Complementarity in quantum information processing

Joseph M. Renes

ETH zürich

Complementarity addresses the question

What is the nature of light?

momentum fluctuations due to radiation pressure, Einstein 1909

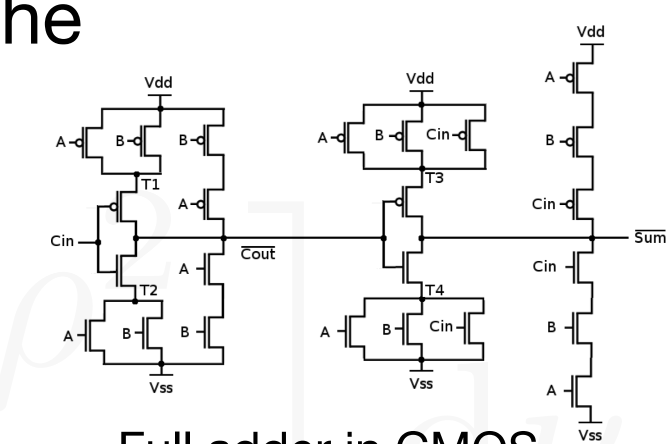
$$\overline{\Delta^2} = \frac{1}{c}\left[h\rho\nu + \frac{c^3\rho^2}{8\pi\nu^2}\right]\mathrm{d}\nu\, f\tau$$

first term: particle picture   second term: wave picture

"It is therefore my opinion that the next stage in the development of theoretical physics will bring us a theory of light that can be understood as a **kind of fusion of the wave and emission theories of light**."

Complementarity also applies to information processing

Regard classical info processing protocol as the "particle" description of a quantum process.



Full adder in CMOS

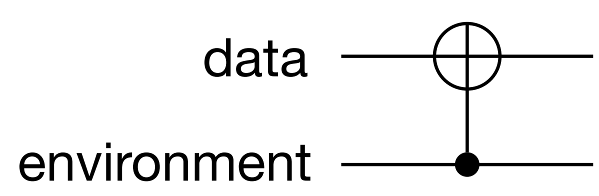
Q: What does the "wave" description tell us about the original protocol?

A: Security!

amplitude

σ_Z basis

phase



σ_X basis

Leakage of amplitude information is equivalent to phase errors

Outline

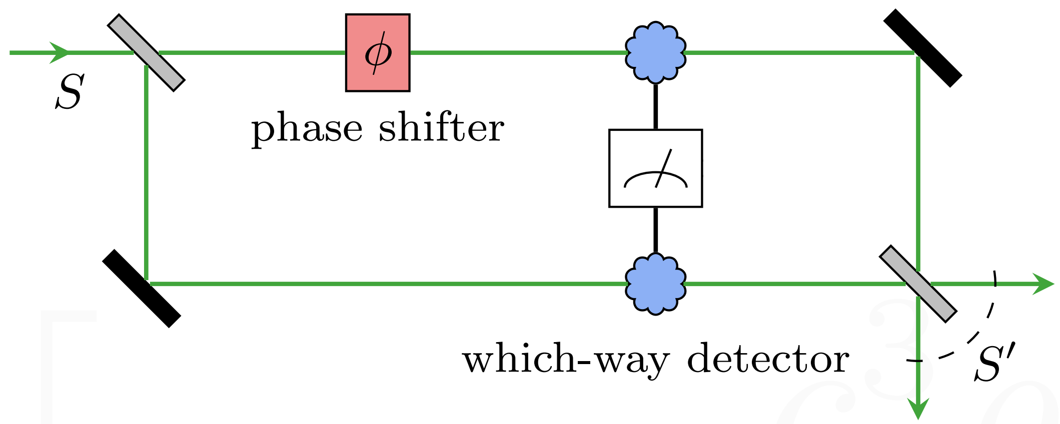
Quantifying complementarity via uncertainty games

Entropic formulations

Applications to QKD and QEC

Complementarity of the MZ interferometer

"particle" observable:
well-defined path



"wave" observable:
well-defined interference

"particle" state:
eigenvector of σ_z

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

"wave" state:
eigenvector of σ_x

wave states are superpositions of particle states and vice versa

---

Classical protocol ~ "particle" description:

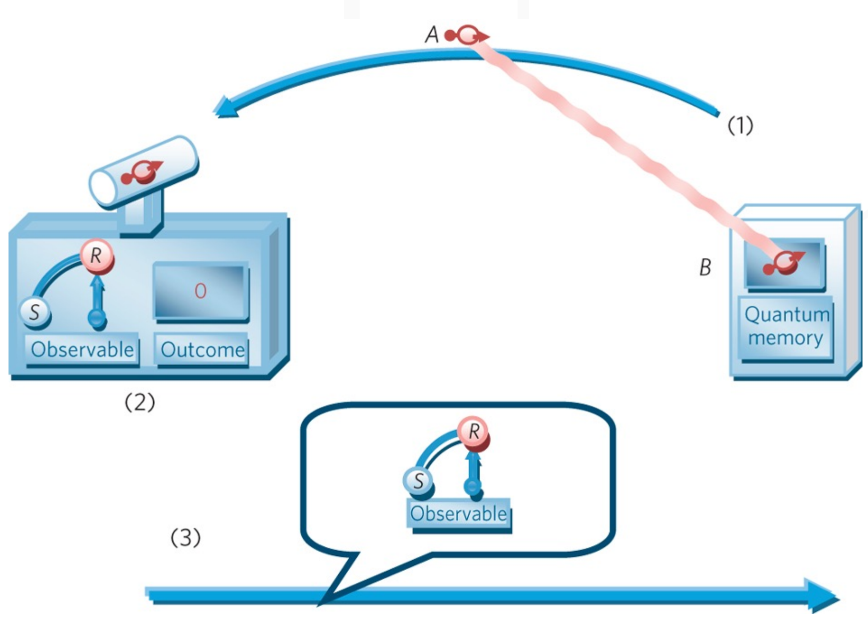
— Associate bit values with "particle" properties
— Measuring σ_z gives a classical RV
— Track only quantum evolution of σ_z

$$0 \leftrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \qquad 1 \leftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

Quantifying complementarity: Uncertainty games

Uncertainty principle: Cannot *simultaneously* know complementary values

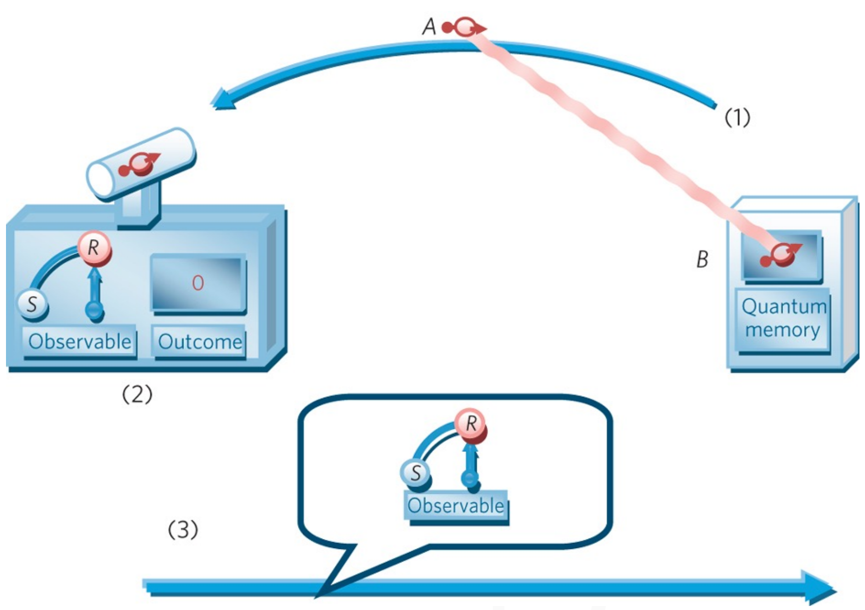
Game:



Alice makes 1 of 2 complementary measurements; Bob tries to guess.

Can Bob win?

Quantifying complementarity: Uncertainty games



Alice makes 1 of 2 complementary measurements; Bob tries to guess.

