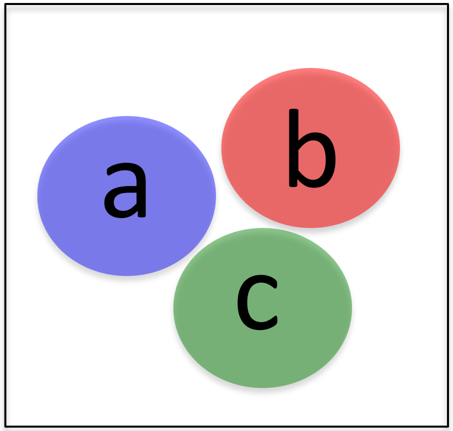
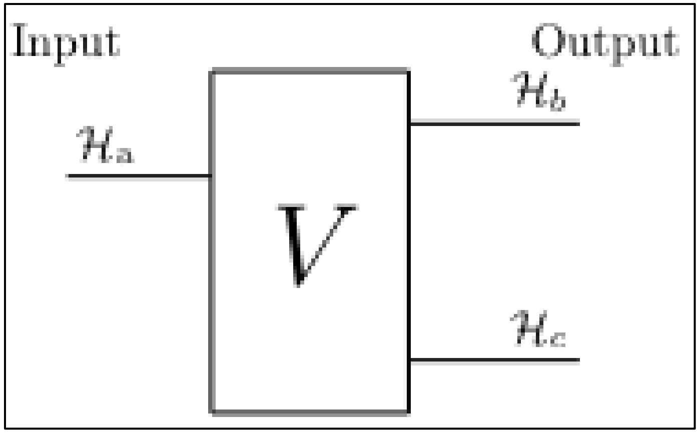
Information-theoretic treatment of tripartite systems and quantum channels

Patrick Coles
Carnegie Mellon University
Pittsburgh, PA
USA

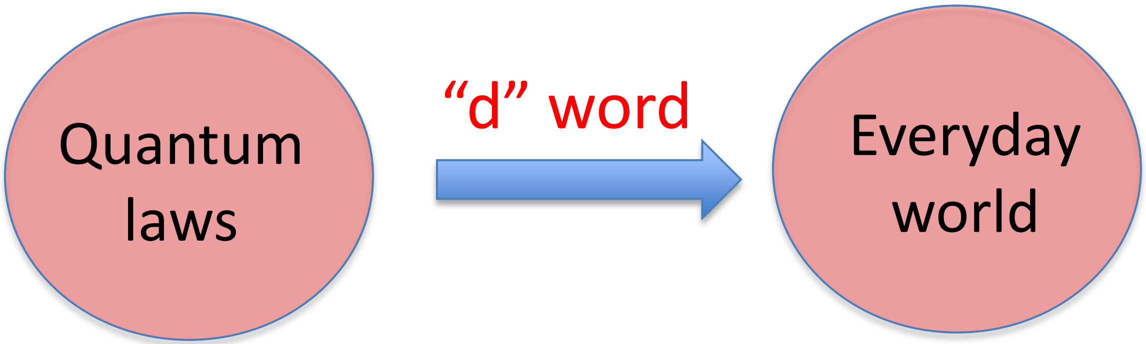
ArXiv: 1006.4859



Co-authors
Li Yu
Vlad Gheorghiu
Robert Griffiths



Research program



<u>Approach</u>

~~1.) Dynamics of prototypical systems~~
~~(Consistent histories)~~

2.) Information theory

How is quantum information unusual?

- *More general* than classical information

- Classical information: always possible to combine two logical statements to make a new logical statement

  "Spain won the Euro-Cup AND Spain won the World Cup."

- "The z-component of an electron spin is +1/2 AND its x-component is -1/2."
  NONSENSE

  x and z are incompatible types of information

- *Challenge: finding relations between incompatible types of information*

- Strong tradeoff in transmitting incompatible (i.e. quantum) information
  - through a channel and its complementary channel
  - to distinct parties of a multipartite state

Types and location of information

<u>Type of information</u>

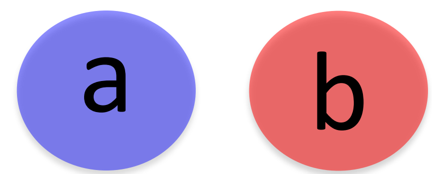
Technically: Decomposition of the identity

$$I_a = \sum_j P_{aj}$$

where $\{P_{aj}\}$ is set of orthogonal projectors

we also consider more general decompositions (POVMS)

Information of some type about *a* can be located inside *b* (in that some property of *b* is correlated to this property of *a*)

