Duality of channels and codes

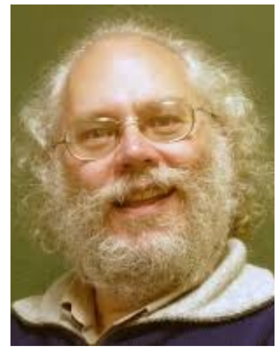
Joseph M. Renes

ETH zürich

IEEE Trans Inf Theory 64, 577 (2018)

arXiv:1708.05685 [quant-ph]

VOLUME 85, NUMBER 2 PHYSICAL REVIEW LETTERS 10 JULY 2000



Simple Proof of Security of the BB84 Quantum Key Distribution Protocol

Peter W. Shor[1] and John Preskill[2]
[1]*AT&T Labs Research, Florham Park, New Jersey 07932*
[2]*Lauritsen Laboratory of High Energy Physics, California Institute of Technology, Pasadena, California 91125*
(Received 28 February 2000)

We prove that the 1984 protocol of Bennett and Brassard (BB84) for quantum key distribution is secure. We first give a key distribution protocol based on entanglement purification, which can be proven secure using methods from Lo and Chau's proof of security for a similar protocol. We then show that the security of this protocol implies the security of BB84. The entanglement purification based protocol uses Calderbank-Shor-Steane codes, and properties of these codes are used to remove the use of quantum computation from the Lo-Chau protocol.

PACS numbers: 03.67.Dd

Security $\Longleftrightarrow$ Error correction

VOLUME 93, NUMBER 8 PHYSICAL REVIEW LETTERS week ending 20 AUGUST 2004

Relating Quantum Privacy and Quantum Coherence: An Operational Approach

I. Devetak[1] and A. Winter[2]
[1]*IBM T. J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598, USA*
[2]*School of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom*
(Received 10 July 2003; published 19 August 2004)

Given many realizations of a state or a channel as a resource, two parties can generate a secret key as well as entanglement. We describe protocols to perform the secret key distillation (as it turns out, with optimal rate). Then we show how to achieve optimal entanglement generation rates by ''coherent'' implementation of a class of secret key agreement protocols, proving the long-conjectured ''hashing inequality.''

DOI: 10.1103/PhysRevLett.93.080501 PACS numbers: 03.67.Dd, 03.67.Hk, 03.67.Pp

This talk:
clear & tight formalization of the connection, w/ applications

- Dual channels & entropies
- Use in polar codes & belief propagation decoding
- Privacy amplification & source coding
- Duality in classical BP

Complementary, or dual channel

R, IEEE TIT 64, 577 (2018)

CQ channel

$$z \dashrightarrow \boxed{W} \longrightarrow \varphi_z$$

Dual CQ channel

$$x \dashrightarrow \boxed{W^\perp} \longrightarrow \vartheta_x$$

Equality in uncertainty relation: $H(Z|W(Z)) + H(X|W^\perp(X)) = 1$

Equality for arbitrary entropies! $\mathbb{H}(Z|W(Z)) + \mathbb{H}^\perp(X|W^\perp(X)) = 1$

$\mathbb{H}^\perp(A|C)_\rho = -\mathbb{H}(A|B)_\rho$ for ρ pure

e.g. $\mathbb{H} = H_{\min}, \mathbb{H}^\perp = H_{\max}$, smooth versions, Rényi, etc.

Complementary, or dual channel

R, IEEE TIT 64, 577 (2018)

CQ channel

$$z \dashrightarrow \boxed{W} \rightarrow \varphi_z$$

Dual CQ channel

$$x \dashrightarrow \boxed{W^\perp} \rightarrow \vartheta_x$$

Equality in uncertainty relation: $H(Z|W(Z)) + H(X|W^\perp(X)) = 1$

Equality for arbitrary entropies! $\mathbb{H}(Z|W(Z)) + \mathbb{H}^\perp(X|W^\perp(X)) = 1$

