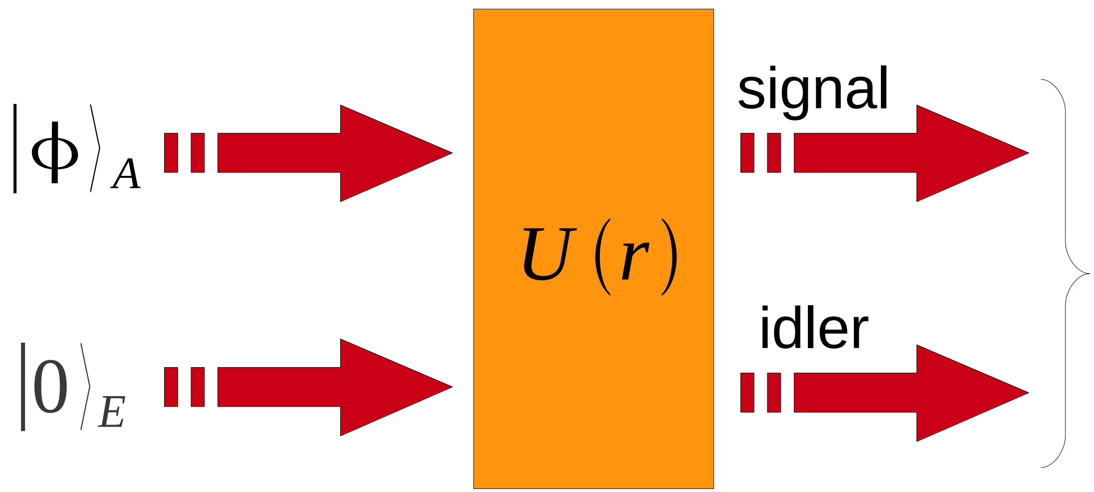
entanglement entropy of a pure state

We are now dealing with the output entanglement of a **two-mode squeezer**

$$U(r)=\exp\left(\frac{r}{2}\left(ab-a^{+}b^{+}\right)\right)$$



Gaussian Minimum Entanglement Conjecture



actual output state :

$$|\Phi\rangle_{AB} = U(r)|\phi\rangle_A|0\rangle_E$$

compare with vacuum input :

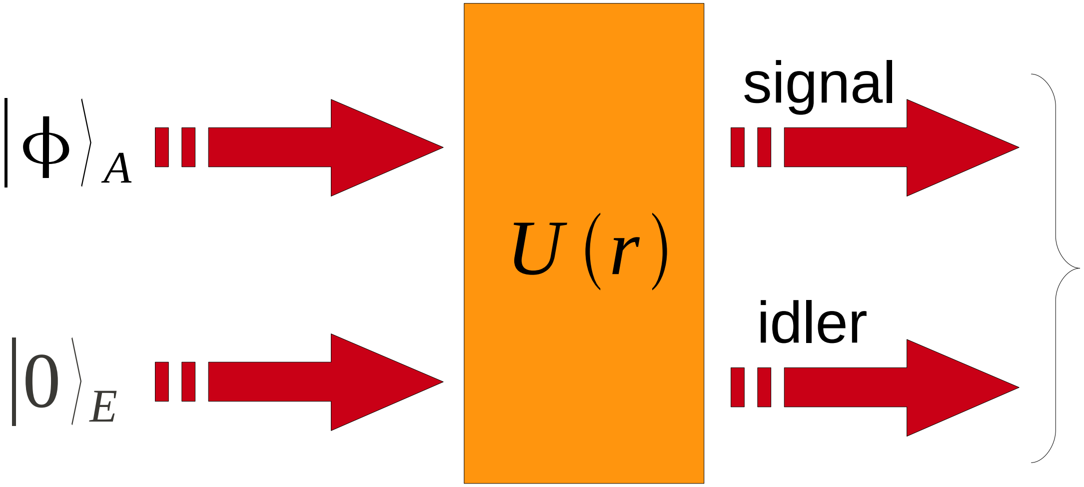
$$|V\rangle_{AB} = U(r)|0\rangle_A|0\rangle_E$$

2-mode vacuum squeezed state
(EPR state)

Conjecture II (bis) $$min_{\phi} E(|\Phi\rangle_{AB}) = E(|V\rangle_{AB})$$

... this is now a conjecture about the entanglement
generated by a 2-mode squeezer !