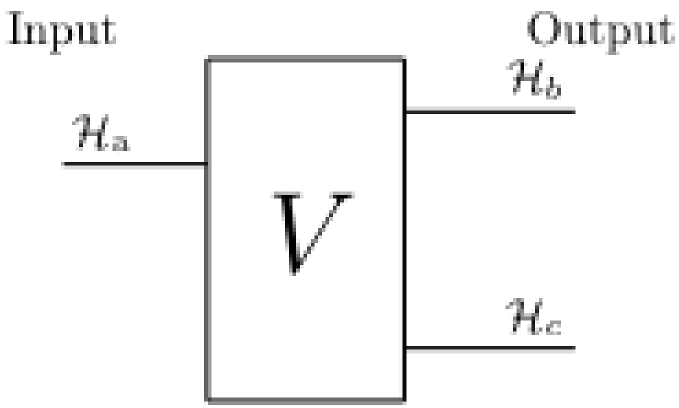


Are the conditional density operators on b, associated with the P_a information, distinguishable?

$$p_j \rho_{bj} = \mathrm{Tr}_a(P_{aj}\rho_{ab}) \qquad p_j := \Pr(P_{aj})$$

…. we aim to quantify this

Quantum Channel Problem

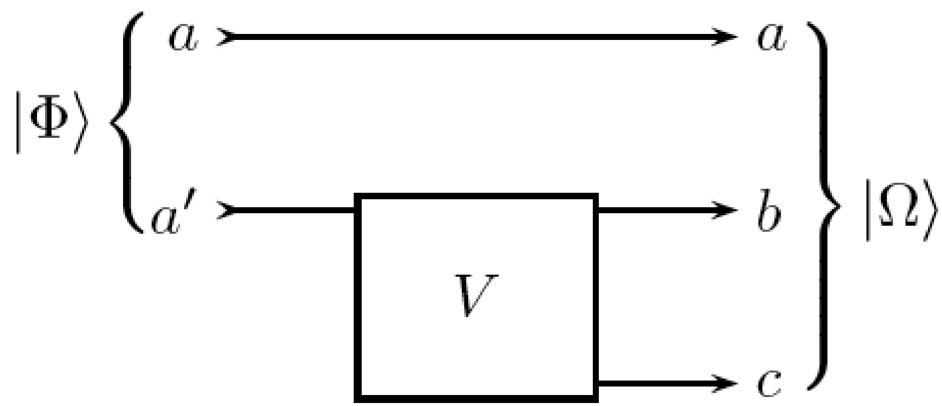


$$V^\dagger V = I_a$$

complementary channels

- D word
- Cryptography

Introduce reference system



$|\Phi\rangle$ is maximally entangled

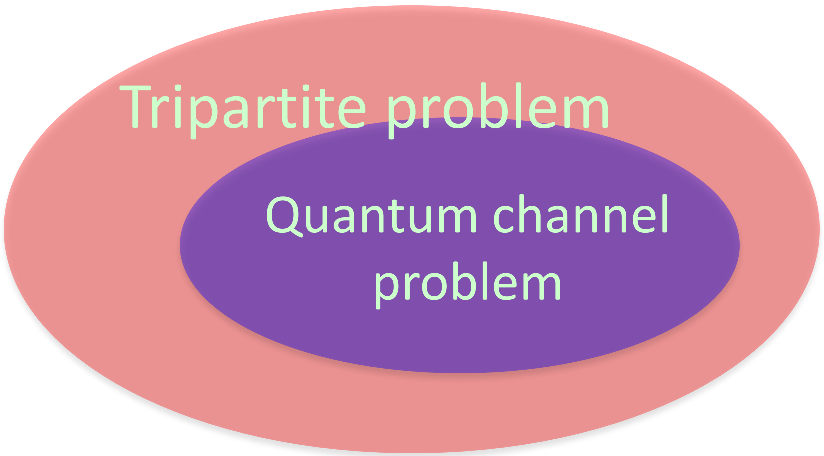
$$|\Omega\rangle = (I_a \otimes V)|\Phi\rangle$$

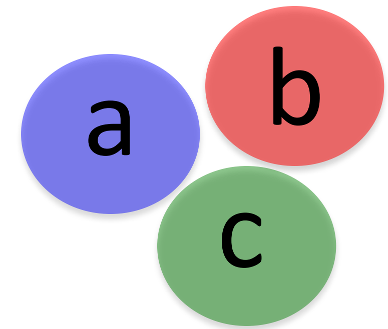
$$\rho_a = \mathrm{Tr}_{bc}(|\Omega\rangle\langle\Omega|) = I_a/d_a$$

Or start from the tripartite pure state,
use map-state duality to construct isometry

$$\sqrt{d_a}|\Omega\rangle = \sum_j |a_j\rangle \otimes |s_j\rangle \qquad V = \sum_j |s_j\rangle\langle a_j|$$

Three-party problem





$$\mathcal{H}_{abc} = \mathcal{H}_a \otimes \mathcal{H}_b \otimes \mathcal{H}_c$$

$$d_a,\ d_b,\ d_c$$

$$I_a = \sum_j P_{aj}, \quad I_b = \sum_k Q_{bk}, \quad I_c = \sum_l R_{cl}$$

What can we say about the probability distribution?

