Fully Quantum Arbitrarily Varying Channels: Random Coding & Dichotomy

H. Boche, C. Deppe, J. Nötzel, A. Winter
(ICREA & Universitat Autònoma de Barcelona)

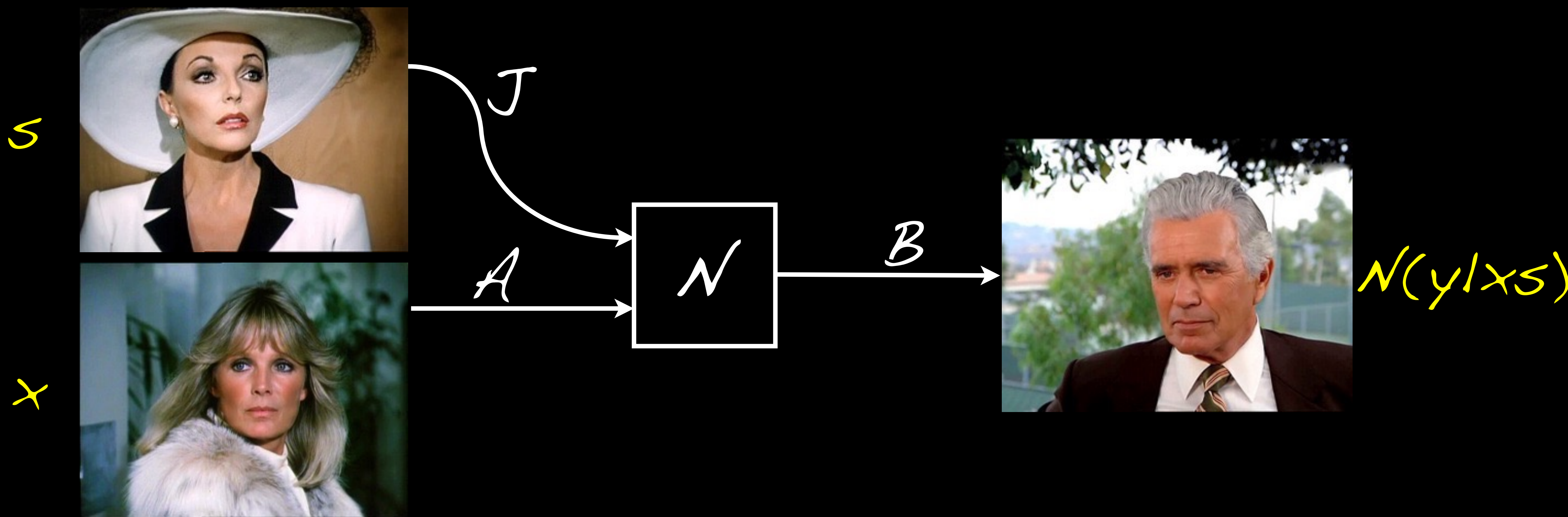
= arXiv[quant-ph]:1801.04572 =

Outline

1. Quantum jammer channels: compound, AVC
2. Capacities: C and Q
3. Reducing arbitrarily varying to compound
4. Elimination of correlation: dichotomy
5. Reflections and conclusions

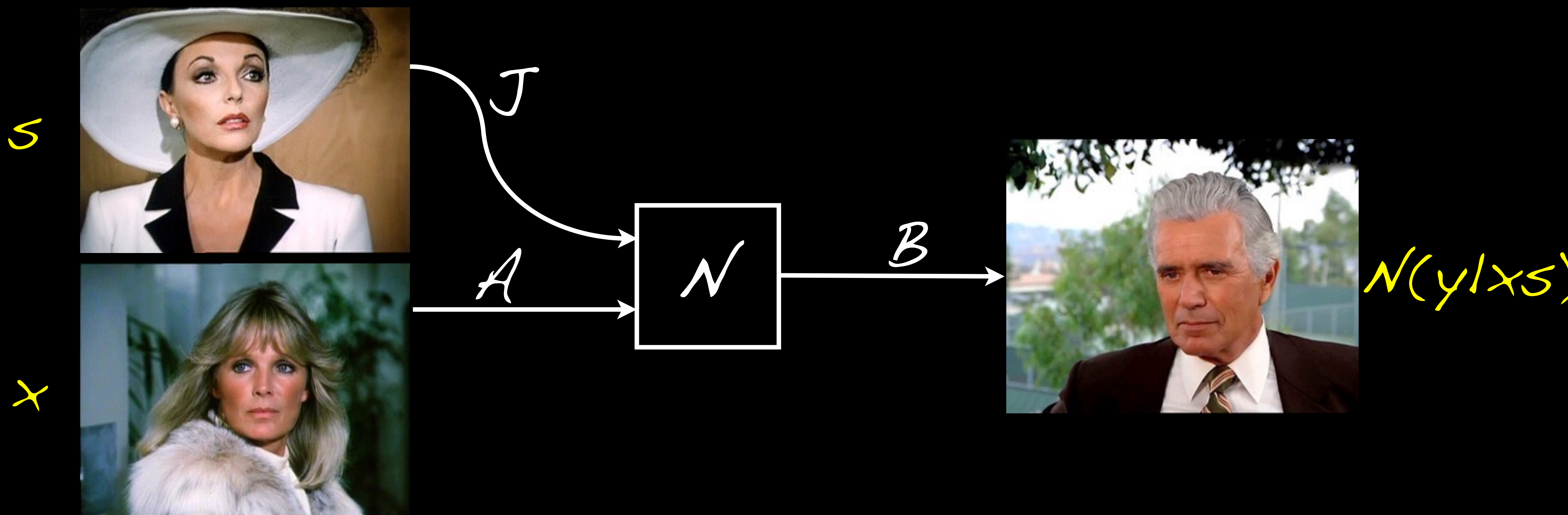
1. Jammer channels

The classical jammer is basically a multiple access channel, but with one sender (A) cooperating with the receiver (B), and the other sender (J) acting adversarially.