Proof for Gaussian vs non-Gaussian states



actual output state:

$$|\Phi\rangle_{AB} = U(r)|\phi\rangle_A|0\rangle_E$$

2-mode vacuum squeezed state:

$$|V\rangle_{AB} = U(r)|0\rangle_A|0\rangle_E$$

- easy to prove for **Gaussian** states

$$E\left(|\Phi_{Gauss}\rangle_{AB}\right) \geq E\left(|V\rangle_{AB}\right)$$

- expansion of **non-Gaussian** states in Fock basis

$$|\phi\rangle_A = \sum_k c_k |k\rangle$$

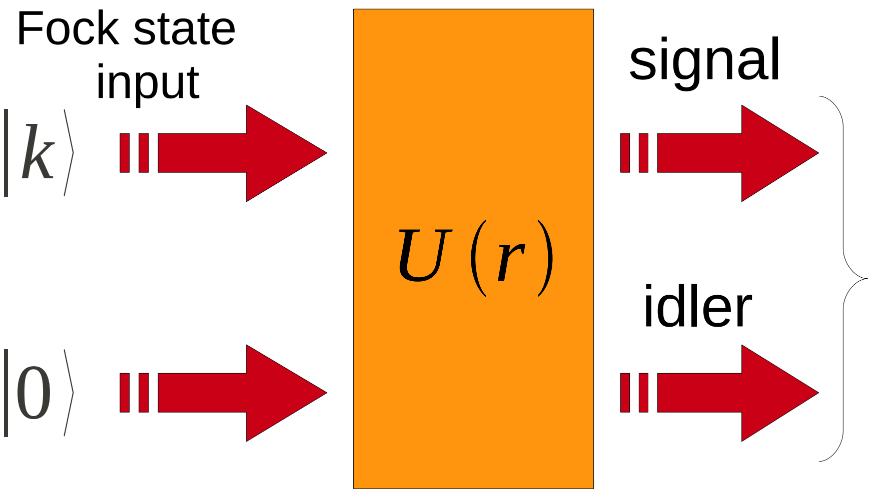
Fock states

... only an incomplete proof for Fock states !

Fock State Inputs

$$E(k) = H\left[P_n(k)\right]$$ Shannon entropy

$$P_n(k) = \frac{1}{\cosh^{2(k+1)} r} \binom{n+k}{n} \tanh^{2n} r$$



$$|\Psi_k\rangle = \sum_{n=0}^{\infty} \sqrt{P_n(k)}\; |n+k\rangle |n\rangle$$

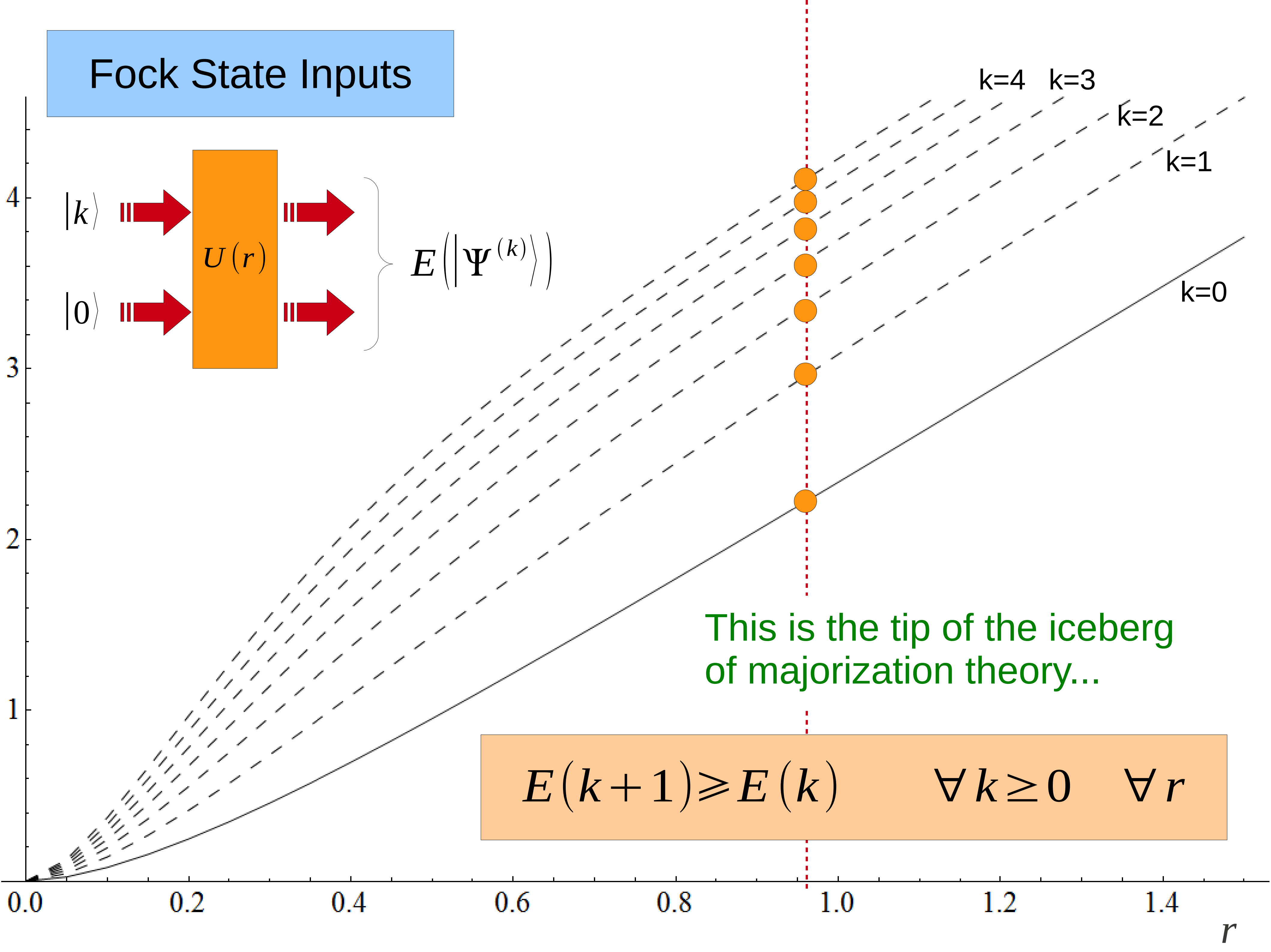
Using Pascal identity $$\binom{n+k+1}{n} = \binom{n+k}{n} + \binom{n+k}{n-1}$$