Consequences: tight relation between channel & its dual

capacity $I(W) + I(W^\perp) = \log d$

dispersion $V(W) = V(W^\perp)$

W reliable iff $W^\perp$ has constant output

Dual channel: Construction

1. Take a classical input / quantum output channel

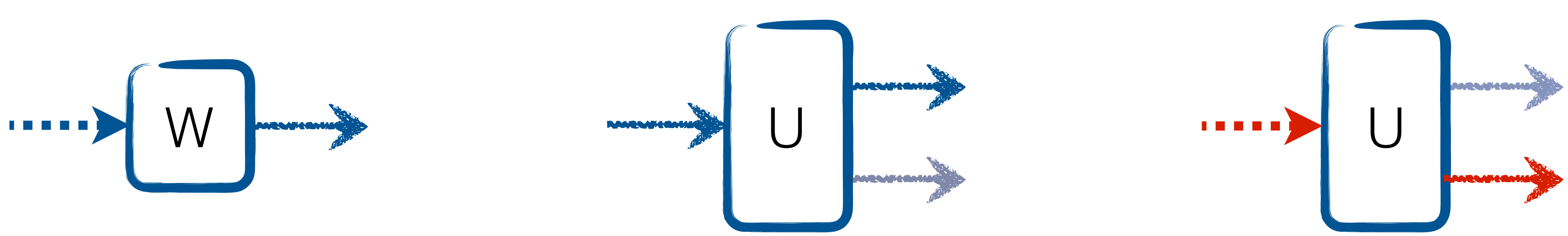
$$z \dashrightarrow \boxed{W} \longrightarrow W(z) = \varphi_z$$

2. Regard it as a quantum channel

$$\rho \longrightarrow \boxed{\mathcal{N}} \longrightarrow \mathcal{N}(\rho) = \sum_z \langle z|\rho|z\rangle \varphi_z$$

3. Consider *complementary* output for *conjugate* input

$$W^{\perp}(x) := \mathcal{N}^{\sharp}(|\tilde{x}\rangle\langle\tilde{x}|)$$



Dual channel: Alternate view

Obtain both outputs from single quantum state:

$$|\psi\rangle_{ABC_1C_2} \propto \sum_z |z\rangle_A \, |z\rangle_{C_1} \, |\varphi_z\rangle_{BC_2}$$

Entropies: $H(Z|W(Z)) = H(Z_A|B)_\psi$

$$H(X|W^\perp(X)) = H(X_A|C_1C_2)_\psi$$

Examples: duals of classical channels

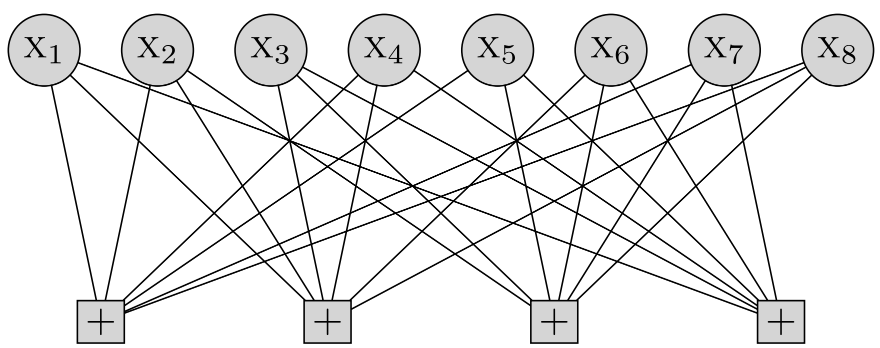
$$\mathrm{BEC}(p)^\perp = \mathrm{BEC}(1-p)$$

$$\mathrm{BSC}(\delta)^\perp = W : x \to Z^x|\eta\rangle$$

$$|\eta\rangle = \sqrt{\delta}|0\rangle + \sqrt{1-\delta}|1\rangle$$

- Dual channels & entropies
- Use in polar codes & belief propagation decoding
- Privacy amplification & source coding
- Duality in classical BP

Polar codes & belief propagation



Polar codes & BP utilize two convolutions:

$$W \circledast W(z) = \varphi_z \otimes \varphi_z$$

$$W \boxast W(z) = \tfrac{1}{2}[\varphi_0 \otimes \varphi_z + \varphi_1 \otimes \varphi_{1 \oplus z}]$$