1. Jammer channels

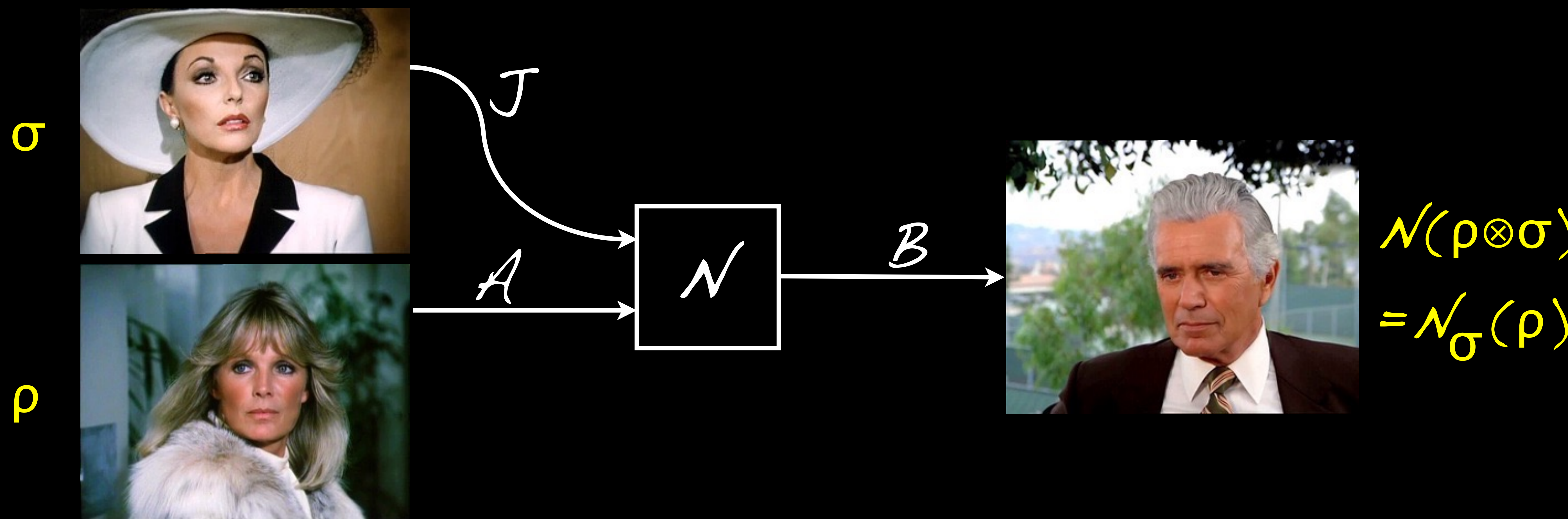
The classical jammer is basically a multiple access channel, but with one sender (A) cooperating with the receiver (B), and the other sender (J) acting adversarially.



ℓ channel uses = product; jammer: $s_1 s_2 \ldots s_\ell$

1. Quantum jammer channels

Generalise it to a quantum channel $\mathcal{N}$, i.e. cptp (completely positive, trace preserving) linear map; maps states on $A \otimes J$ to states on B:

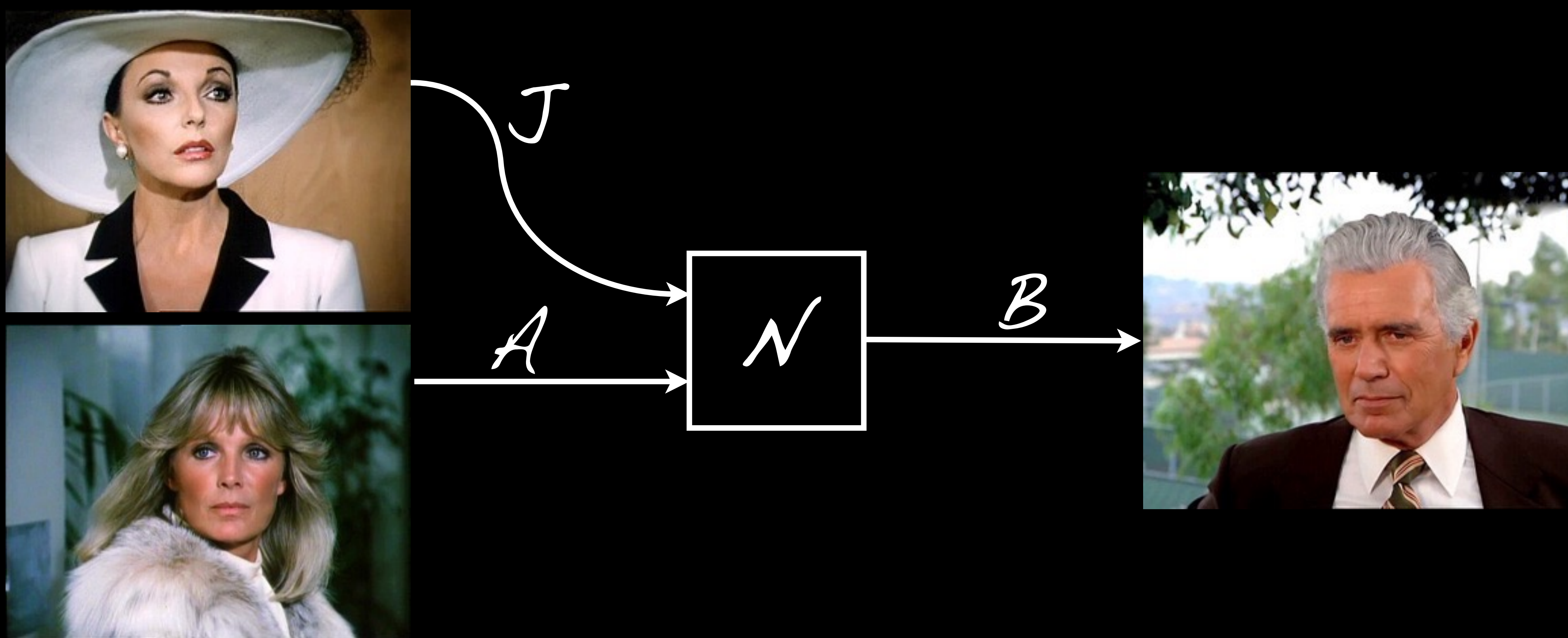


1. Quantum jammer channels

Generalise it to a quantum channel $\mathcal{N}$, i.e. cptp (completely positive, trace preserving) linear map; maps states on $A\otimes J$ to states on B:

σ

ρ



$\mathcal{N}(\rho\otimes\sigma)$
$=\mathcal{N}_\sigma(\rho)$

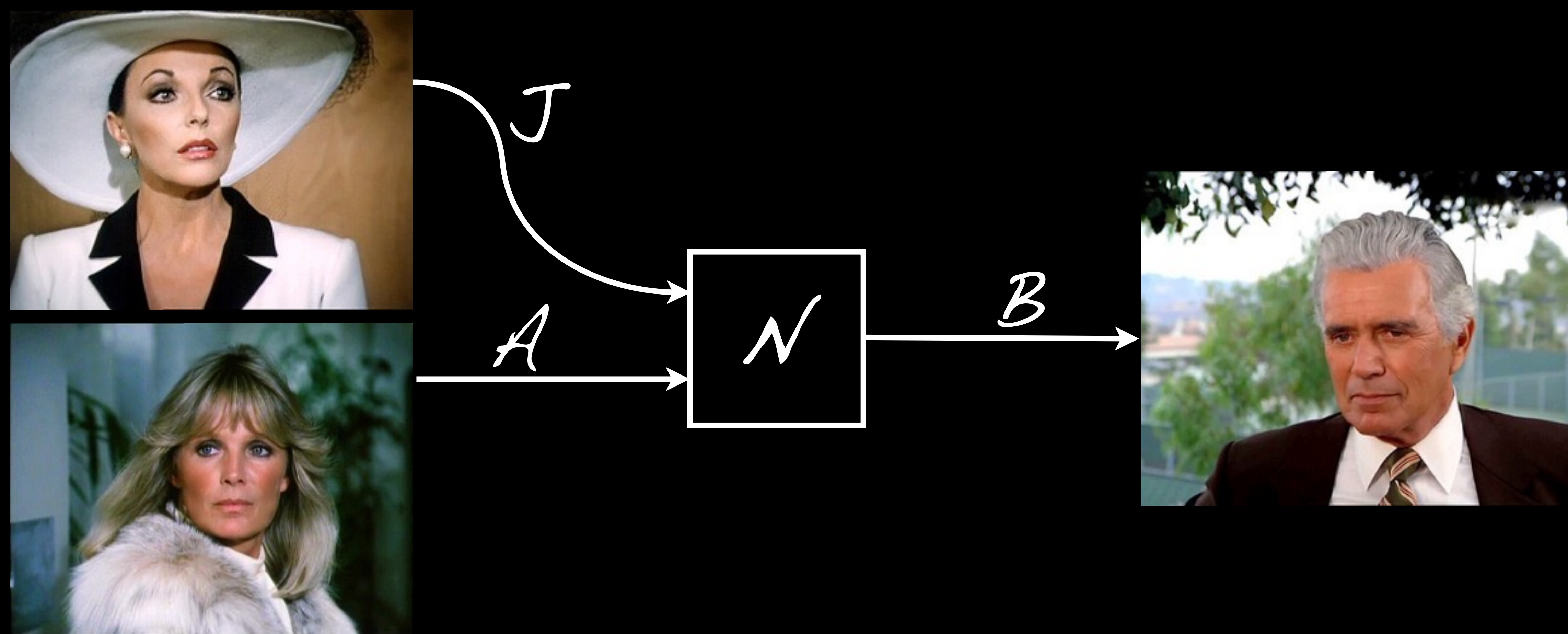
ℓ channel uses = tensor product $\mathcal{N}^{\otimes\ell}$;

1. Quantum jammer channels

Generalise it to a quantum channel $\mathcal{N}$, i.e. cptp (completely positive, trace preserving) linear map; maps states on $A\otimes J$ to states on B:

σ

ρ



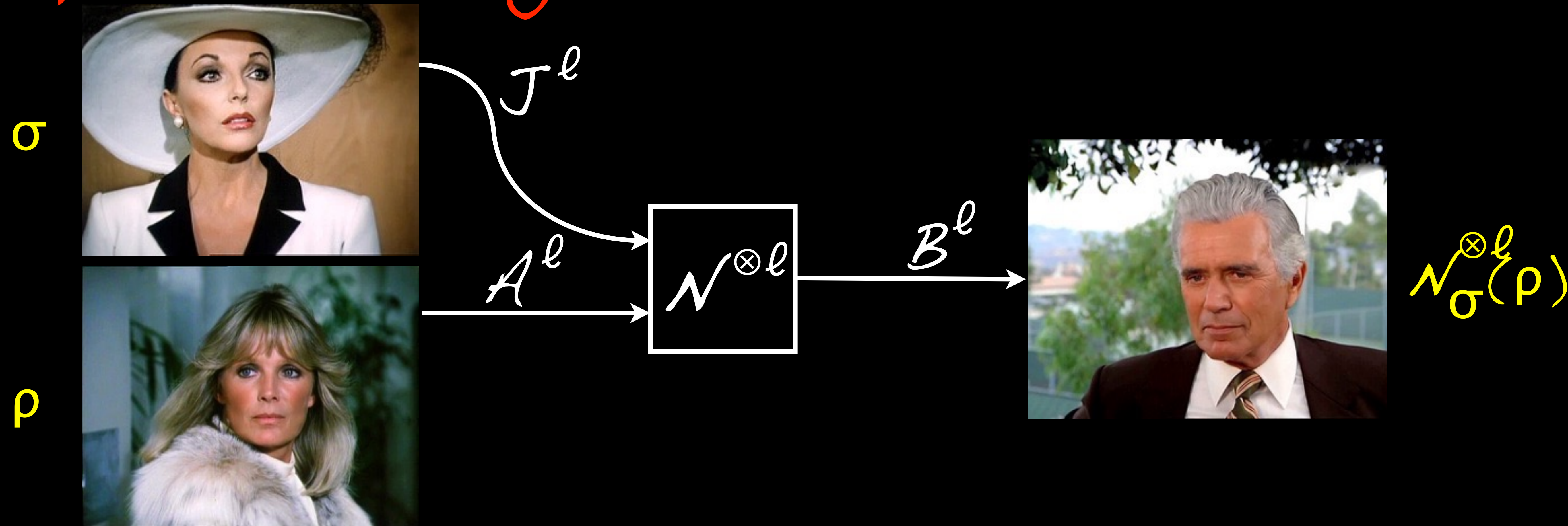
$\mathcal{N}(\rho\otimes\sigma)$
$=\mathcal{N}_\sigma(\rho)$

ℓ channel uses = tensor product $\mathcal{N}^{\otimes\ell}$; however, jammer is not restricted to product states!

Quantum info primer:

* Systems described by (complex) Hilbert spaces $A, B, J, \ldots$, usually of finite dimension $|A|$, etc;
* States are density matrices $\rho \geq 0$, $\mathrm{Tr}\,\rho = 1$ (for diagonal matrices recover probability distributions); state space $S(A)$, etc;
* von Neumann entropy $S(\rho) = -\mathrm{Tr}\,\rho \log \rho$, i.e. the Shannon entropy of the spectrum;
* State transformations are completely positive, trace preserving linear (cptp) maps acting on density matrices – quantum channels;
* Composition of systems by tensor product.

1. Quantum jammer channels



ℓ channel uses = tensor product $\mathcal{N}^{\otimes\ell}$; however, jammer is not restricted to product states!

Arbitrary jammer states σ: QAVC

– correlated noise

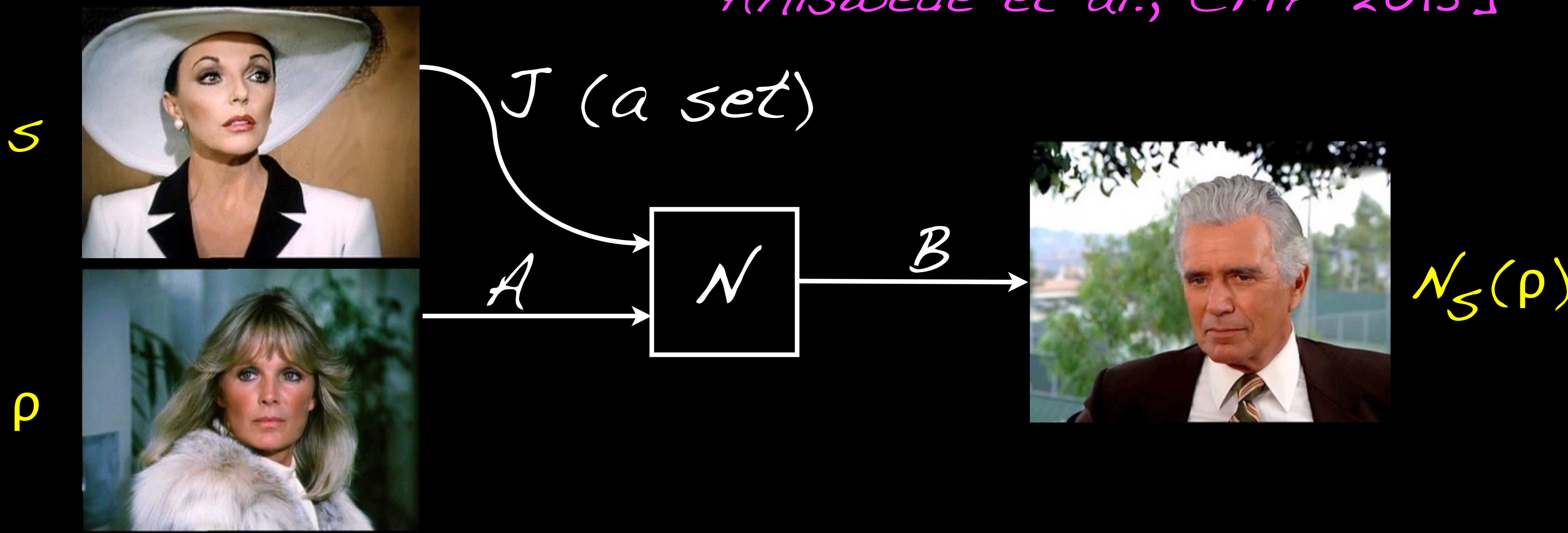
Tensor power states $\sigma^{\otimes\ell}$: compound channel

– effective channels all i.i.d.