$$P_n(k+1) = (1-\lambda^2) P_n(k) + \lambda^2 P_{n-1}(k+1)$$ with $\lambda = \tanh r$

Concavity of entropy $$E(k+1) \geqslant (1-\lambda^2) E(k) + \lambda^2 E(k+1)$$

$$E(k+1) \geqslant E(k) \qquad \forall\, k \geq 0$$

vacuum state beats
all other Fock states

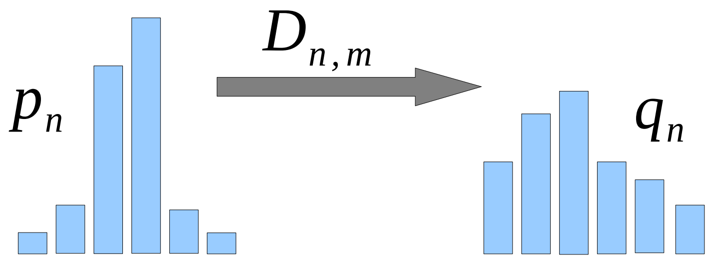


Fock State Inputs
$|k\rangle$
$|0\rangle$
$U(r)$
$E\left(\left|\Psi^{(k)}\right\rangle\right)$
k=4
k=3
k=2
k=1
k=0
1
2
3
4
0.0
0.2
0.4
0.6
0.8
1.0
1.2
1.4
r
This is the tip of the iceberg of majorization theory...
$E(k+1) \geqslant E(k) \quad \forall k \geq 0 \quad \forall r$

Majorization Theory = (partial) order relation for probability distributions

$\xrightarrow{D_{n,m}}$

"p_n majorizes q_n"
$p_n \succ q_n$



with p_n, q_n probability distributions

if and only if

- p_n can be converted to q_n by applying a *random permutation*

  $q_n = \sum_m D_{n,m} p_m$ $\quad D_{n,m}$ is *doubly-stochastic* matrix

or

- $\sum_{n=0}^{m} p_n^{\downarrow} \geq \sum_{n=0}^{m} q_n^{\downarrow} \quad \forall\, m \geq 0$ $\quad$ (p is "*more peaked*" than q)

or

- $\sum_n h(p_n) \leq \sum_n h(q_n) \quad \forall\, h(x)$ concave function

  e.g. entropy: $h(x) = -x \log(x)$

  $\Rightarrow$ $H(p_n) \leq H(q_n)$ $\quad$ entropy can only <u>increase</u>

Quantum application : Interconversion of pure bipartite states

M. Nielsen, G. Vidal, 2000

$D_{n,m}$ →

p_n majorizes q_n

p_n, q_n probability distributions

LOCC ←

$|\psi\rangle$ majorizes $|\phi\rangle$

$$|\psi\rangle = \sum_n \sqrt{p_n}\,|e_n\rangle\,|f_n\rangle \qquad |\phi\rangle = \sum_n \sqrt{q_n}\,|e_n'\rangle\,|f_n'\rangle$$

with p_n majorizing q_n

- $|\phi\rangle$ can be converted to $|\psi\rangle$ by applying a *deterministic LOCC*
- $E(|\psi\rangle) \leq E(|\phi\rangle)$ entanglement can only decrease

Trick: $\rho_A = tr_B(|\psi\rangle\langle\psi|) = \sum_n p_n \underbrace{|e_n\rangle\langle e_n|}_{\text{orthonormal}}$ eigenbasis representation

$= \sum_n q_n \underbrace{|\zeta_n\rangle\langle\zeta_n|}_{\text{not orthonormal}}$ … possible if p_n majorizes q_n

Explicit conversion LOCC

LOCC ←

$|\psi\rangle$ majorizes $|\phi\rangle$

$$|\psi\rangle = \sum_n \sqrt{p_n}\, |e_n\rangle\, |f_n\rangle$$

$$|\psi\rangle = \sum_n \sqrt{q_n}\, |\zeta_n\rangle\, |f_n{''}\rangle$$ above trick (provided p_n majorizes q_n)

