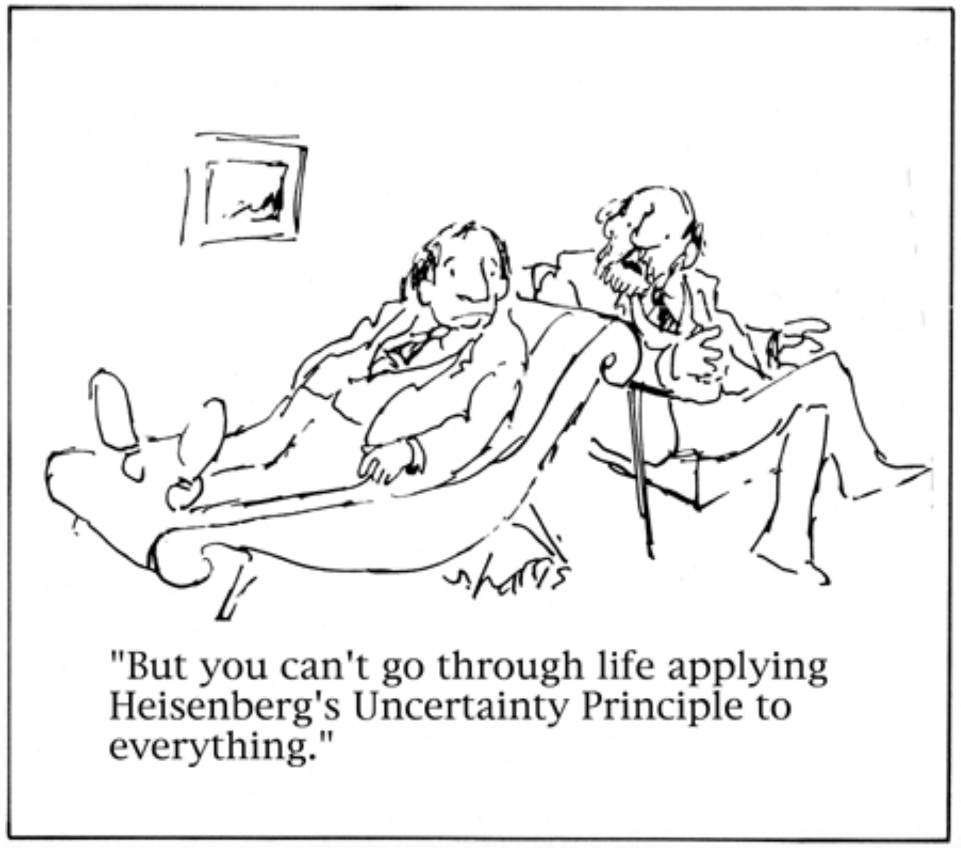


Operational uncertainty relations and their uses

Joseph M. Renes
Institute of Theoretical Physics
ETH zürich

Quantum Incompatibility 2017

arXiv: 1612.02051

Quantum 1, 20 (2017)

JMR, Volkher B. Scholz, and Stefan Huber

29 August 2017

Background & (my) motivation

while building quantum error correcting codes:

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

a kind of preparation uncertainty relation

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

generalized to min/max; used in QKD:

$$H_{\min}(X_A|B)_\rho + H_{\max}(Z_A|C)_\rho \geq 1$$

Tomamichel, Renner PRL 106, 110506 (2011)

only works on average; want a *channel* statement like:

if Bob could determine X input perfectly,
then Eve gets same output for every Z input

Classical leakage resilience from fault-tolerant quantum computation

Felipe G. Lacerda[*1,2], Joseph M. Renes[†1], and Renato Renner[‡1]

arXiv 1404.7516

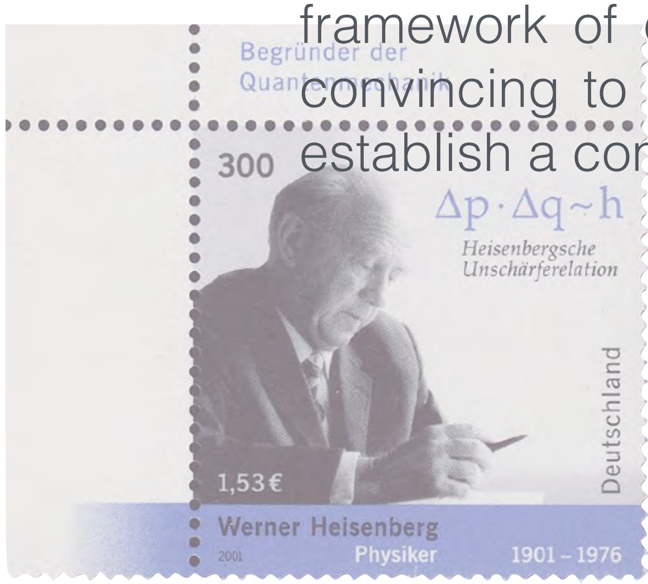
Outline

- Difficulty of formulating uncertainty relations
- Simple notions of error and disturbance
- Results
- Uses
- A look at the proof