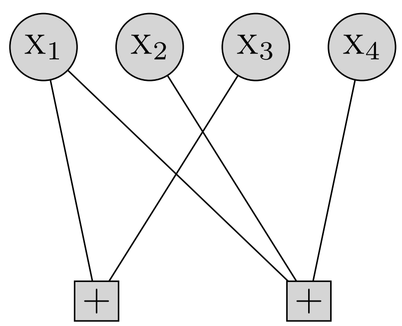
Convolutions are interchanged by duality

$$(W_1 \circledast W_2)^{\perp} = W_1^{\perp} \boxast W_2^{\perp}$$

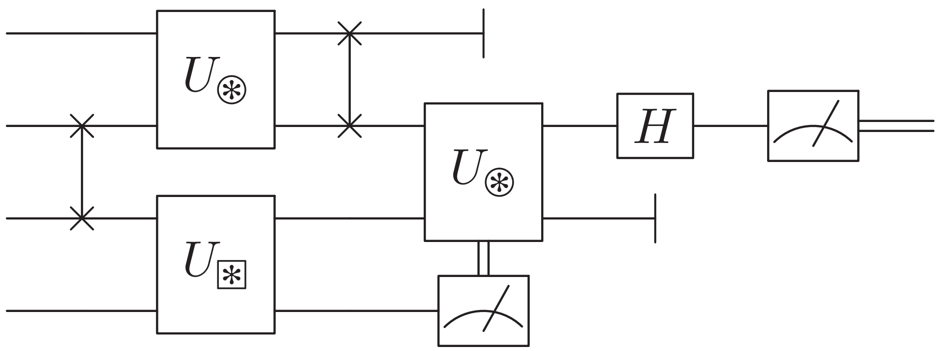
polarization rates to high & low entropy are equivalent

Duality in quantum BP decoding

R, NJP 19, 072001 (2017)



How to construct $U_{\circledast}$ and $U_{\boxast}$?



$$W \circledast W(z) = \varphi_z \otimes \varphi_z$$

$$W \boxast W(z) = \tfrac{1}{2}[\varphi_0 \otimes \varphi_z + \varphi_1 \otimes \varphi_{1\oplus z}]$$