$$\Pr(P_{aj}, Q_{bk}, R_{cl}) = \mathrm{Tr}(P_{aj} Q_{bk} R_{cl} \rho_{abc})$$

<u>All-or-nothing theorems</u>

e.g. all information about *a* in *b*, then none in *c*

Goal: generalize all-or-nothing results to case of partial information

Information measures

General form

$$\chi_K(\{p_j,\rho_j\}) = S_K(\sum_j p_j\rho_j) - \sum_j p_j S_K(\rho_j)$$

$$\chi_K(P_a,b) := S_K(\rho_b) - \sum_j p_j S_K(\rho_{bj})$$

Particular entropy functions

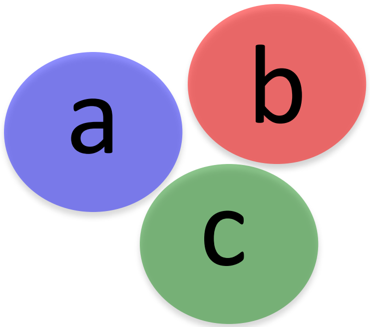
$$S_V(\rho) = -\mathrm{Tr}(\rho\log\rho),$$

$$S_R(\rho) = \frac{1}{1-q}\log\mathrm{Tr}(\rho^q), \quad 0 < q \leqslant 1,$$

$$S_T(\rho) = \frac{1}{1-q}[\mathrm{Tr}(\rho^q) - 1], \quad 0 < q \leqslant \infty$$

$$S_Q(\rho) = 1 - \mathrm{Tr}(\rho^2).$$

Basis invariance of information difference



<u>Definitions</u>

Entropy bias $\Delta S_K^{bc} := S_K(\rho_b) - S_K(\rho_c)$

Information bias $\Delta_K^{bc}(P_a) := \chi_K(P_a, b) - \chi_K(P_a, c)$

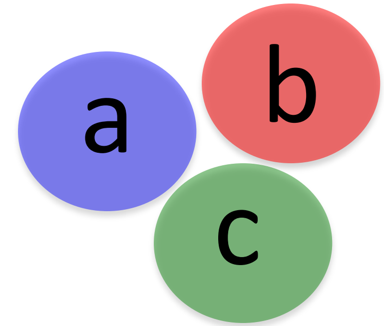
<u>Theorem</u>

Consider orthonormal bases *u* and *w* for system *a*

$\rho_{abc} = |\Omega\rangle\langle\Omega|$ (pure state)

$$\begin{aligned}\Delta_K^{bc}(w) &= \chi_K(w, b) - \chi_K(w, c) \\ &= S_K(\rho_b) - S_K(\rho_c) = \Delta S_K^{bc}\end{aligned}$$

Basis invariance of information difference

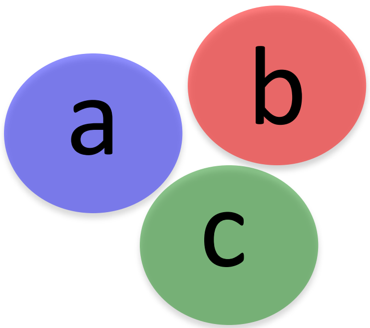


$$\rho_{abc} = |\Omega\rangle\langle\Omega|$$

Difference between Bob's and Charlie's scores is the same every game!

Example

$$\chi_V(z,b) - \chi_V(z,c) = \chi_V(x,b) - \chi_V(x,c)$$
$$\chi_V(z,b) - \chi_V(x,b) = \chi_V(z,c) - \chi_V(x,c)$$



$$\rho_{abc} = |\Omega\rangle\langle\Omega|$$

Suppose Bob has perfect classical information about Alice

$$\chi_V(z,b) = \log d_a$$
$$\chi_V(x,b) = 0$$

Then it follows that:

$$\chi_V(z,c) = \log d_a$$
$$\chi_V(x,c) = 0$$

So classical information always gets copied

Shannon and von Neumann measures

Classical entropy: $$H(P) = H(\{p_j\}) = -\sum_j p_j \log p_j$$

Classical mutual information: $$H(P:Q) = H(P) + H(Q) - H(P,Q)$$

A relation between classical and quantum entropies:

$$\chi_V(\{p_j, \rho_j\}) = S_V(\sum_j p_j \rho_j) - \sum_j p_j S_V(\rho_j) \leqslant H(\{p_j\})$$

$$\chi_V(\{p_j, \rho_j\}) = H(\{p_j\})$$ iff all ρ_j are orthogonal

$$\theta(P_a, b) := H(P_a) - \chi_V(P_a, b)$$ *is a positive quantity "missing information"*

Uncertainty Principle

Robertson. Phys. Rev. (1929)

$$\Delta A \Delta B \geq \frac{1}{2} |\langle \psi | [A, B] | \psi \rangle|$$

Right-hand-side depends on the state.