LOCC ↑ ↕ U

$$|\phi\rangle = \sum_n \sqrt{q_n}\, |e_n{'}\rangle\, |f_n{'}\rangle$$

POVM: $A_m = \sum_n \omega^{nm} |\zeta_n\rangle\langle e_n{'}|$ with $\omega = e^{i2\pi/d}$ and $\sum_m A_m^+ A_m = I$

$$(A_m \times I)\, |\phi\rangle = \sum_n \sqrt{q_n}\, \omega^{nm}\, |\zeta_n\rangle\, |f_n{'}\rangle \equiv |\phi_m\rangle$$ depends on outcome m

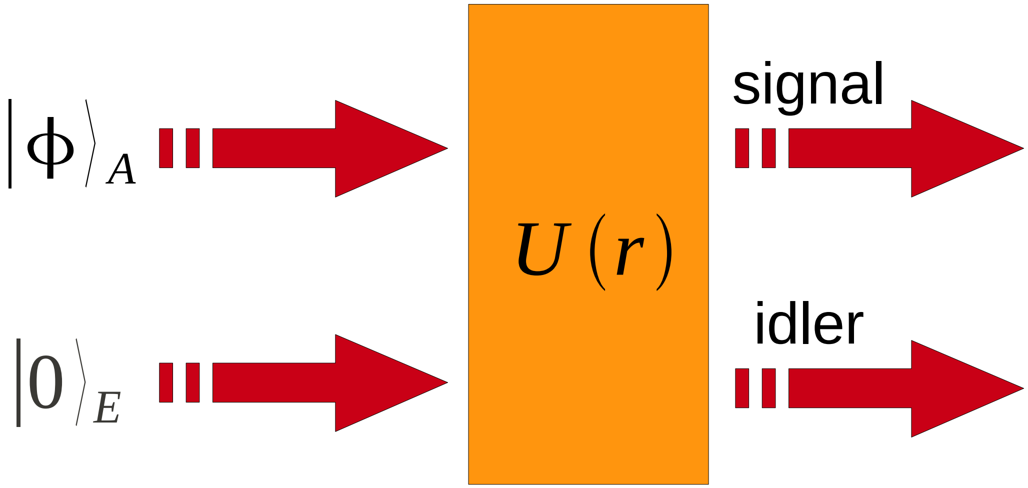
Conditional U: $B_m = \sum_n \omega^{-nm} |f_n{''}\rangle\langle f_n{'}|$ conditional on m

$$(I \times B_m)\, |\phi_m\rangle = \sum_n \sqrt{q_n}\, |\zeta_n\rangle\, |f_n{''}\rangle \equiv |\psi\rangle$$

Gaussian Majorization Conjecture

For a given 2-mode squeezer (Bogoliubov transformation),

the 2-mode vacuum squeezed state **majorizes** all other output states !!!



actual output state:

$$|\Phi\rangle_{AB} = U(r)|\phi\rangle_A |0\rangle_E$$

2-mode vacuum squeezed state:

$$|V\rangle_{AB} = U(r)|0\rangle_A |0\rangle_E$$

Conjecture III $|V\rangle_{AB}$ majorizes $|\Phi\rangle_{AB}$ $\forall \; |\phi\rangle_A$