$$W_1 \boxast W_2 = (W_1^{\perp} \circledast W_2^{\perp})^{\perp}$$

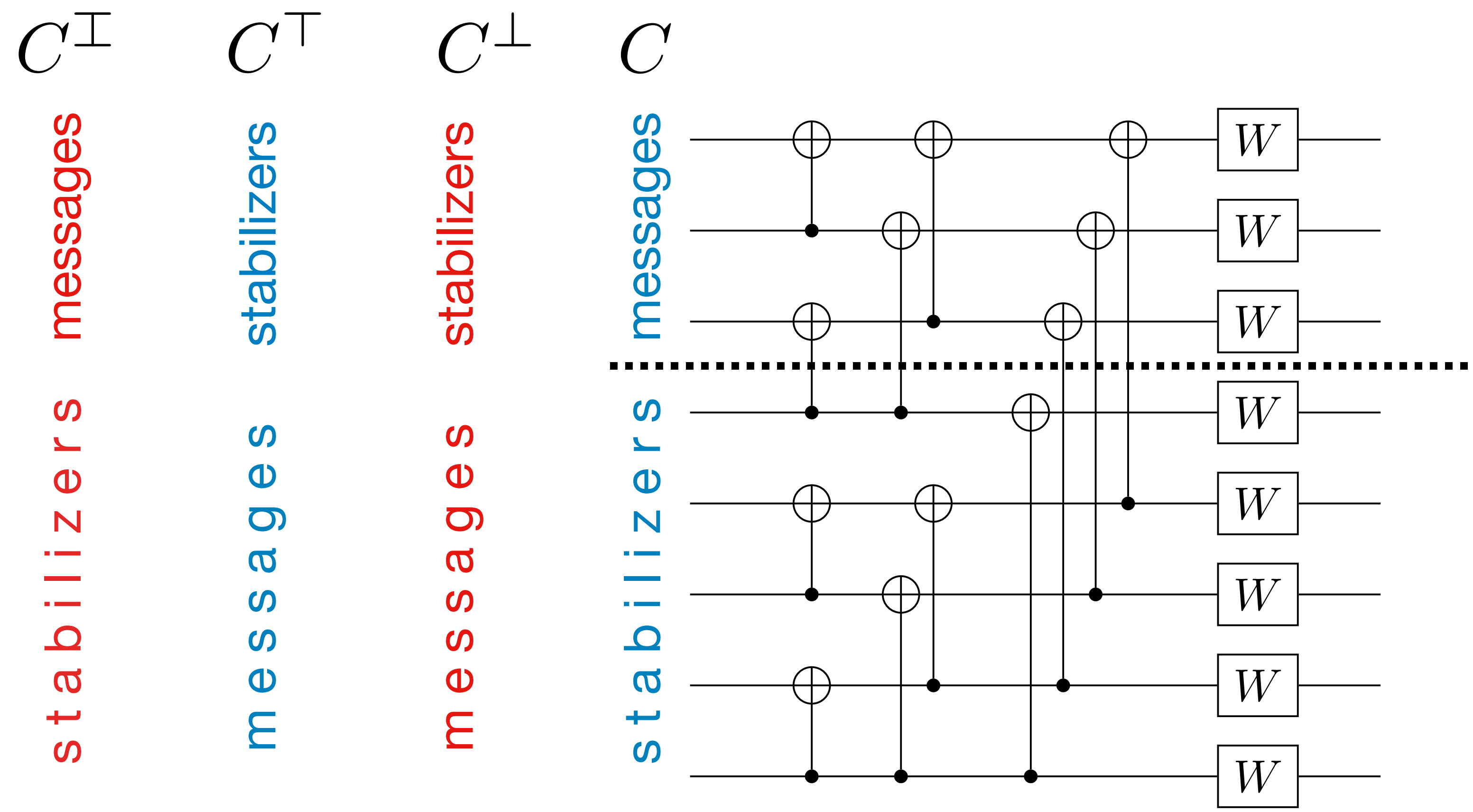
pure state

BSC

Inherit structure for pure state channel BP from BSC

- Dual channels & entropies
- Use in polar codes & belief propagation decoding
- Privacy amplification & source coding
- Duality in classical BP

Dual codes



X basis Z basis (reversible) encoding circuit

$$(W^n \circ E_C)^{\perp} = (W^n)^{\perp} \circ R_{C^{\bot\!\!\!\top}}$$

E_C: encoder for C $R_{C^{\bot\!\!\!\top}}$: random encoding into $C^{\bot\!\!\!\top}$

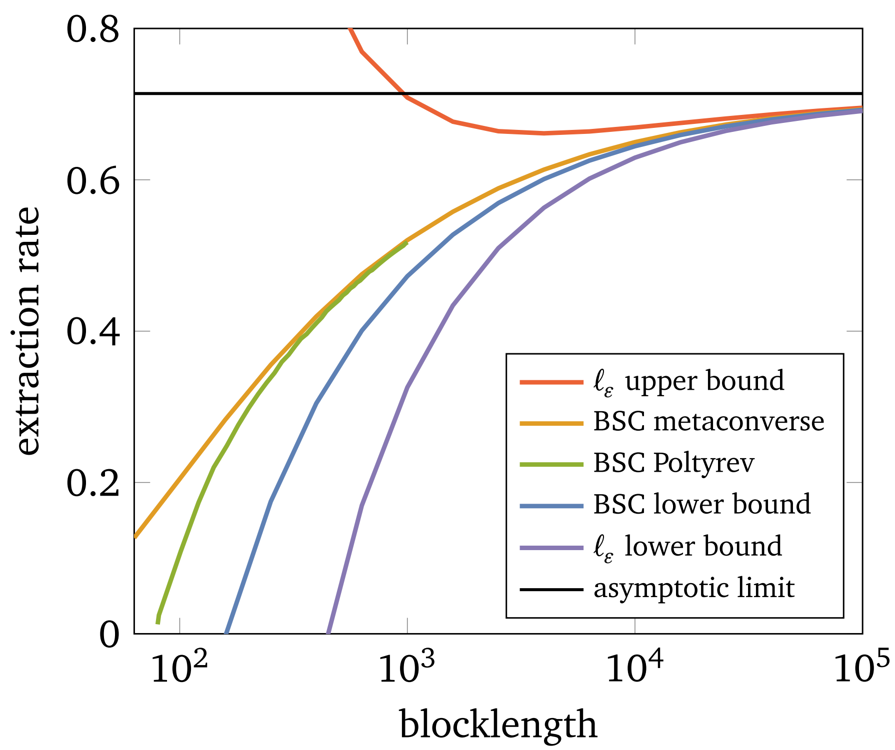
Error correction & privacy amplification