1. Quantum jammer channels

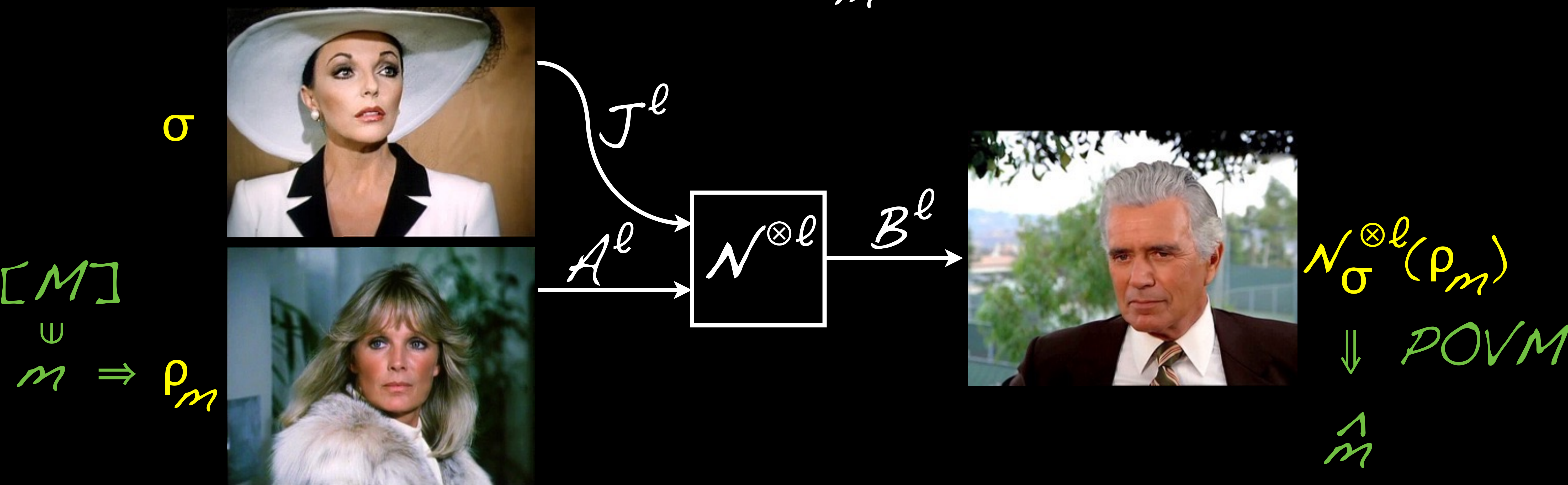
Previously considered models were hybrids: link from A is modelled quantumly, but jammer has a discrete state set (s).

[Ahlswede/Blinovsky, IEEE-IT 2007;
Ahlswede et al., CMP 2013]



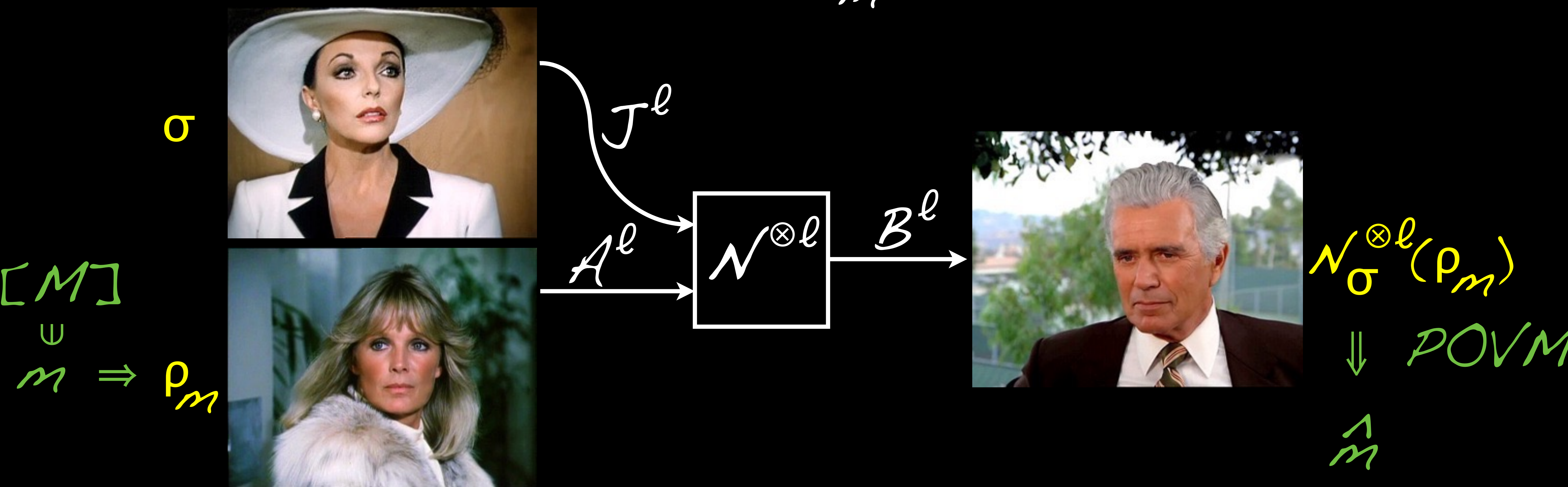
2. Capacities: C & Q

Classical transm. code $\mathcal{C} = \{(\rho_m, D_m) : m \in [M]\}$, where $\rho_m \in \mathcal{S}(J^\ell)$ are signal states and the $D_m \geq 0$ form a POVM: $\sum_m D_m = I$