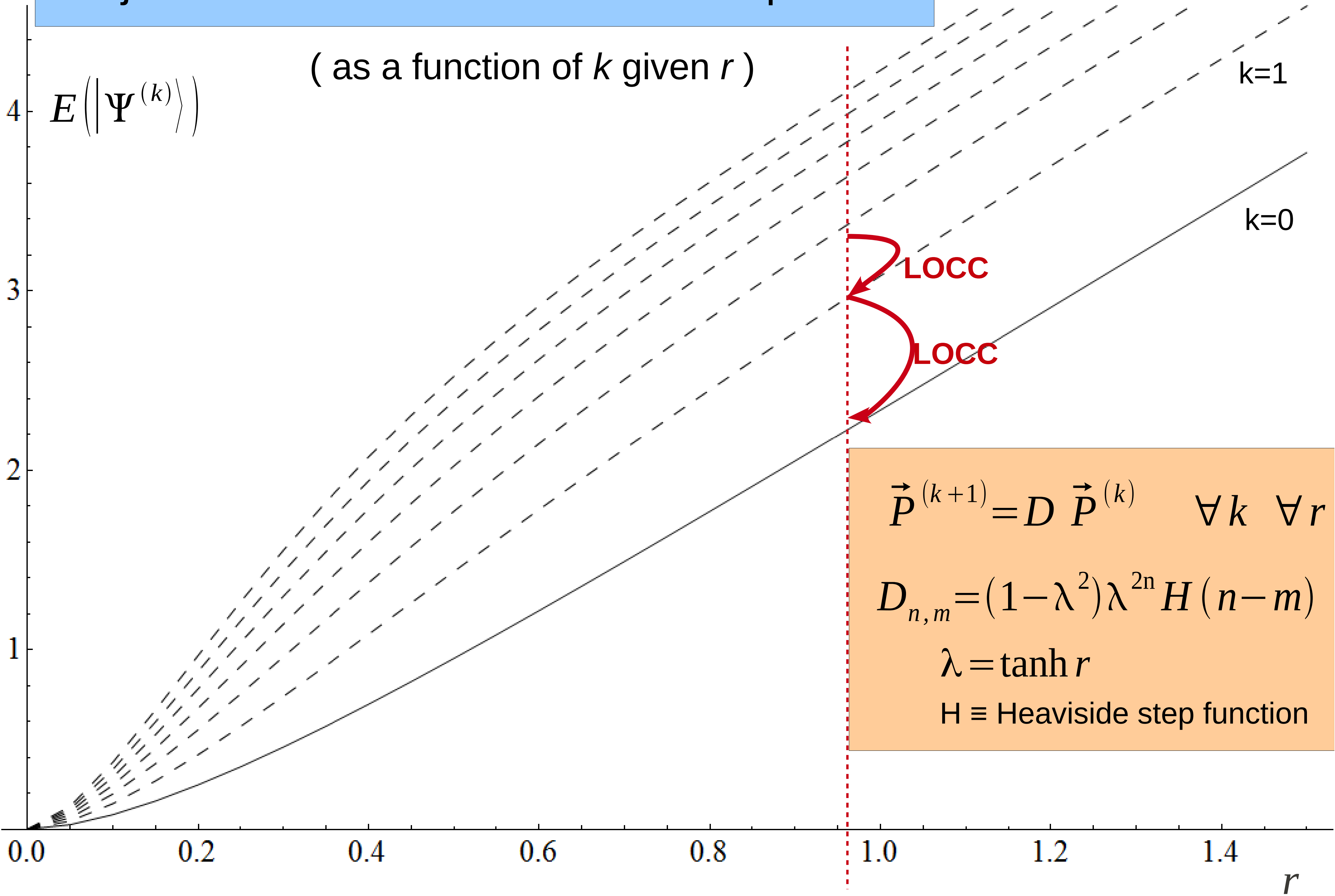
$$|V\rangle_{AB} \xleftarrow{\text{LOCC}} |\Phi\rangle_{AB} \quad \text{implying} \quad E(|V\rangle_{AB}) \le E(|\Phi\rangle_{AB})$$

... stronger than minimum entropy/entanglement conjecture

... but perhaps easier to prove (?)

Majorization relations in a 2-mode squeezer

(as a function of k given r)



$$\vec{P}^{(k+1)} = D\,\vec{P}^{(k)} \qquad \forall k \quad \forall r$$

$$D_{n,m} = (1-\lambda^2)\lambda^{2n} H(n-m)$$

$$\lambda = \tanh r$$

H ≡ Heaviside step function

Explicit LOCC

$$|\Psi_k\rangle = \sum_{n=0}^{\infty} \sqrt{p_n(k)}\ |n+k\rangle|n\rangle$$

$$\Uparrow$$

$$|\Psi_{k+1}\rangle = \sum_{n=0}^{\infty} \sqrt{p_n(k+1)}\ |n+k+1\rangle|n\rangle$$

Alice applies a POVM

$$\begin{cases} A_{YES} = \sum_{m=0}^{\infty} \sqrt{\dfrac{(1-\lambda^2)\, p_m(k)}{p_m(k+1)}}\ |m+k\rangle\langle m+k+1| \\ A_{NO} = \sum_{m=0}^{\infty} \sqrt{\dfrac{\lambda^2\, p_{m-1}(k+1)}{p_m(k+1)}}\ |m+k\rangle\langle m+k+1| \end{cases}$$