$m_\epsilon(W)$: optimal code size, error ϵ

$\ell_\epsilon(W)$: optimal key length, dist. ϵ

$$\ell_\epsilon(W^\perp) = m_{\epsilon^2}(W)$$

Example: randomness extraction



$\delta = 0.05$ $\epsilon = 10^{-6}$

Duality of source and channel coding

"The statement and proof of the two preceding results contain a curious duality between erased/known symbols in source coding and known/erased symbols in channel coding."

— Martinian & Yedidia, Allerton 2004

"curious duality" had to be!

Dual channel lets us convert channel coding into source coding

R, arXiv:1708.05685 [quant-ph]

- Dual channels & entropies
- Use in polar codes & belief propagation decoding
- Privacy amplification & source coding
- Duality in classical BP

EXIT functions

entropic function used in analysis of linear codes, particularly in message-passing algorithms

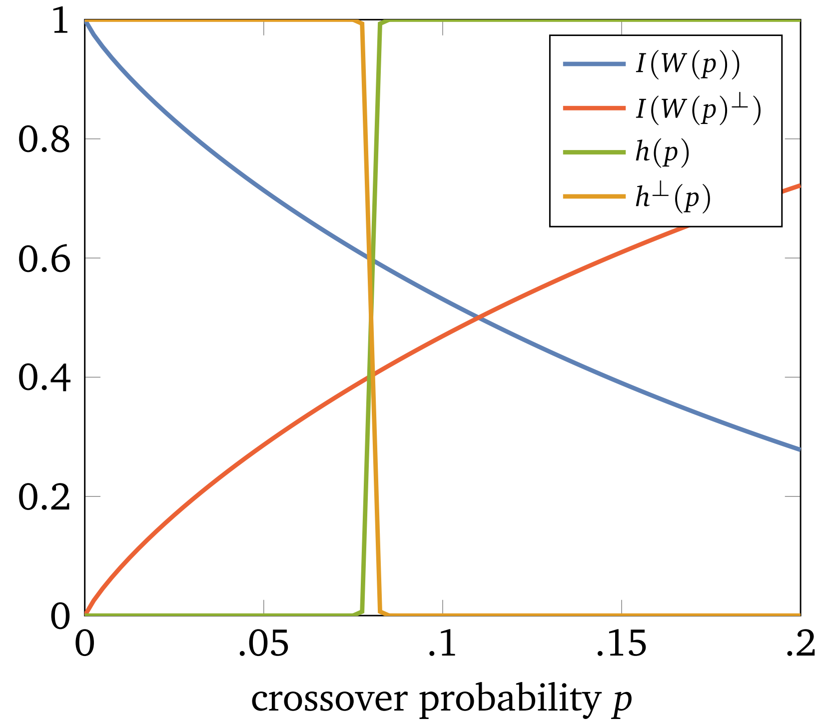
related to reliability of decoding

ensemble of randomly chosen codeword + channel output

$$\Xi_{\mathsf{H}}(W,C) := \frac{1}{n}\sum_{i=1}^{n} \mathsf{H}(Z_i|B^n_{\sim i})$$