Version T

1. Bob prepares qubit, sends to Alice
2. Bob announces guess for *both* measurements

4. Alice randomly measures, tells Bob.

Bob has to guess at both

Cannot always win

Version B

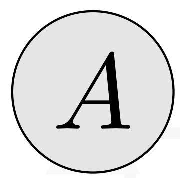
1. Bob prepares qubit, sends to Alice
2. Alice commits to one measurement,
3. Alice asks for guess, Bob delivers.
4. Alice measures, tells Bob.

Bob has to be ready to guess either

Can win: use entanglement

New entropic uncertainty relations

Maassen & Uffink 1988



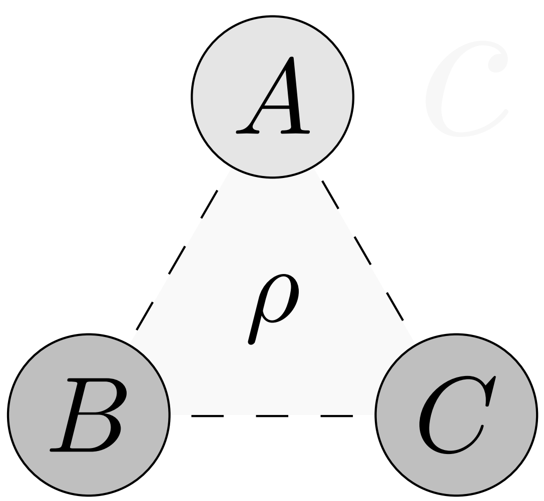
$$H(X_A)_\rho + H(Z_A)_\rho \geq \log \frac{1}{c}$$

$$c = \max_{j,k} |\langle \psi_j | \varphi_k \rangle|^2$$

With side information:

R & Boileau, PRL 103, 020402 (2009)

Berta, Christandl, Colbeck, R, Renner, NatPhys 6, 659 (2010)



Bipartite $H(X_A|B)_\rho + H(Z_A|B)_\rho \geq \log \frac{1}{c} + H(A|B)_\rho$

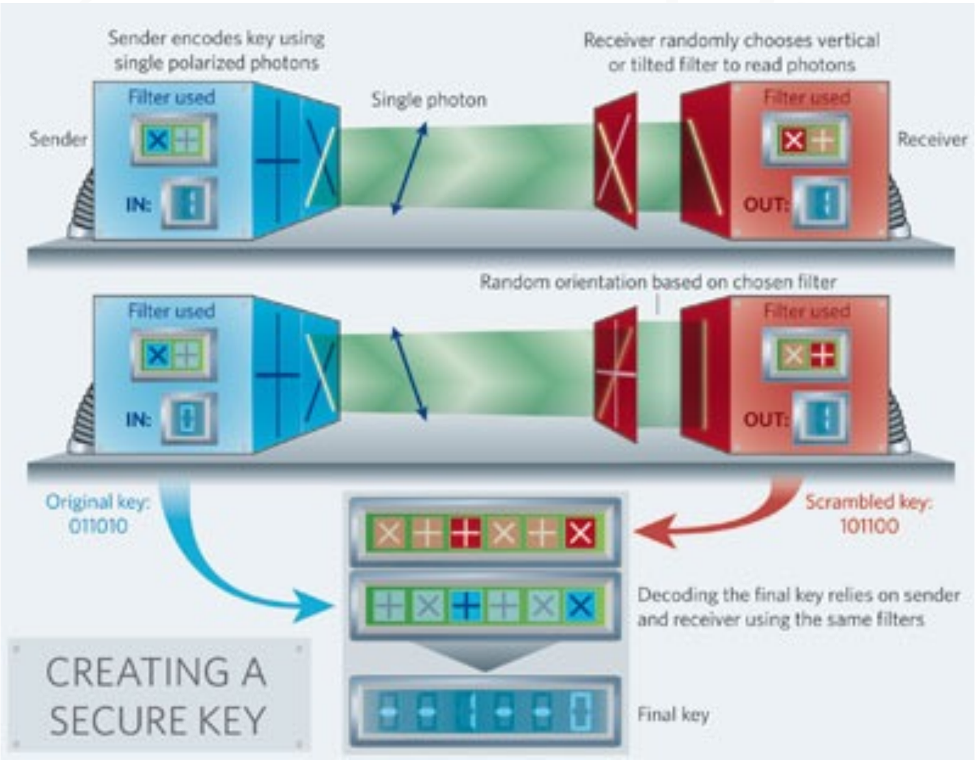
Tripartite $H(X_A|C)_\rho + H(Z_A|B)_\rho \geq \log \frac{1}{c}$