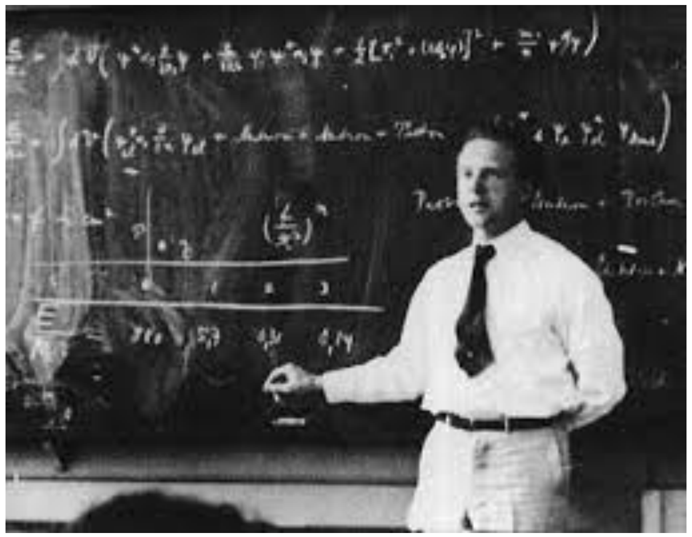
Difficulties

Since our talks often continued till long after midnight, and did not produce a satisfactory conclusion despite protracted efforts over several months, both of us became utterly exhausted and rather tense. Hence Bohr decided in February 1927 to go skiing in Norway, and I was quite glad to be left behind in Copenhagen, where I could think about these hopelessly complicated problems undisturbed. I now concentrated all my efforts on the mathematical representation of the electron path in the cloud chamber, and when **I realized fairly soon that the obstacles before me were quite insurmountable, I began to wonder whether we might not have been asking the wrong sort of question all along.** But where had we gone wrong? The path of the electron through the cloud chamber obviously existed; one could easily observe it. The mathematical framework of quantum mechanics existed as well, and was much too convincing to allow for any changes. Hence it ought to be possible to establish a connection between the two, hard though it appeared to be.

- Heisenberg, “Physics and Beyond”

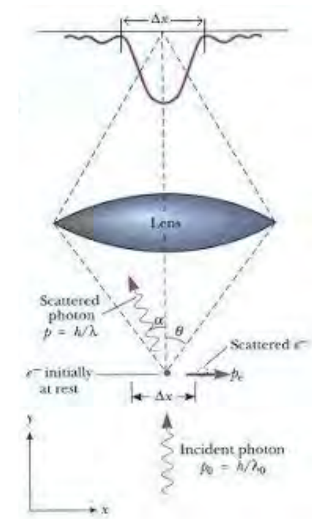


Mathematical



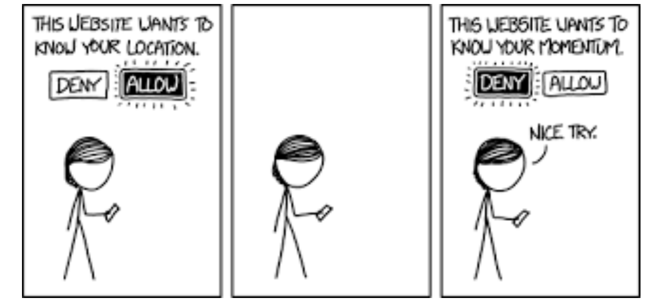
need machinery to describe
general measurements

Most uncertainty relations
are model-dependent



Now we have POVMs, quantum instruments,
completely-positive maps, etc…

Conceptual



Uncertainty *principle* makes it hard to formulate meaningful uncertainty *relations*

Error

Usual recipe: Compare true value with measured result.

- Only eigenstates have a “true value”
- Compare distributions instead?
  No simultaneous measurement!

Disturbance

Usual recipe: Compare true value with new value.

- No “true value”
- What, precisely, is disturbed?