2. Capacities: C & Q

Classical transm. code $C = \{(\rho_m, D_m) : m \in [M]\}$, where $\rho_m \in S(J^\ell)$ are signal states and the $D_m \geq 0$ form a POVM: $\sum_m D_m = I$



$$P_{err}(C,\sigma) = Pr\{m \neq \hat{m}\} = 1 - \frac{1}{M} \sum_m Tr\, (\mathcal{N}^{\otimes \ell}(\rho_m \otimes \sigma)) D_m$$

2. Capacities: C & Q

Classical transm. code $\mathcal{C}=\{(\rho_m, \mathcal{D}_m):m\in[M]\}$, where $\rho_m \in \mathcal{S}(J^\ell)$ are signal states and the $\mathcal{D}_m \geq 0$ form a POVM: $\sum_m \mathcal{D}_m = I$

$$P_{err}(\mathcal{C},\sigma) = \Pr\{m\neq\hat{m}\} = 1 - \frac{1}{M}\sum_m \mathrm{Tr}\,(\mathcal{N}^{\otimes\ell}(\rho_m\otimes\sigma))\mathcal{D}_m$$

We call $\mathcal{C}$ an (ℓ,ε)-compound code if for all $\sigma \in \mathcal{S}(J)$, $P_{err}(\mathcal{C},\sigma^{\otimes\ell}) \leq \varepsilon$;

2. Capacities: C & Q

Classical transm. code $\mathcal{C}=\{(\rho_m,D_m):m\in[M]\}$, where $\rho_m \in \mathcal{S}(J^\ell)$ are signal states and the $D_m \geq 0$ form a POVM: $\sum_m D_m = I$

$$P_{err}(\mathcal{C},\sigma) = \Pr\{m\neq\hat{m}\} = 1 - \frac{1}{M}\sum_m \mathrm{Tr}\,(\mathcal{N}^{\otimes\ell}(\rho_m\otimes\sigma))D_m$$

We call $\mathcal{C}$ an (ℓ,ε)-compound code if for all $\sigma\in\mathcal{S}(J)$, $P_{err}(\mathcal{C},\sigma^{\otimes\ell})\leq\varepsilon$;

$\mathcal{C}$ is an (ℓ,ε)-code (or QAVC code) if for all $\sigma\in\mathcal{S}(J^{\otimes\ell})$, $P_{err}(\mathcal{C},\sigma)\leq\varepsilon$ (more stringent)

2. Capacities: C & Q

We regard these codes as deterministic, but note that the encoder in a certain sense is stochastic; no analogue of the classical distinction det.-vs-stoch. encoder.

In contrast, a random code is a family of codes (C_λ), where λ is a random variable, shared between sender and receiver.

2. Capacities: C & Q

We regard these codes as deterministic, but note that the encoder in a certain sense is stochastic; no analogue of the classical distinction det.-vs-stoch. encoder.

In contrast, a random code is a family of codes (C_λ), where λ is a random variable, shared between sender and receiver.

We call C a random (ℓ,ε)-code if for all $\sigma \in S(J^{\otimes \ell})$, $\mathbb{E}_\lambda P_{err}(C_\lambda,\sigma) \leq \varepsilon$.

2. Capacities: C & Q

Leads to three potentially different capacities (maximum rate for $\ell \to \infty$, while $\varepsilon \to 0$): $C_{det}(\mathcal{N}) \leq C_{rand}(\mathcal{N}) \leq C(\{\mathcal{N}_\sigma\})$

deterministic QAVC capacity

random QAVC capacity

compound capacity (equal det./random)

2. Capacities: C & Q

Leads to three potentially different capacities (maximum rate for $\ell \to \infty$, while $\varepsilon \to 0$): $C_{det}(\mathcal{N}) \leq C_{rand}(\mathcal{N}) \leq C(\{\mathcal{N}_\sigma\})$

deterministic QAVC capacity

random QAVC capacity

compound capacity (equal det./random)

What is the status of the inequality signs?

2. Capacities: C & Q

The compound capacity $C(\{N_\sigma\})$ is the easiest to characterise:

$$C(\{N_\sigma\}) = \sup_{\ell} \frac{1}{\ell} \max_{\{p_x, \rho_x\}} \min_{\sigma} I(X:B^\ell),$$

where the max is over all ensembles of input states $\rho_x \in S(A^\ell)$, and the min is over all jammer states $\sigma \in S(J)$;

[Bjelaković et al., CMP 2009; Mosonyi, IEEE-IT 2015]

2. Capacities: C & Q

The compound capacity $C(\{N_\sigma\})$ is the easiest to characterise:

$$C(\{N_\sigma\}) = \sup_\ell \frac{1}{\ell} \max_{\{p_x,\rho_x\}} \min_\sigma I(X:B^\ell),$$

where the max is over all ensembles of input states $\rho_x \in S(A^\ell)$, and the min is over all jammer states $\sigma \in S(J)$;

$I(X:B^\ell) = S(\sum p_x \omega_x) - \sum p_x S(\omega_x)$ is the Holevo information of the ensemble of states $\omega_x = N^{\otimes \ell}(\rho_x \otimes \sigma^{\otimes \ell}) = (N_\sigma)^{\otimes \ell}(\rho_x) \in S(B^\ell)$

[Bjelaković et al., CMP 2009; Mosonyi, IEEE-IT 2015]

Main results (spoilers!):

$$C_{det}(\mathcal{N}) \leq C_{rand}(\mathcal{N}) \leq C(\{\mathcal{N}_\sigma\})$$

Main results (spoilers!):

$$C_{det}(\mathcal{N}) \leq C_{rand}(\mathcal{N}) = C(\{\mathcal{N}_\sigma\})$$

Result 1: always =
(OK, that was known
before, but we show
how from any decent
compound code to
build a random code)

Main results (spoilers!):

$$C_{det}(\mathcal{N}) \text{ `=' } C_{rand}(\mathcal{N}) = C(\{\mathcal{N}_\sigma\})$$