Applications: quantum communication and cryptography

Use in quantum cryptography

Secret key creation: need bound on Eve's info

$$H(X_A|C)_\rho + H(Z_A|B)_\rho \geq \log \frac{1}{c}$$



In BB84 QKD:
one basis generates the key,
the other tests for leakage

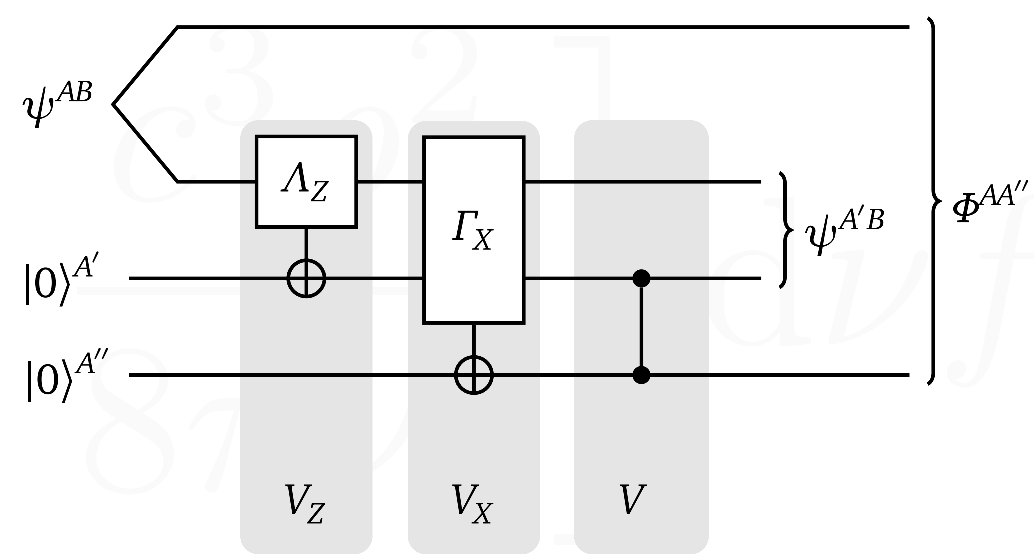
The possibility of testing is what makes quantum crypto "quantum"

Use in quantum error correction

$$H(X_A|B)_\rho + H(Z_A|B)_\rho \geq \log\frac{1}{c} + H(A|B)_\rho$$

Decode "amplitude" then "phase"

Renes & Boileau PRA 78, 032335 (2008)



Uses:

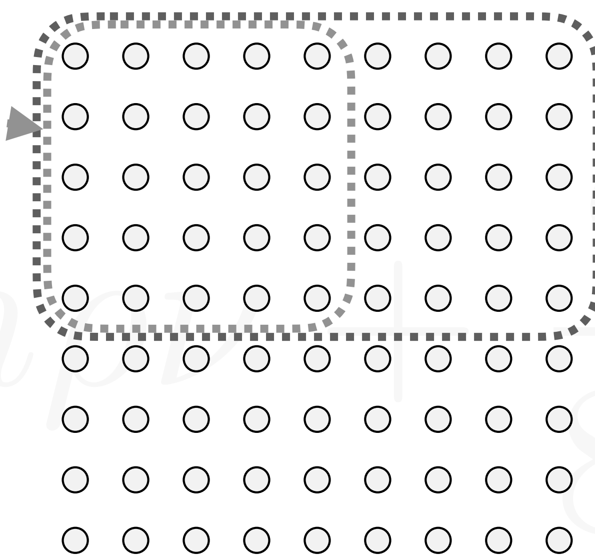
1. Structured decoder for *arbitrary* channels @ capacity
2. Channel-adapted decoders
3. Quantum polar codes