entropy of the i-th bit given all but the i-th output

$$\Xi_{\mathsf{H}}(W,C) + \Xi_{\mathsf{H}^\perp}(W^\perp,C^\perp) = 1$$



use to show given code achieves capacity

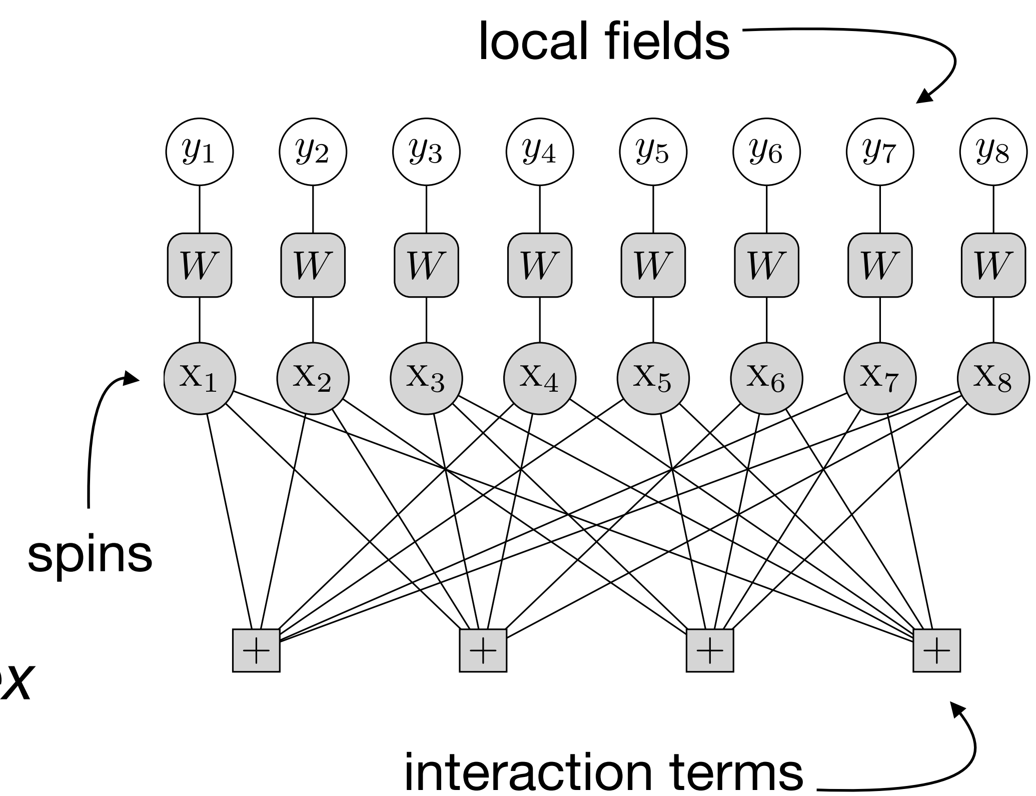
threshold must occur at capacity

so, only need to show threshold exists

Duality in classical BP

When does classical BP work?