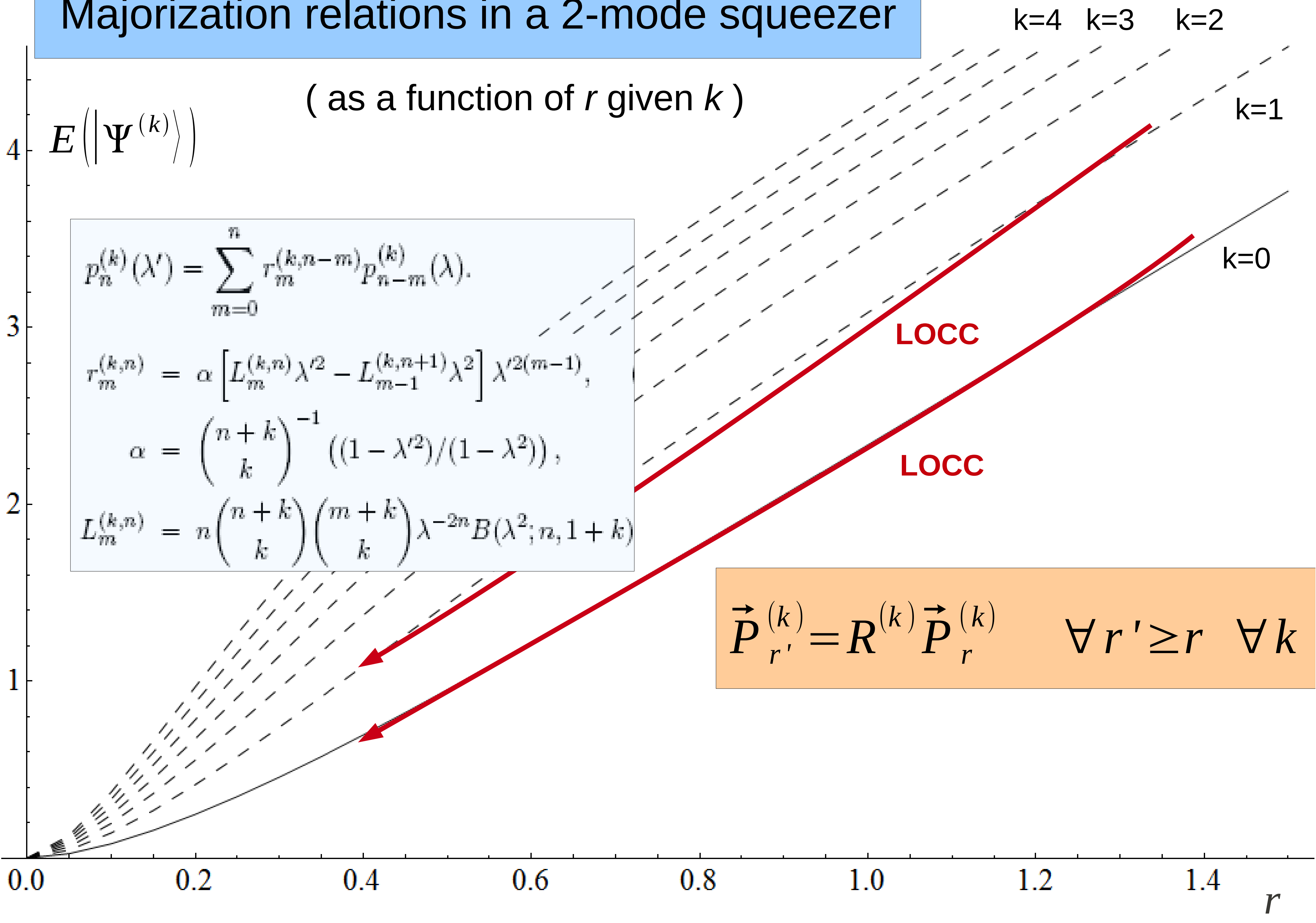
$$(A_{YES}\times 1)\,|\Psi_{k+1}\rangle = \sqrt{(1-\lambda^2)}\ \sum_{n=0}^{\infty} \sqrt{p_n(k)}\ |n+k\rangle|n\rangle = \sqrt{(1-\lambda^2)}\ |\Psi_k\rangle \quad \text{YES}$$

$$(A_{NO}\times 1)\,|\Psi_{k+1}\rangle = \sqrt{\lambda^2}\ \sum_{n=0}^{\infty} \sqrt{p_n(k+1)}\ |n+k+1\rangle|n+1\rangle \rightarrow \sqrt{\lambda^2}\ |\Psi_{k+1}\rangle \quad \text{NO}$$

If “NO” she communicates it to Bob who applies $U = \sum_{m=0}^{\infty} |m\rangle\langle m+1|$
and then they start a new round again

Majorization relations in a 2-mode squeezer

(as a function of *r* given *k*)