Result 2: always =, unless $C_{det}(\mathcal{N}) = 0$ (This is a quantum version of Ahlswede's capacity dichotomy)

Result 1: always = (OK, that was known before, but we show how from any decent compound code to build a random code)

Works the same for quantum capacity Q (high-fidelity transm. of qubits):

$$Q_{det}(\mathcal{N}) \text{ `='} \; Q_{rand}(\mathcal{N}) = Q(\{\mathcal{N}_\sigma\})$$

Result 2: always $=$, unless $C_{det}(\mathcal{N}) = 0$ (This is a quantum version of Ahlswede's capacity dichotomy)

Result 1: always $=$ (OK, that was known before, but we show how from any decent compound code to build a random code)

3. Compound to QAVC codes

To prove $C_{rand}(\mathcal{N}) = C(\{\mathcal{N}_\sigma\})$, we use any (ℓ,ε)-compound code $\mathcal{C}$, and as shared randomness a random permutation λ of $[\ell]$; used to permute the input registers and to un-permute the outputs.

3. Compound to QAVC codes

To prove $C_{rand}(\mathcal{N}) = C(\{\mathcal{N}_\sigma\})$, we use any (ℓ,ε)-compound code C, and as shared randomness a random permutation λ of $[\ell]$; used to permute the input registers and to un-permute the outputs.

Reduces jammer strategies to permutation symmetric ones, which can be polynomially bounded by a convex combination of $\sigma^{\otimes \ell}$.

[Christandl/Koenig/Renner, PRL 2009]

3. Compound to QAVC codes

To prove $C_{rand}(N) = C(\{N_\sigma\})$, we use any (ℓ,ε)-compound code C, and as shared randomness a random permutation λ of $[\ell]$; used to permute the input registers and to un-permute the outputs.

Reduces jammer strategies to permutation symmetric ones, which can be polynomially bounded by a convex combination of $\sigma^{\otimes\ell}$.

[Christandl/Koenig/Renner, PRL 2009]

Finally, observe that $P_{err}(C,\sigma)$ is linear in σ.

3. Compound to QAVC codes

To prove $C_{rand}(\mathcal{N}) = C(\{\mathcal{N}_\sigma\})$, we use any (ℓ,ε)-compound code C, and as shared randomness a random permutation λ of $[\ell]$; used to permute the input registers and to un-permute the outputs.

Proposition 1: If C has error probability ε, then the above random code (C_λ) has error $\varepsilon' \leq poly(\ell).\varepsilon$.

Now, only need compound codes with super-polynomially fast error convergence ✓

4. Elimination of correlation

To prove $C_{det}(N) = C_{rand}(N)$, if the former is positive, we show that negligible (to be precise, $O(\log \ell)$) randomness is required to achieve the latter.

4. Elimination of correlation

To prove $C_{det}(N) = C_{rand}(N)$, if the former is positive, we show that negligible (to be precise, $O(\log \ell)$) randomness is required to achieve the latter.

Idea: $\mathbb{E}_\lambda P_{err}(C_\lambda, \sigma)$, for every jammer state σ, is average of values in $[0;1]$, so we can exponentially approximate it using n i.i.d. samples $\lambda_1, \lambda_2, \ldots, \lambda_n$ (Hoeffding bound); then union bound over σ.

4. Elimination of correlation

To prove $C_{det}(N) = C_{rand}(N)$, if the former is positive, we show that negligible (to be precise, $O(\log \ell)$) randomness is required to achieve the latter.

Idea: $\mathbb{E}_\lambda P_{err}(C_\lambda, \sigma)$, for every jammer state σ, is average of values in $[0;1]$, so we can exponentially approximate it using n i.i.d. samples $\lambda_1, \lambda_2, \dots, \lambda_n$ (Hoeffding bound); then union bound over σ. Fails, because discretisation requires $\exp(|J|^\ell)$ states ⚡

4. Elimination of correlation

Better idea: $P_{err}(C_\lambda,\sigma)$ is a linear function of σ, with values in [0;1], so it can be written $P_{err}(C_\lambda,\sigma) = Tr\ \sigma E_\lambda$, with some operator $0 \leq E_\lambda \leq I$.

4. Elimination of correlation

Better idea: $P_{err}(C_\lambda,\sigma)$ is a linear function of σ, with values in $[0;1]$, so it can be written $P_{err}(C_\lambda,\sigma) = \mathrm{Tr}\, \sigma\mathcal{E}_\lambda$, with some operator $0 \le \mathcal{E}_\lambda \le I$.

Hence, $\mathbb{E}_\lambda P_{err}(C_\lambda,\sigma) = \mathbb{E}_\lambda \mathrm{Tr}\, \sigma\mathcal{E}_\lambda = \mathrm{Tr}\, \sigma(\mathbb{E}_\lambda \mathcal{E}_\lambda)$, and it is enough to bound the largest eigenvalue of the average of $\mathcal{E}_\lambda$...

4. Elimination of correlation

Better idea: $P_{err}(C_\lambda,\sigma)$ is a linear function of σ, with values in $[0;1]$, so it can be written $P_{err}(C_\lambda,\sigma) = \mathrm{Tr}\,\sigma\mathcal{E}_\lambda$, with some operator $0 \leq \mathcal{E}_\lambda \leq I$.

Hence, $\mathbb{E}_\lambda P_{err}(C_\lambda,\sigma) = \mathbb{E}_\lambda \mathrm{Tr}\,\sigma\mathcal{E}_\lambda = \mathrm{Tr}\,\sigma(\mathbb{E}_\lambda\mathcal{E}_\lambda)$, and it is enough to bound the largest eigenvalue of the average of $\mathcal{E}_\lambda$...