Good *small* codes for near-term use

Choice of code & decoder has huge impact on performance

Bacon-Shor code
& adapted Clifford decoder

Piedrafita and R, PRL 119, 250501 (2017)



surface code & MWPM decoder

Petrović, ETH Master's thesis, 2017

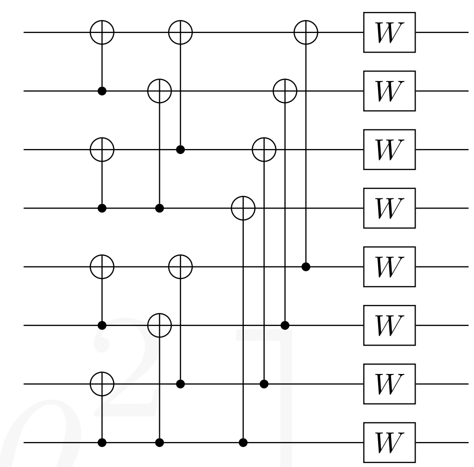
Physical qubits subject to
amplitude damping noise

Complementarity breaks problem down into easier pieces

Efficient & high-rate quantum codes

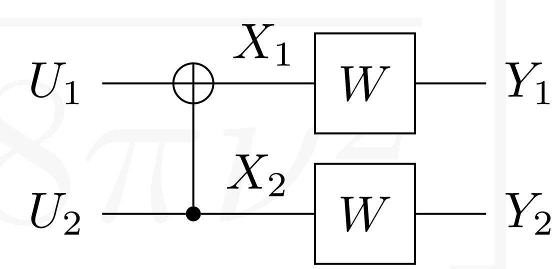
Polar codes, Arıkan 2009:

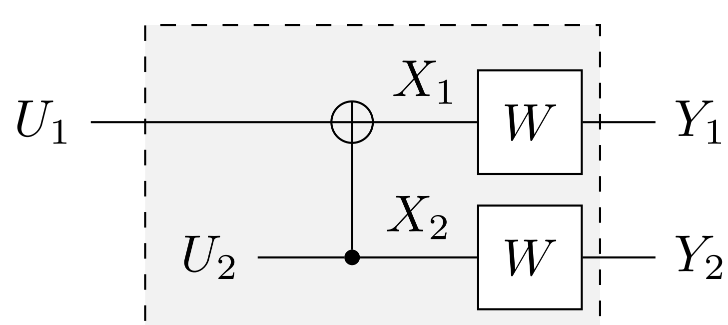
- first *efficient* classical ECC to achieve capacity
- encoding: recursive use of CNOT gate



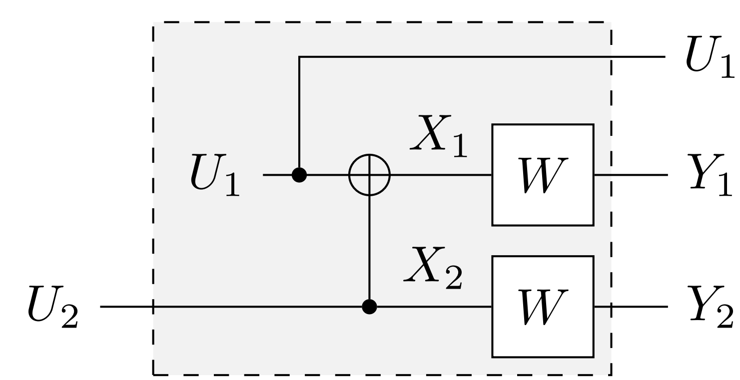
Construction:

- combine 2 channels with CNOT,
- split into better and worse,
- repeat till channels *polarize*