The theory is intruding on the *definition* of error & disturbance…

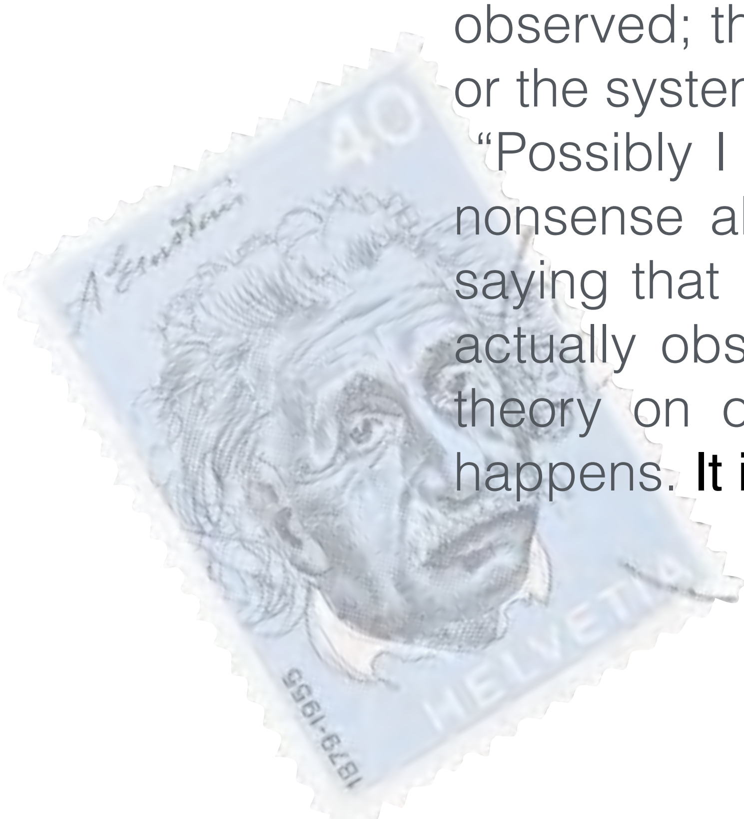
Operational notions of error and disturbance

"We cannot observe electron orbits inside the atom," I must have replied, "but the radiation which an atom emits during discharges enables us to deduce the frequencies and corresponding amplitudes of its electrons. After all, even in the older physics wave numbers and amplitudes could be considered substitutes for electron orbits. Now, since a good theory must be based on directly observable magnitudes, I thought it more fitting to restrict myself to these, treating them, as it were, as representatives of the electron orbits."

"But you don't seriously believe," Einstein protested, "that none but observable magnitudes must go into a physical theory?"

"Isn't that precisely what you have done with relativity?" I asked in some surprise. "After all, you did stress the fact that it is impermissible to speak of absolute time, simply because absolute time cannot be observed; that only clock readings, be it in the moving reference system or the system at rest, are relevant to the determination of time."

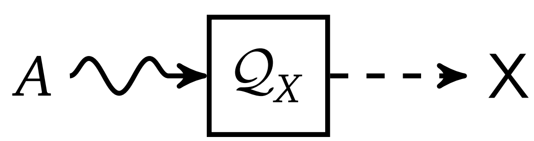
"Possibly I did use this kind of reasoning," Einstein admitted, "but it is nonsense all the same. Perhaps I could put it more diplomatically by saying that it may be heuristically useful to keep in mind what one has actually observed. But on principle, it is quite wrong to try founding a theory on observable magnitudes alone. In reality the very opposite happens. **It is the theory which decides what we can observe.**"



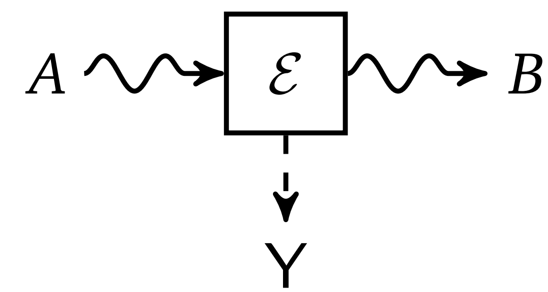
- Heisenberg, "Physics and Beyond"

