

Complementarity and Privacy in Quantum Information Theory

Joseph M. Renes  and Jean-Christian Boileau 



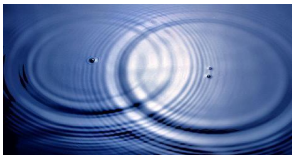
Theoretical Quantum Physics, Institut für Angewandte Physik
Technische Universität Darmstadt



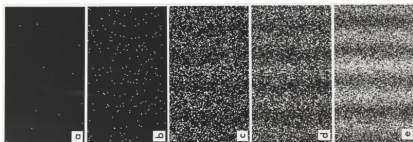
Center for Quantum Information and Quantum Control
University of Toronto

DPG Frühjahrstagung Darmstadt 2008 March 13

Complementarity: Essence of Quantum Mechanics



or



The double slit experiment "is impossible, absolutely impossible, to explain in any classical way, and has in it the heart of quantum mechanics. In reality, it contains the only mystery." -Feynman

Privacy: Ubiquitous in Quantum Information Theory

- ☞ Quantum cryptography
- ☞ Entanglement! (monogamy)
- ☞ Informs nearly every aspect of QIT

Importance of both privacy and complementarity is no coincidence!

To convince you, this talk will. . .

- 1 Build up to a new information-theoretic description of complementarity
- 2 Use this to decouple eavesdroppers & environments, ensuring privacy
- 3 Briefly discuss how central results of QIT stem from complementarity

Complementary Tradeoffs

- Not just a dichotomy, also exist intermediate states Wootters & Zurek
PRD 19 473 (1979)
- Tradeoffs:
 - ① Path info vs fringe visibility (double slit) wz 79
 - ② Fringe visibility vs path predictability (interferometer) Greenberger & Yasin,
PLA 128 392 (1988)
 - ③ Also mixed states Jaeger, Shimony, Vaidman, PRA 51 54 (1995); Englert PRL 77 2154 1996
 - ④ many more ...

Information-Theoretic (Operational) Approach

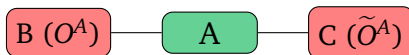
- ① Focus on measurable quantities (observables)
 - instead of trying to quantify properties
- ② How much information can be obtained about complementary observables?
 - must be some upper limit depending on the observables. . .

Entropic Uncertainty Relation Maassen & Uffink PRL 60 1103 (1988)

$$H(O^A) + H(\tilde{O}^A) \geq -\log \max_{jk} |\langle j|\tilde{k}\rangle|^2$$

O^A, \tilde{O}^A operators on system A ; eigenvectors $|j\rangle$ and $|\tilde{k}\rangle$; $H(\cdot)$ entropy.

- but how much info can we *simultaneously* extract?
- include measurement systems in the description!



Information Exclusion Principle Hall PRL 74 3307 (1995)

$$I(O^A:\Lambda^B) + I(\tilde{O}^A:\Gamma^C) \leq H(O^A) + H(\tilde{O}^A) + \log \max_{jk} |\langle j|\tilde{k}\rangle|^2$$

Λ^B, Γ^C measurements on B, C . $I(\cdot:\cdot)$ mutual information (classical).

- ➡ tradeoff in simultaneously available, complementary classical information

Complementary Information Tradeoff (conjectured)

$$I(O^A:B) + I(\tilde{O}^A:C) \leq H(O^A) + H(\tilde{O}^A) + \log \max_{j,k} |\langle j|\tilde{k}\rangle|^2$$

- “quantized” information exclusion principle
 - replace classical mutual info with quantum mutual info (Holevo quantity)
- stronger than classical version (locking); implies uncertainty relation
- tightest tradeoff for conjugate observables: $-\log \max_{j,k} |\langle j|\tilde{k}\rangle|^2 = \log \dim(A)$
- related to: quantum channel uncertainty relation Christandl & Winter
IEEE TIT 51 3159 (2005).
 - “dynamic” version of “static” CIT
 - holds for conjugate observables
 - proof from strong subadditivity; can apply proof to CIT
- numerical evidence for non-conjugate observables ($d \approx 20$)
- can saturate the bound for conjugate observables with nonextremal states

Complementarity leads directly to privacy/decoupling

Decoupling

Given $|\psi\rangle^{ABC}$ with $S(\psi^A) \leq -\log \max_{jk} |\langle j|\tilde{k}\rangle|^2 \leq \log \dim(A)$, suppose

(i) $I(O^A:B) = H(O^A) - \epsilon$ and (ii) $I(\tilde{O}^A:B) = H(\tilde{O}^A) - \tilde{\epsilon}$

Then $\|\psi^{AC} - \psi^A \otimes \psi^C\|_1 \leq \sqrt{2 \log 2} \sqrt{\epsilon + \tilde{\epsilon}}$.

- ➡ like monogamy of entanglement, but more general
- ➡ can decouple w/o needing conjugate observables

Applied decoupling

- ENTANGLEMENT

for conjugate O^A, \tilde{O}^A , decoupling implies

ψ^{AB} is (approximately) maximally-entangled

- PRIVATE STATES

including a shield system S into $I(\tilde{O}^A:BS)$,

decoupling + $I(O^A:\Lambda^B) = H(O^A) - \epsilon$ implies

measurement of O^A and Λ^B gives an approximate secret key

- DISTILLATION

A supplies “missing” info to B ; leads to new proofs of:

- Quantum Csiszar-Körner bound on secret key distillation rate: $K_{\rightarrow}(\psi^{ABSE}) \geq I(Z^A:B) - I(Z^A:E)$
- Hashing inequality for entanglement distillation: $E_{\rightarrow}(\psi^{AB}) \geq S(B) - S(AB)$
- Direct coding theorem for channel capacity: $Q(\mathcal{N}) \geq I_c(\rho, \mathcal{N})$

Conclusion:

Fundamental results of quantum information theory rest on the phenomenon of complementarity