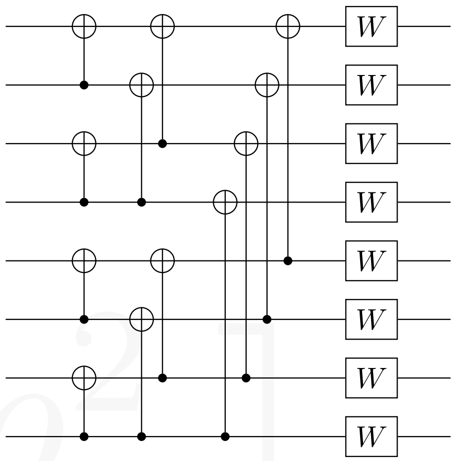


worse channel



better channel

Efficient & high-rate quantum codes

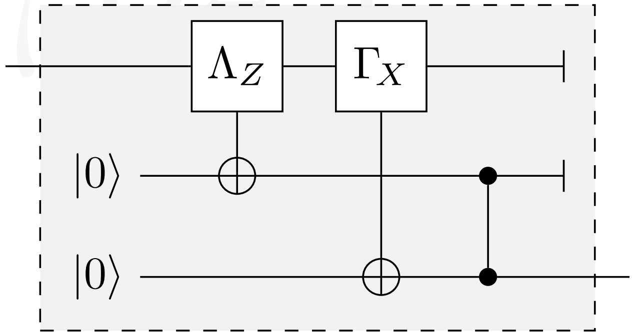


Polar codes, Arıkan 2009:

- first *efficient* classical ECC to achieve capacity
- encoding: recursive use of CNOT gate

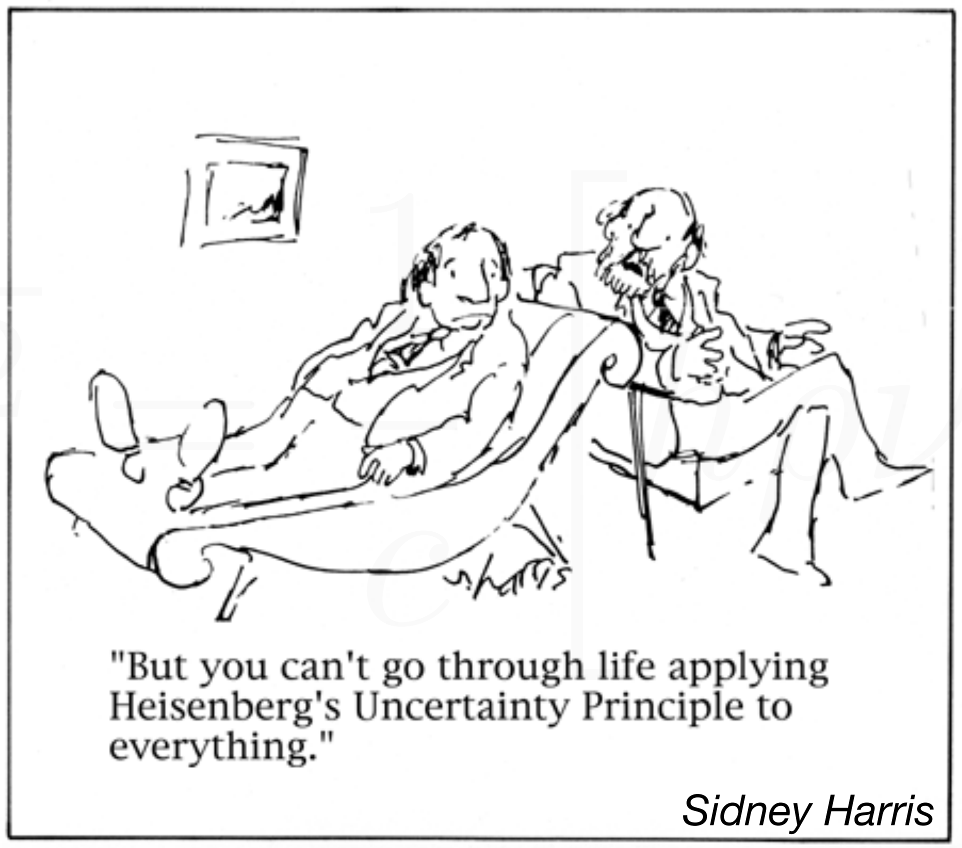
Quantum version:

- polarization of both amplitude and phase
- build quantum decoder from classical
- efficient, high-rate codes for Pauli & erasure
- “alignment” of polar codes



R, Dupuis, Renner, PRL 109, 050504 (2012); QIP 2012
R & Wilde, IEEE TIT 60, 2090 (2014)
R, Sutter, Dupuis, Renner, IEEE TIT 61, 6395 (2015)
R, Sutter, Hassani, IEEE JSAC 34, 224 (2016)

Summary



Sure you can!
At least, to crypto and coding

$$\overline{\Delta^2} = \frac{1}{c}\left[h\rho\nu + \frac{c^3\rho^2}{8\pi\nu^2}\right]\mathrm{d}\nu\, f\tau$$