Distinguishability

ideal measurement



real device



How well can the real apparatus be distinguished from the ideal apparatus, *in any experiment whatsoever?*

$$P_{\text{guess}}(\mathcal{E}_{\text{real}}, \mathcal{E}_{\text{ideal}})$$

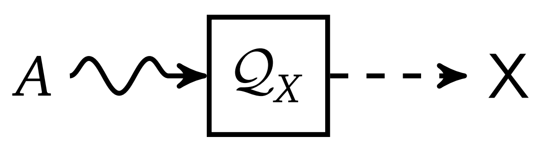
$$\delta(\mathcal{E}_{\text{real}}, \mathcal{E}_{\text{ideal}}) = 2P_{\text{guess}}(\mathcal{E}_{\text{real}}, \mathcal{E}_{\text{ideal}}) - 1$$

$$\delta(\mathcal{E}_{\text{real}}, \mathcal{E}_{\text{ideal}}) = \tfrac{1}{2}\|\mathcal{E}_{\text{real}} - \mathcal{E}_{\text{ideal}}\|_\diamond$$

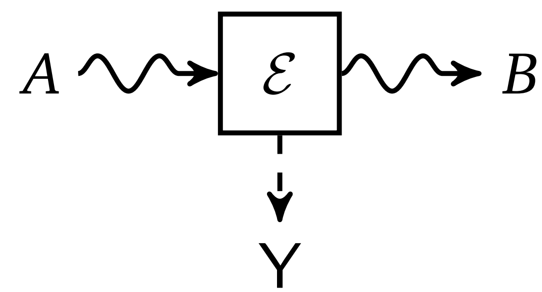
need entangled inputs…

Measurement error

ideal measurement

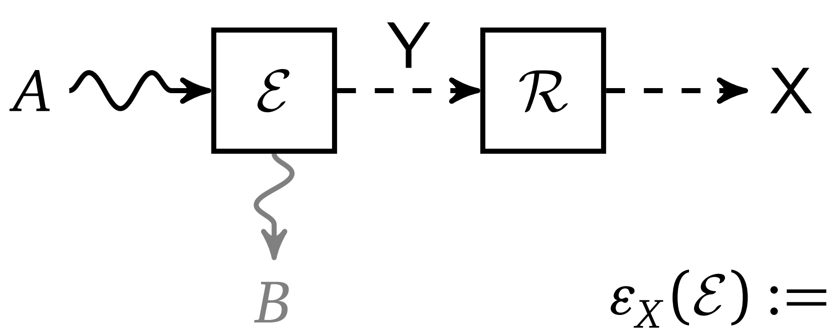


real device

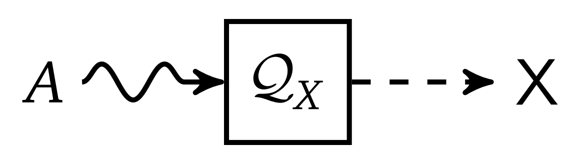


$$P_{\text{guess}}(\mathcal{Q}_X, \mathcal{E}) = 1$$

fix:



$\approx_{\varepsilon_X}$



$$\varepsilon_X(\mathcal{E}) := \inf_{\mathcal{R}} \delta(\mathcal{Q}_X, \mathcal{E}\mathcal{R}\mathcal{T}_B).$$

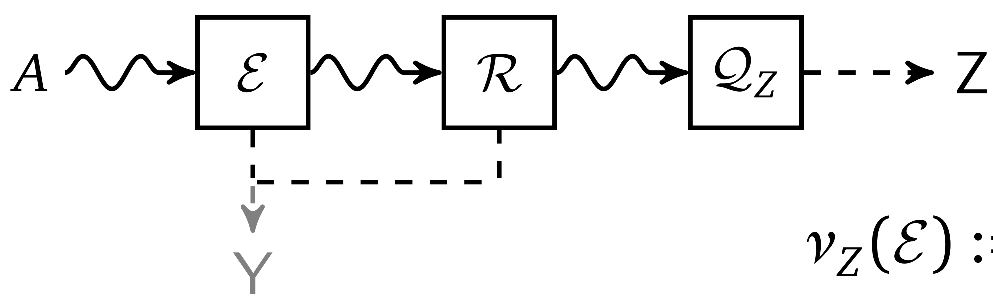
the entire optimization is a semidefinite program

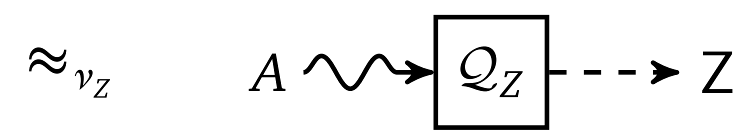
Disturbance

What, exactly, is disturbed by measurement?