Can be zero,
e.g. A=Z, B=X,
|ψ> = z-eigenstate.

$$\Delta X = \sqrt{\langle \psi | X^2 | \psi \rangle - \langle \psi | X | \psi \rangle^2}$$

Entropy: alternative measure of spread

Maassen, Uffink. PRL (1988)

$$H(u) + H(w) \geq -\log(r^2)$$

$$r = \max_{j,k} |\langle u_j | w_k \rangle|$$

Mutually unbiased bases (MUBs)

$$r = 1/\sqrt{d} \qquad H(x) + H(z) \geq \log d$$

The main result

ArXiv: 1006.4859

Theorem

POVMs on $\mathcal{H}_a$

$P_a = \{P_{aj}\}$

$\bar{P}_a = \{\bar{P}_{ak}\}$

$$\theta(P_a, b) := H(P_a) - \chi_V(P_a, b)$$

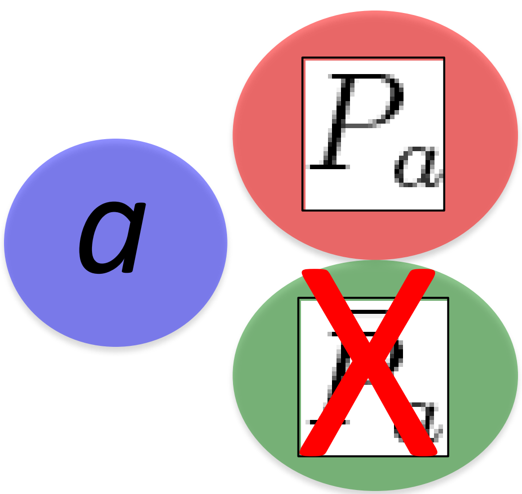
"missing information"

$$\theta(P_a, b) + \theta(\bar{P}_a, c) \geqslant -\log \max_{j,k} \mathrm{Tr}[P_{aj}\bar{P}_{ak}]$$

Very general, Very strong
uncertainty relation

Presence of P_a *information in b*

EXCLUDES $\bar{P}_a$ *information from c*



Appreciating this result

Orthonormal bases

$$u = \{|u_j\rangle\langle u_j|\}$$
$$w = \{|w_k\rangle\langle w_k|\}$$

$$\theta(u,b) + \theta(w,c) \geqslant -\log r^2$$
$$r = \max_{j,k} |\langle u_j|w_k\rangle|$$

Mutually unbiased bases (MUBs)

$$\theta(u,b) + \theta(w,c) \geqslant \log d_a$$

Both an entropic uncertainty relation AND information exclusion relation

$$H(u) + H(w) \geqslant \chi_V(u,b) + \chi_V(w,c) + \log d_a$$

Suppose $\theta(u,b)=0$…. then $H(w)=\log d_a$ AND $\chi_V(w,c)=0$

$$\theta(u_a,b) = S_V(u_a|b)$$
$$S_V(u_a|b) := S_V[\mathcal{U}_a(\rho_{ab})] - S_V(\rho_b)$$
$$\mathcal{U}_a(\rho_{ab}) = \sum_j P_{aj}\rho_{ab}P_{aj}$$

Equivalent to "strong complementary information tradeoff" conjectured by Renes, Boileau (PRL 2009), proven by Berta et al. (Nature Physics 2010)

Corollaries

Strengthened uncertainty relations for mixed states

Maassen, Uffink (1988) $$H(u) + H(w) \geqslant -\log(r^2)$$

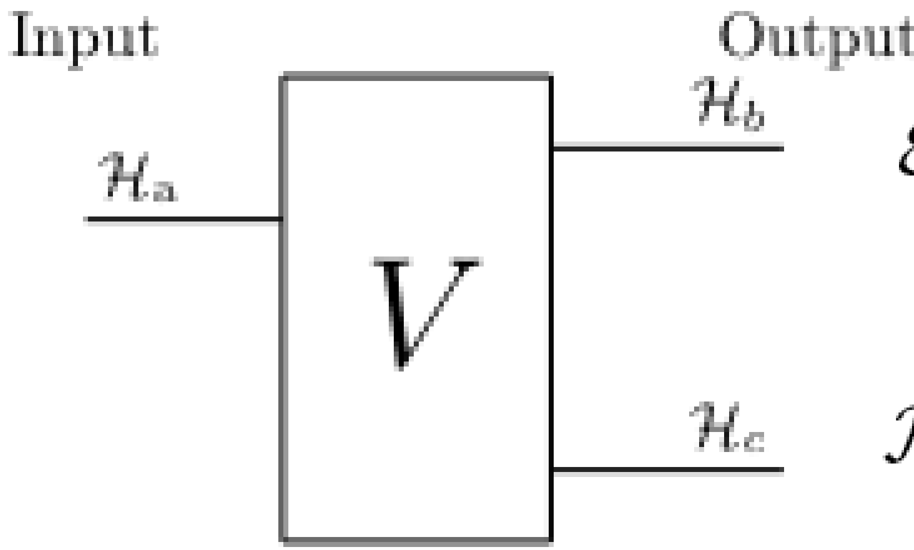
Corollary of our result $$H(u) + H(w) \geqslant -\log r^2 + S_V(\rho_a)$$