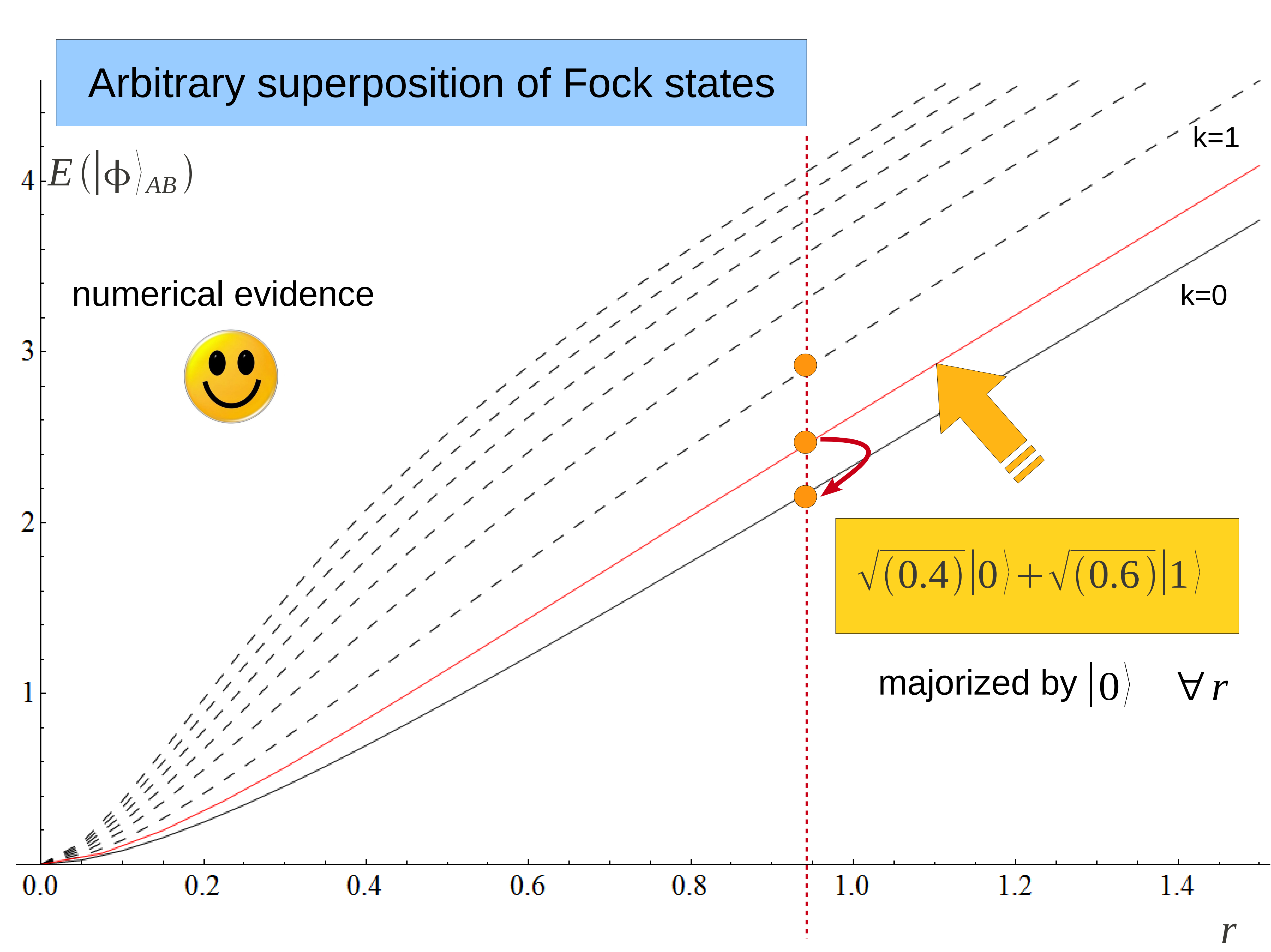
$$p_n^{(k)}(\lambda') = \sum_{m=0}^{n} r_m^{(k,n-m)} p_{n-m}^{(k)}(\lambda).$$

$$r_m^{(k,n)} = \alpha \left[L_m^{(k,n)}\lambda'^2 - L_{m-1}^{(k,n+1)}\lambda^2\right]\lambda'^{2(m-1)},$$