Two answers: past preparation or future measurement

Disturbance to future measurement of Z





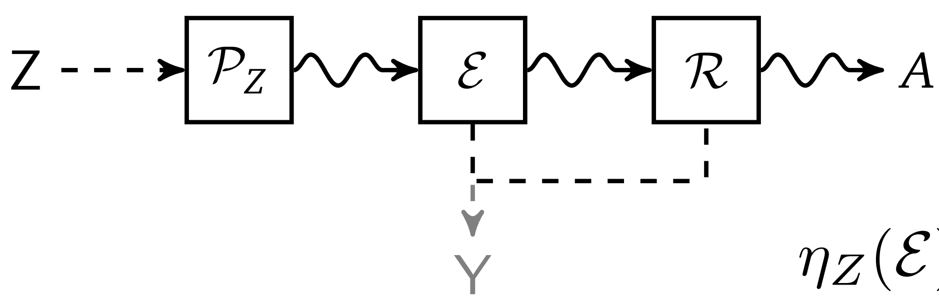
$$\nu_Z(\mathcal{E}) := \inf_{\mathcal{R}} \delta(\mathcal{Q}_Z, \mathcal{E}\mathcal{R}\mathcal{T}_{\mathsf{Y}}\mathcal{Q}_Z)\,.$$

related to joint measureability

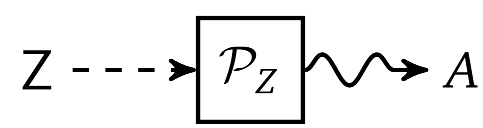
any joint measurement can be decomposed into a sequential measurement

Preparation disturbance

“merit”

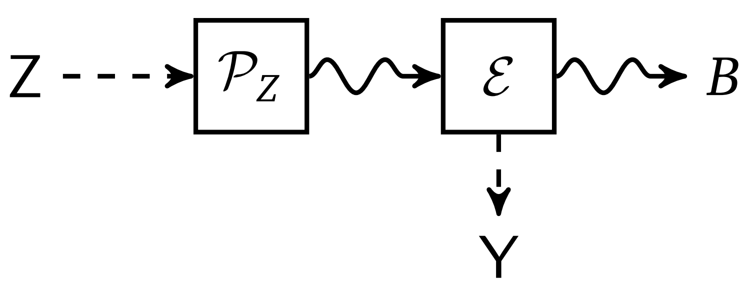


$\approx_{\eta_Z}$

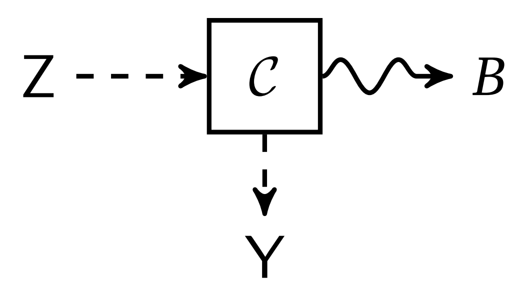


$$\eta_Z(\mathcal{E}) = \inf_{\mathcal{R}} \delta(\mathcal{P}_Z, \mathcal{P}_Z \mathcal{E} \mathcal{R} \mathcal{T}_Y)$$

“demerit”



$\approx_{\frac{d-1}{d} - \widehat{\eta}_Z}$



$$\hat{\eta}_Z(\mathcal{E}) = \frac{d-1}{d} - \inf_{\mathcal{C}:\text{const.}} \delta(\mathcal{P}_Z \mathcal{E}, \mathcal{C})$$

Position & momentum

ideal preparation and measurement have finite precision: σ_Q, σ_P

we assume Gaussian noise in the quantum instrument

but we still use idealized distinguishability in error and disturbance

$$\varepsilon_X(\mathcal{E}) := \inf_{\mathcal{R}} \delta(\mathcal{Q}_X, \mathcal{E}\mathcal{R}\mathcal{T}_B).$$

this setup is inconsistent; precision-limited distinguishability should be smaller.