$d_a = 2$ For qubits, *x, y,* and *z* form a complete set of MUBs

Sanchez-Ruiz (1995) $$H(x) + H(y) + H(z) \geqslant 2\log 2$$

Corollary of our result $$H(x) + H(y) + H(z) \geqslant 2\log 2 + S_V(\rho_a)$$

The *dynamic* uncertainty principle



$\mathcal{E}$: channel to b

$\mathcal{F}$: channel to c

<u>Output density operators</u>

$$\rho_{bj} = \mathcal{E}(|w_j\rangle\langle w_j|)$$
$$= \mathrm{Tr}_c(V|w_j\rangle\langle w_j|V^\dagger)$$

- Feed in *w* basis states
- Input probabilities $\{p_j\}$

<u>Quantify distinguishability at the output</u>

$$\chi_K(\{p_j\}, w, \mathcal{E}) = S_K(\sum p_j \rho_{bj}) - \sum p_j S_K(\rho_{bj})$$

The *dynamic* uncertainty principle

Quantify distinguishability at the output

$$\chi_K(\{p_j\}, w, \mathcal{E}) = S_K(\sum p_j \rho_{bj}) - \sum p_j S_K(\rho_{bj})$$

Corollary of our result

Arbitrary bases *u* and *w*, $r = \max_{j,k} |\langle u_j | w_k \rangle|$

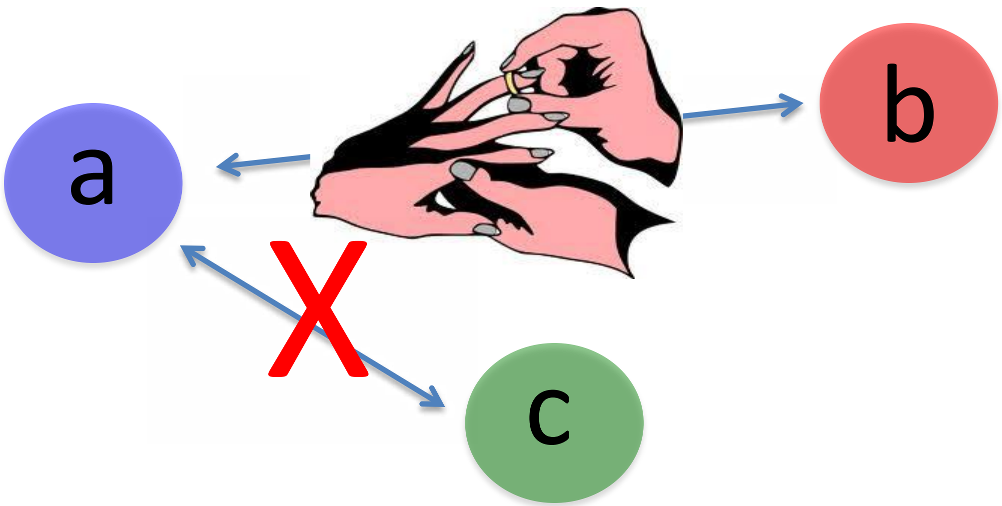
complementary quantum channels $\mathcal{E}$ and $\mathcal{F}$.

$$\chi_V(\{1/d_a\}, u, \mathcal{E}) + \chi_V(\{1/d_a\}, w, \mathcal{F}) \leqslant 2 \log(d_a r)$$

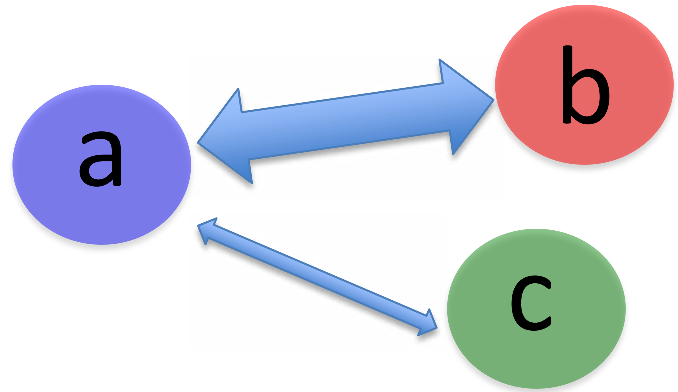
Can’t build a machine that can send *z*-info to Bob and *x*-info to Charlie

No copying or No splitting or Monogamy

Monogamy of entanglement



Gradual approach to monogamy



If $\theta(w, b) \leqslant \alpha$ $\quad$ every orthonormal basis w of $\mathcal{H}_a$

then $\chi_V(w, c) \leqslant \alpha$ every orthonormal basis w of $\mathcal{H}_a$

Proof: Every basis has at least one MUB

But do we really have to know that Bob has every type *w* of information about Alice to ensure Charlie has none?

Two-type presence

Alice & Bob
Date #1

+

Alice & Bob
Date #2

(provided dates are sufficiently different)

→ Alice & Bob

→ Charlie (no Alice)

Quantum mutual information

$$I(a:b) = S_V(\rho_a) + S_V(\rho_b) - S_V(\rho_{ab})$$

$$I(a:b) \geq 2\log d_a - 2[\theta(x,b) + \theta(z,b)]$$

$$I(a:c) \leq \theta(x,b) + \theta(z,b)$$

More general form, for arbitrary bases, on ArXiv

One-type presence/absence

Alice & Bob
Date #1:
Drinks

Alice & Charlie
Date #1:
Drinks

Charlie (no Alice)

Charlie completely decoupled from Alice!