- spin model: Correlations decay ⇒ BP is good
- error-probability ~ temperature



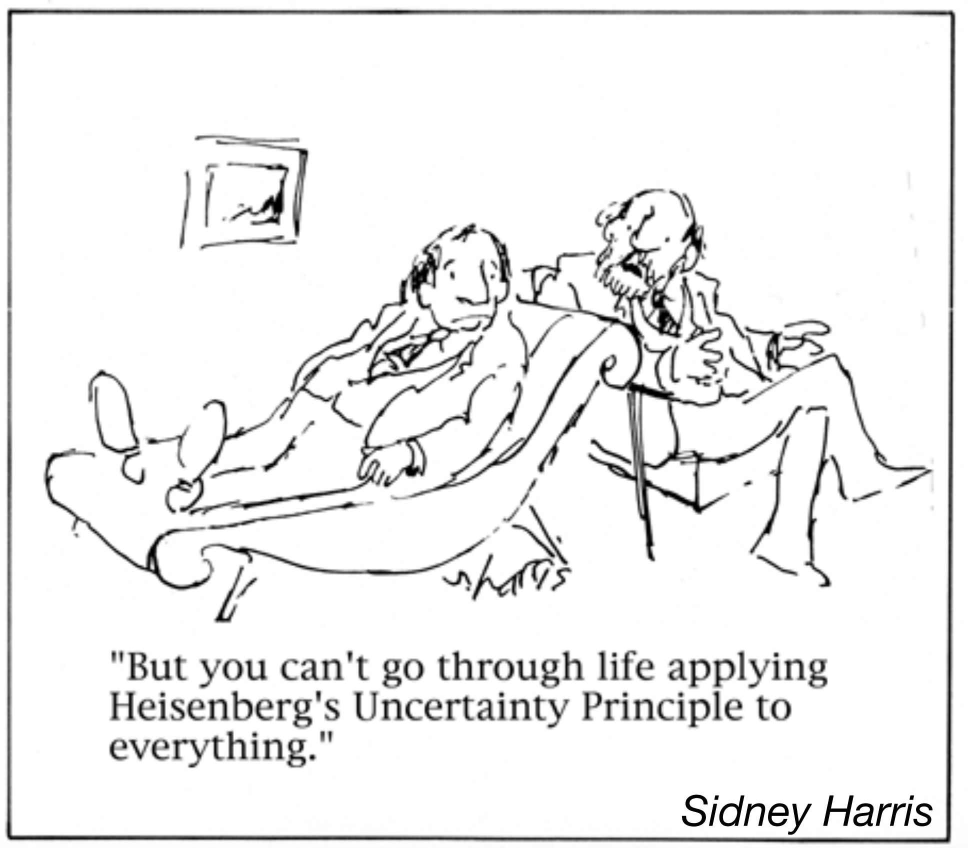
Dualize (Fourier) to find correlation decay:

- low temperature ⇔ high temperature
- works for BEC; generally local fields are *complex*

The dual channel is involved somehow…

- local field is related to likelihood function of channel
- complex local field is precisely the “quantum likelihood” of the dual channel!
- goal: understand appearance of dual channel; study classical BP

Summary



Sure you can!
At least, to crypto and coding

Many more open questions.

Is there a duality relation for BP?

IEEE Trans Inf Theory 64, 577 (2018)

arXiv:1708.05685 [quant-ph]

Proof of equality in uncertainty relation

1. Definitions

$$D(\rho, \sigma) := \mathrm{Tr}[\rho(\log \rho - \log \sigma)]$$

$$H(A|B)_\rho = \log |A| - D(\rho_{AB}, \pi_A \otimes \rho_B)$$

$$H(Z_A|B)_\rho = \log |A| - D(\bar{\rho}_{AB}, \pi_A \otimes \rho_B)$$

$$H(X_A|B)_\rho = \log |A| - D(\tilde{\rho}_{AB}, \pi_A \otimes \rho_B)$$

2. Entropy of purification

$$H(X_A|B)_\rho - H(X_A|C)_\rho = H(A|B)_\rho$$

chain rules, plus

$$H(B|X_A)_\rho = H(C|X_A)_\rho$$

for pure ρ_{ABC}

3. General chain rule

$$D(\rho_{AB}, \pi_A \otimes \rho_B) = \underbrace{D(\rho_{AB}, \tilde{\rho}_{AB}) + D(\tilde{\rho}_{AB}, \pi_A \otimes \rho_B)}_{}$$

$$\mathrm{Tr}[\rho_{AB} \log \rho_{AB} - \rho_{AB} \log \tilde{\rho}_{AB} + \tilde{\rho}_{AB} \log \tilde{\rho}_{AB} - \tilde{\rho}_{AB} \log(\pi_A \otimes \rho_B)]$$

4. Monotonicity

$$D(\rho_{AB}, \sigma_{AB}) \geq D(\bar{\rho}_{AB}, \bar{\sigma}_{AB})$$

$$\begin{aligned} H(X_A|B)_\rho - H(A|B)_\rho &= D(\rho_{AB}, \tilde{\rho}_{AB}) \\ &\geq D(\bar{\rho}_{AB}, \pi_A \otimes \rho_B) \\ &= \log |A| - H(Z_A|B)_\rho \end{aligned}$$

$$\Rightarrow \quad H(X_A|B)_\rho + H(Z_A|B)_\rho \geq \log |A| + H(A|B)_\rho$$

$$\Rightarrow \quad H(X_A|C)_\rho + H(Z_A|B)_\rho \geq \log |A|$$