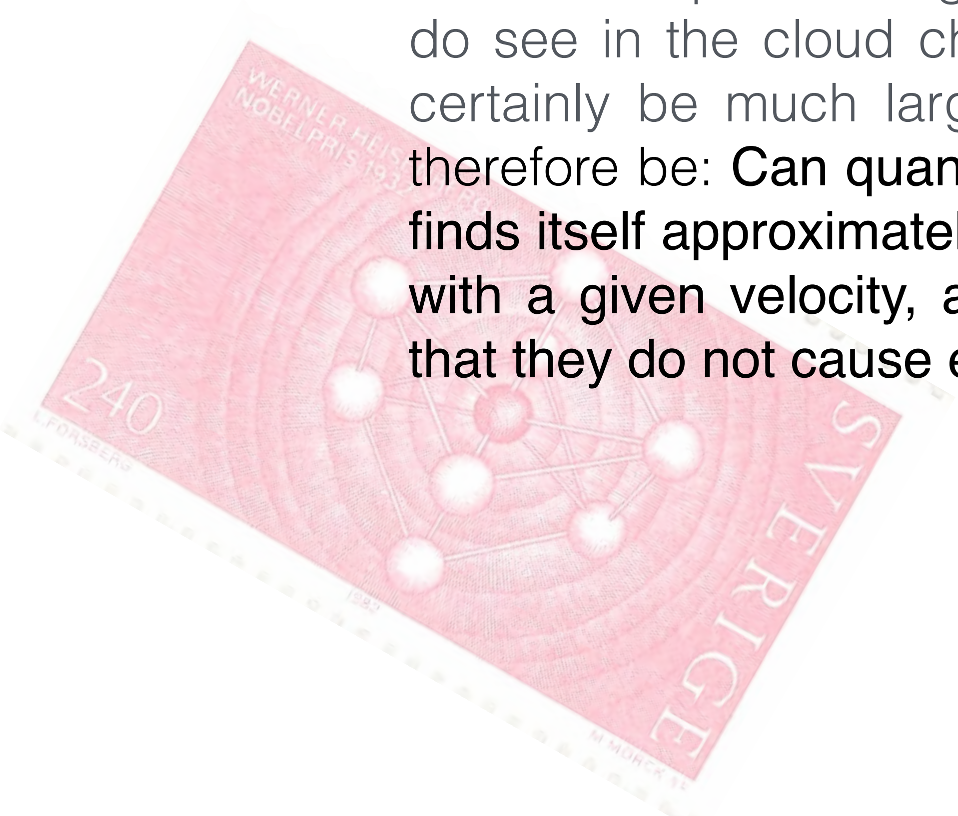
but the proof goes through easily

New uncertainty relations

It must have been one evening after midnight when I suddenly remembered my conversation with Einstein and particularly his statement, “It is the theory which decides what we can observe.” I was immediately convinced that the key to the gate that had been closed for so long must be sought right here. I decided to go on a nocturnal walk through Faelled Park and to think further about the matter.

We had always said so glibly that the path of the electron in the cloud chamber could be observed. But perhaps what we really observed was something much less. Perhaps we merely saw a series of discrete and ill-defined spots through which the electron had passed. In fact, all we do see in the cloud chamber are individual water droplets which must certainly be much larger than the electron. The right question should therefore be: Can quantum mechanics represent the fact that an electron finds itself approximately in a given place and that it moves approximately with a given velocity, and can we make these approximations so close that they do not cause experimental difficulties?

- Heisenberg, “Physics and Beyond”



Measures of complementarity

apply error and disturbance measures

$$c_M(X,Z) = \nu_Z(\mathcal{Q}_X) \qquad\qquad c_P(X,Z) = \eta_Z(\mathcal{Q}_X)$$

$$= \varepsilon_Z(\mathcal{Q}_X) \qquad\qquad \widehat{c}_P(X,Z) = \widehat{\eta}_Z(\mathcal{Q}_X)$$

$$c_M(X,Z), c_P(X,Z) \geq 1 - \tfrac{1}{d}\sum_x \max_z |\langle\varphi_x|\theta_z\rangle|^2$$

$$\widehat{c}_P(X,Z) \geq \tfrac{d-1}{d} - \tfrac{1}{d}\max_z \tfrac{1}{2}\sum_x \left|\tfrac{1}{d} - \langle\varphi_x|\theta_z\rangle|^2\right|$$