One-type presence/absence

Quantitative version

$$I(a:c) \le \chi_V(z,c) + \theta(z,b)$$

Suppose the *z* type of information about *a* is perfectly present in *b*:

$$\theta(z,b) = 0$$

… and absent from *c*:

$$\chi_V(z,c) = 0$$

Then *a* and *c* are completely uncorrelated:

$$\rho_{ac} = \rho_a \otimes \rho_c.$$

All-or-nothing theorem not previously known?

Results for Tripartite states

- All-or-nothing theorems
- Theorems for MUBs

- Partial information theorems
- More general types of information

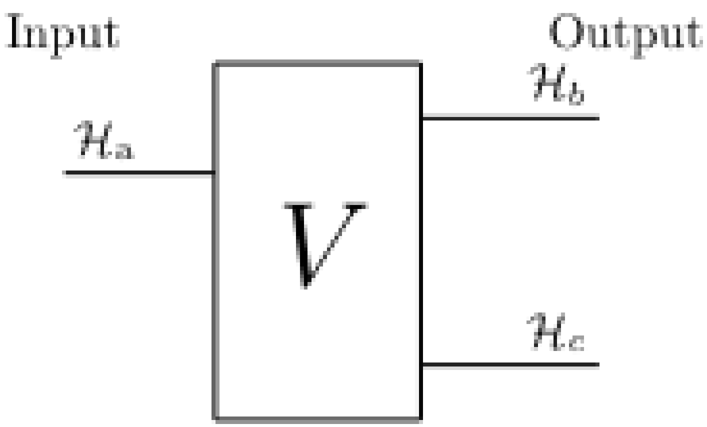
- Basis invariance of information bias $$\Delta_K(w) = \Delta S_K$$
- Uncertainty principle $$\theta(x,b) + \theta(z,c) \geq \log d_a$$
- Monogamy (No copying) $$I(a:b) \geq 2\log d_a - 2[\theta(x,b) + \theta(z,b)]$$
- Two type presence $$I(a:c) \leq \theta(x,b) + \theta(z,b)$$
- One type presence / absence $$I(a:c) \leq \chi_V(z,c) + \theta(z,b)$$

All of these results apply to complementary quantum channels!

One would have never stumbled upon our results using a global measure of entanglement, it is crucial to look at *individual types of information* to study these phenomena

Patrick Coles
Carnegie Mellon
Postdoc in Quantum Information & Foundations

Equations for complementary channels



Quadratic measure

$$I_Q(w,b) = \frac{1}{d-1}\sum_{m=1}^{d-1} \|\mathcal{E}_b(W^m)\|^2 \,/\, \|\mathcal{E}_b(I)\|^2$$

d: input dimension

$\mathcal{E}_b$: channel to b

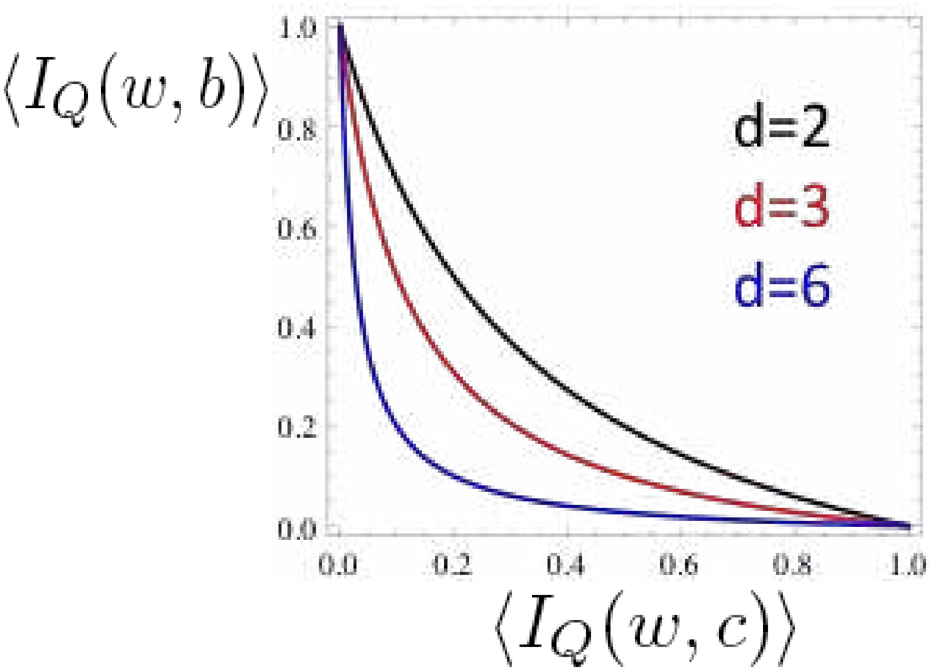
$\mathcal{E}_c$: channel to c

$$W = \sum_{j=0}^{d-1} \omega^j |w_j\rangle\langle w_j|$$

$$\omega = \mathrm{e}^{2\pi \mathrm{i}/d}$$

Normalized such that: $0 \leq I_Q(w,b) \leq 1$

=1 iff all states are orth. at output



Average over all types

$$\langle I_Q(w,b)\rangle = \mathrm{Avg}[I_Q(UwU^\dagger, b)]_U$$

$$\langle I_Q(w,b)\rangle = \frac{1-\langle I_Q(w,c)\rangle}{1+(d^2-1)\langle I_Q(w,c)\rangle}$$

Generalizes Somewhere Theorem AND No Splitting Theorem in single equation!