Now use the matrix Hoeffding bound to show that average of $\mathcal{E}_{\lambda_i}$ $(i=1,\dots,n)$ is small!

[Ahlswede/AW, IEEE-IT 2002]

4. Elimination of correlation

Matrix Hoeffding bound: Let X_i be i.i.d random Hermitian $d\times d$-matrices $(i=1,\ldots,n)$, with $0 \leq X_i \leq I$. If $\mathbb{E}X_i \leq \varepsilon I$, then

$$\Pr\left\{\frac{1}{n}\sum_i X_i \not\leq (\varepsilon+\delta)I\right\} \leq d.\exp(-c.\delta^2 n)$$

[Ahlswede/AW, IEEE-IT 2002; see also Tropp, User-Friendly Matrix Tail Bounds]

4. Elimination of correlation

To prove $C_{det}(N) = C_{rand}(N)$, if the former is positive, we show that negligible (to be precise, $O(\log \ell)$) randomness is required to achieve the latter.

Proposition 2: If there is a random code with error $\le \varepsilon$, then there exists one with error $\le \varepsilon+\delta$, where the random variable takes only $n \le O(\ell/\delta^2)$ values.

4. Elimination of correlation

To prove $C_{det}(N) = C_{rand}(N)$, if the former is positive, we show that negligible (to be precise, $O(\log \ell)$) randomness is required to achieve the latter.

Proposition 2: If there is a random code with error $\leq \varepsilon$, then there exists one with error $\leq \varepsilon + \delta$, where the random variable takes only $n \leq O(\ell/\delta^2)$ values.

If $C_{det}(N) > 0$, this can be generated inefficiently, not losing any rate.

5. Reflections/Conclusion

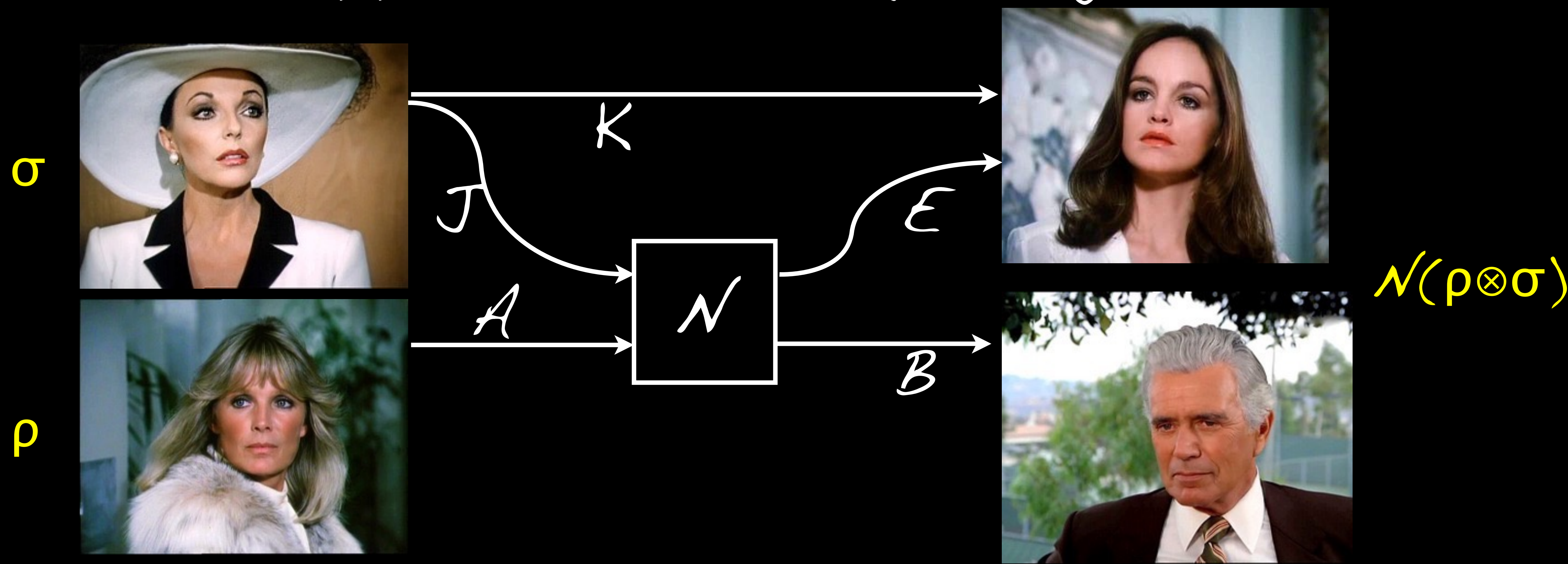
1) Random permutations provide a systematic link between compound and arbitrarily varying jammer, explaining why the capacity formulas are the same
2) Matrix tail bounds establish the fully quantum analogue of the Ahlswede dichotomy, showing that the required randomness is always logarithmic in the block length.

5. Reflections/Conclusion

3) Both results rely on the linearity of the error in σ, and more specifically that it is given by an observable $0 \leq \mathcal{E} \leq \mathcal{I}$, which works for both C and Q. This is non-trivial and may not be the case for other channel capacities.

5. Reflections/Conclusion

4) Don't take it for granted! Consider the private capacity $P(\mathcal{N})$, introducing an eavesdropper informed by the jammer:



The problem is that the privacy criterion (trace norm) isn't linear in σ...

5. Reflections/Conclusion

5) We also used finiteness of $|A|$, $|B|$ and most importantly $|J|$. If we keep input and output finite, can we also allow infinite dimensional J? This presents a problem both for the de Finetti reduction to compound, as well as for the elimination of correlation [Cf. Ahlswede, Z. Wahrsch. Verw. Geb. 1978]

Thanks for watching!