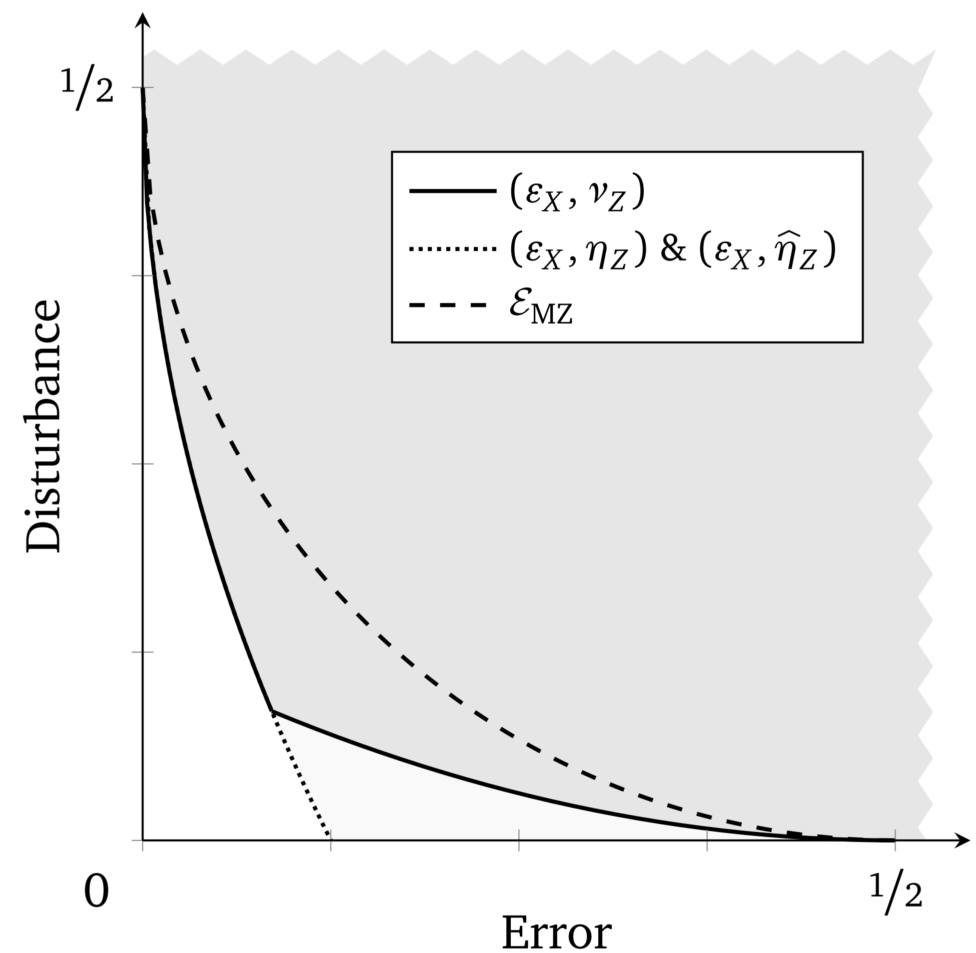
same for conjugate observables

potentially large gap otherwise

Relations for finite dimensions

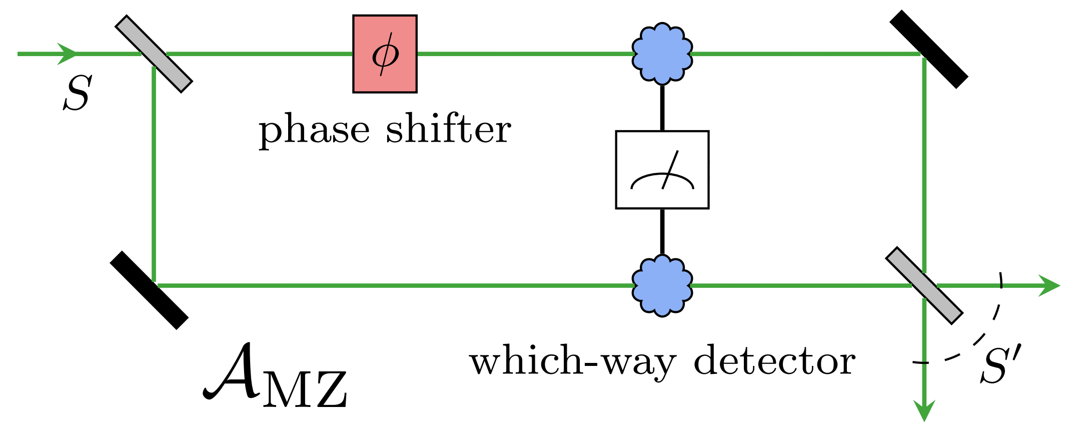
$$\sqrt{2\varepsilon_X(\mathcal{E})} + \nu_Z(\mathcal{E}) \geq c_M(X,Z) \quad \textit{and}$$
$$\varepsilon_X(\mathcal{E}) + \sqrt{2\nu_Z(\mathcal{E})} \geq c_M(Z,X)\,.$$

$$\sqrt{2\varepsilon_X(\mathcal{E})} + \eta_Z(\mathcal{E}) \geq c_P(X,Z) \quad \textit{and}$$
$$\sqrt{2\varepsilon_X(\mathcal{E})} + \widehat{\eta}_Z(\mathcal{E}) \geq \widehat{c}_P(X,Z)\,.$$