$$\alpha = \binom{n+k}{k}^{-1}\left((1-\lambda'^2)/(1-\lambda^2)\right),$$

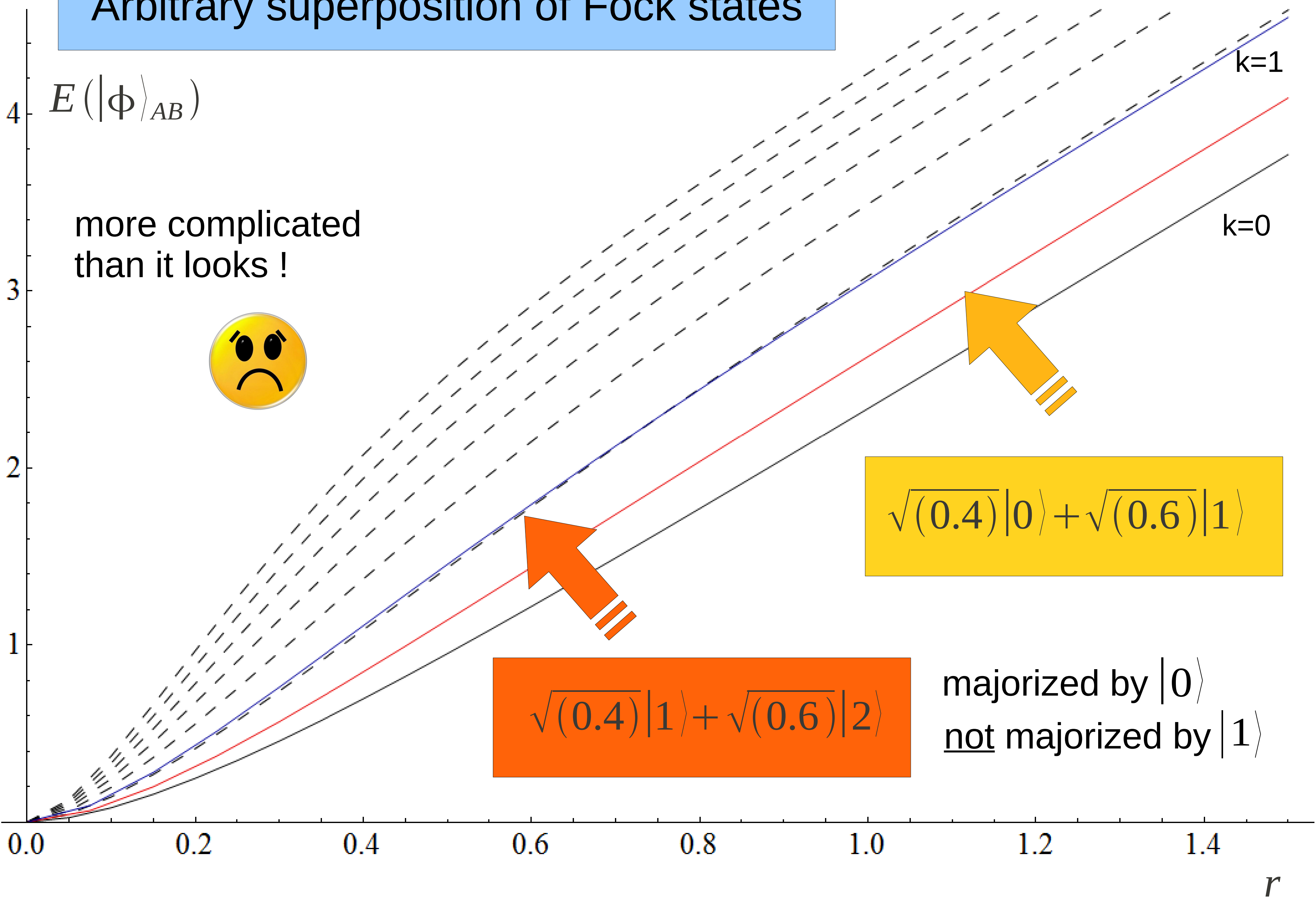
$$L_m^{(k,n)} = n\binom{n+k}{k}\binom{m+k}{k}\lambda^{-2n}B(\lambda^2;n,1+k)$$

$$\vec{P}_{r'}^{(k)} = R^{(k)}\vec{P}_r^{(k)} \qquad \forall r' \geq r \quad \forall k$$



Arbitrary superposition of Fock states
$E(|\phi\rangle_{AB})$
numerical evidence
k=1
k=0
$\sqrt{(0.4)}|0\rangle+\sqrt{(0.6)}|1\rangle$
majorized by $|0\rangle$ $\forall r$
0.0
0.2
0.4
0.6
0.8
1.0
1.2
1.4
r
1
2
3
4

Arbitrary superposition of Fock states



This is not just an abstract mathematical problem !

(even if you don't care at all about quantum bosonic channels !)

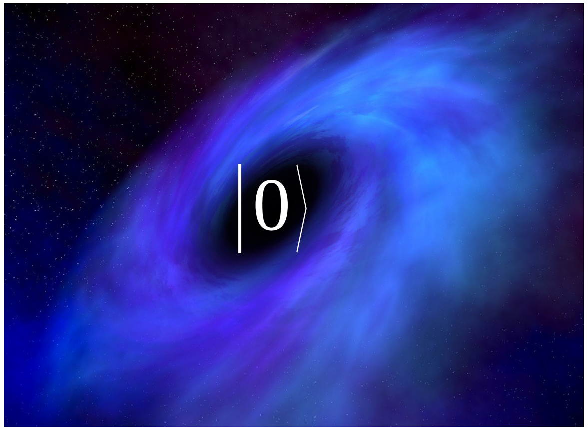
Bogoliubov transformation $\hat{a}_i{}' = \sum_j \left(u_{ij} \hat{a}_j + v_{ij} \hat{a}_j^+ \right)$ is everywhere,

e.g., quantum optics, supraconductivity, Hawking radiation, Unruh effect, ...

this **Gaussian conjecture** may have deeper physical implications !

FUNDAMENTAL STATEMENT :

"Nothing is less random than vacuum"



Very plausible but not (yet) proven...
How can we (dis)prove this statement ?

Take-home message

“ Nothing is less random than vacuum ?”

New approach to solve the “Minimum Output Entropy Conjecture” for Gaussian Bosonic channels

- Reduction to ideal amplifier channel
- Output entanglement of a two-mode squeezer
- Link with majorization theory (proof for Fock states only)
- Missing piece: absence of rotational “symmetry breaking”

Numerical analysis for random input states strongly suggests that (majorization) Gaussian conjecture holds...

Ref.: R. Garcia-Patron, C. Navarrete-Benlloch, S. Lloyd, J. H. Shapiro & N. J. Cerf, PRL 108, 110505 (2012).