Take-home messages

All-or-nothing theorems are just limiting cases of partial-information relations.

Quantum information comes in *different types*

One would have never stumbled upon our results using a global measure of entanglement, it is crucial to look at individual types of information to study these phenomena

Quantum channels can be studied within the framework of tripartite states

Patrick Coles
Carnegie Mellon University

Future directions?

Location of quantum information in 4-party (or n-party) systems

Find more equations, not just inequalities, for the location of quantum information.

Other measures besides von Neumann.

Apply these rules to physical systems of interest (e.g. quantum optics, spins)

Apply these rules to cryptography protocols or other Q.I. tasks

The main result

Lemma

[proven using an EUR of Krishna, Parthasarathy. Ind. J. of Stat. (2002)]

POVMs on $\mathcal{H}_a$

$P_a = \{P_{aj}\}$

$\bar{P}_a = \{\bar{P}_{ak}\}$

POVMs on $\mathcal{H}_b$ and $\mathcal{H}_c$

Q_b and R_c

$$H(P_a : Q_b) + H(\bar{P}_a : R_c) \leqslant H(P_a) + H(\bar{P}_a) + \log \max_{j,k} \left\| (P_{aj})^{1/2} (\bar{P}_{ak})^{1/2} \right\|_\infty^2$$

Theorem

[proven by invoking the HSW theorem for the achievable information transmission]

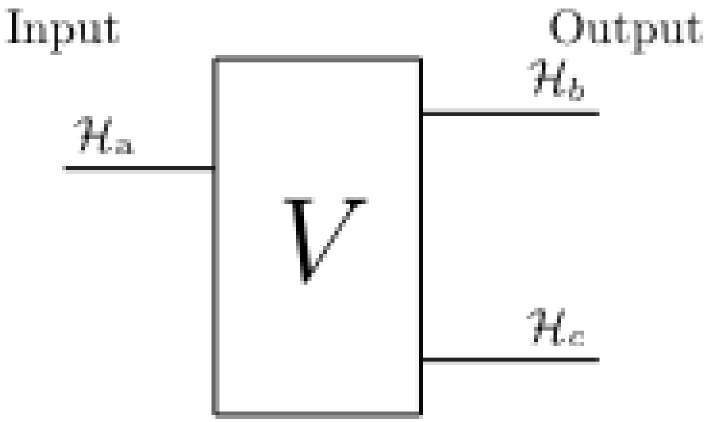
$$\theta(P_a, b) + \theta(\bar{P}_a, c) \geqslant -\log \max_{j,k} \left\| (P_{aj})^{1/2} (\bar{P}_{ak})^{1/2} \right\|_\infty^2 \geqslant -\log \max_{j,k} \mathrm{Tr}[P_{aj} \bar{P}_{ak}]$$

Very general, Very strong
uncertainty relation

All or nothing theorems

- All info about A in B, then none in C
- All info about A in BC, and none in C, then all in B (Pure state ABC)
- All z info about A in B, no x info about A in C
- z and x info about A in B, then all info about A in B

Equations for complementary channels



Quadratic measure

$$I_Q(w,b) = \frac{1}{d-1}\sum_{m=1}^{d-1} \|\mathcal{E}_b(W^m)\|^2 \,/\, \|\mathcal{E}_b(I)\|^2$$

d: input dimension
$\mathcal{E}_b$: channel to b
$\mathcal{E}_c$: channel to c

$$W = \sum_{j=0}^{d-1} \omega^j |w_j\rangle\langle w_j|$$

$$\omega = \mathrm{e}^{2\pi\mathrm{i}/d}$$

Normalized such that:

$$0 \le I_Q(w,b) \le 1$$

=1 iff all states are orth. at output

Consider complete set of MUBs

$$\mathcal{M} = \{w_j\} \quad (d+1 \text{ MUBs})$$

e.g. prime *d*:

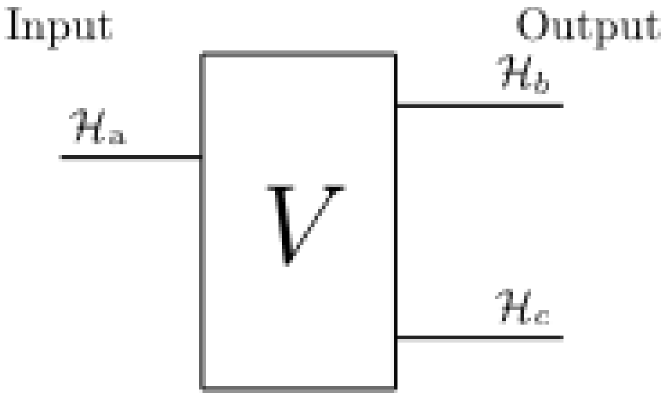
$$Z, X, XZ, XZ^2, \ldots, XZ^{d-1}$$

$$X = \sum_{j=0}^{d-1} |j\rangle\langle j+1|, \quad Z = \sum_{j=0}^{d-1} \omega^j |j\rangle\langle j|$$

Average over complete set

$$\langle I_Q(w,b)\rangle_{\mathcal{M}} = \frac{1}{d+1}\sum_{j=1}^{d+1} I_Q(w_j,b)$$

Equations for complementary channels



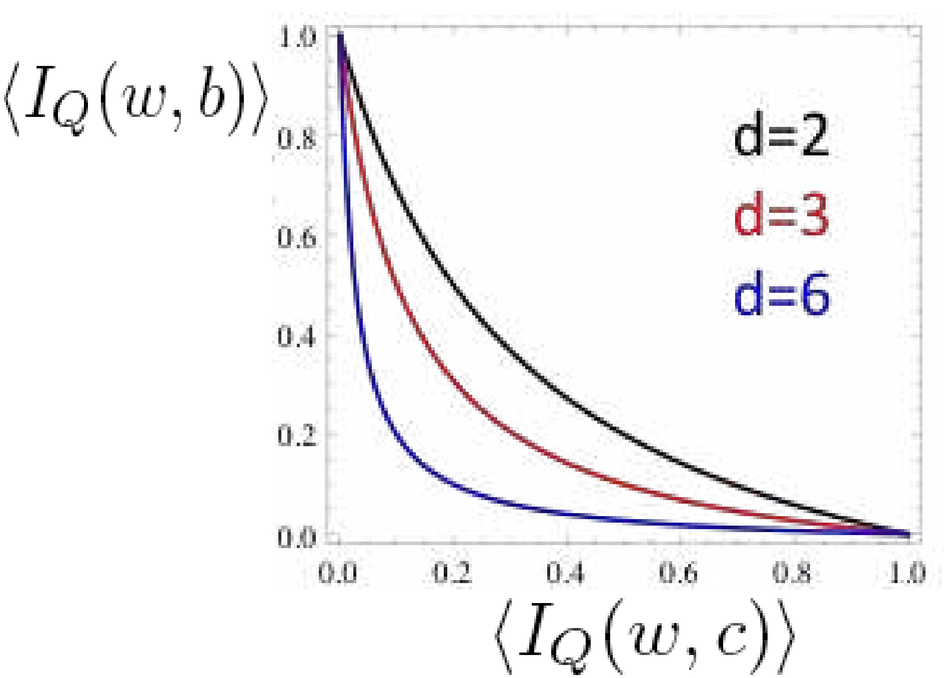
Average over all types

$$\langle I_Q(w,b)\rangle = \mathrm{Avg}[I_Q(UwU^\dagger, b)]_U$$

Prime-power *d* : Average over complete set of MUBs equal to average over all types

$$\langle I_Q(w,b)\rangle = \langle I_Q(w,b)\rangle_{\mathcal{M}}$$

Complete MUB set captures behavior of whole Hilbert space



$$\langle I_Q(w,b)\rangle = \frac{1-\langle I_Q(w,c)\rangle}{1+(d^2-1)\langle I_Q(w,c)\rangle}$$

Generalizes Somewhere Theorem AND No Splitting Theorem in single equation!

Quadratic Measure, complementary channels

$$\rho_{bj} = \mathcal{E}(|w_j\rangle\langle w_j|) = \mathrm{Tr}_c(V|w_j\rangle\langle w_j|V^\dagger)$$

$$\chi_K(\{p_j\}, w, \mathcal{E}) = S_K(\sum p_j \rho_{bj}) - \sum p_j S_K(\rho_{bj})$$

$$d_a = 2$$

$$\chi_Q(\{p_j\}, u, \mathcal{E}) + \chi_Q(\{q_j\}, w, \mathcal{F}) \leqslant 1/2$$

Absence

Bipartite $|\Psi\rangle \in \mathcal{H}_a \otimes \mathcal{H}_b \quad independent\ of\ the\ basis\ w$

$$\chi_K(w,b) = S_K(\rho_b)$$

$$\rho_{abc} = |\Omega\rangle\langle\Omega|$$

$$\chi_V(u,b) = S_V(\rho_a) = J_V(a:b)/2 = H(w)$$

Coherent Information

$$I_{coh}(\rho_{a'},\mathcal{E}) = \Delta S_V^{bc}(|\Omega\rangle) = \Delta_V^{bc}(|\Omega\rangle)$$

Quantum mutual information

$$S_V(\rho_{ab}) + S_V(\rho_{bc}) \geqslant S_V(\rho_{abc}) + S_V(\rho_b)$$