Connection to wave-particle duality

Mach-Zehnder interferometer



Particle-like property:
Path distinguishability from WW detector

Wave-like property:
Interference fringe visibility at output

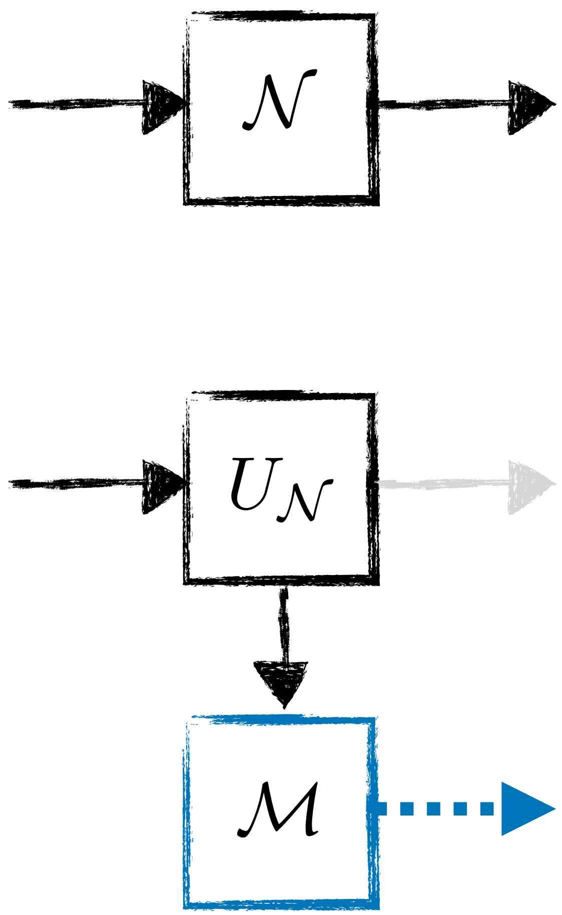
Quantitative complementarity inequality $V^2 + D^2 \leq 1$

BG Englert, PRL 77, 2154 (1996)

$$\varepsilon_X(\mathcal{A}_{\rm MZ}) = \tfrac{1}{2}(1-D) \qquad \eta_Z(\mathcal{A}_{\rm MZ}) \geq \tfrac{1}{2}(1-V)$$

$$(1-2\varepsilon_X(\mathcal{A}_{\rm MZ}))^2 + (1-2\eta_Z(\mathcal{A}_{\rm MZ}))^2 \leq 1$$

Applications: crypto



channel to Eve

we would like Z inputs to be inaccessible

dilate and measure

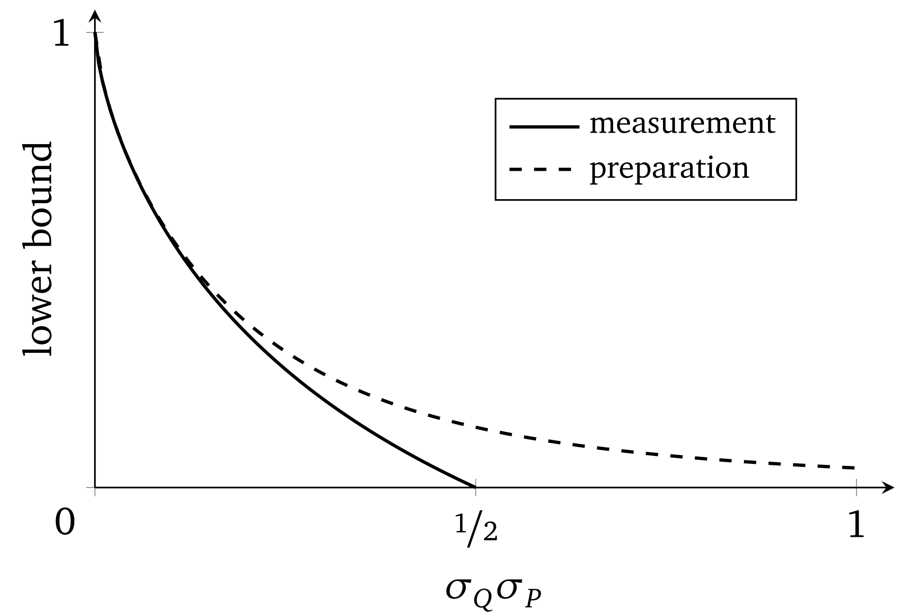
if this is close to an ideal X measurement,
then we have security

$$\delta(P_Z \mathcal{N}, \mathcal{C}) \leq \sqrt{2\varepsilon_X}$$

Position momentum

$$\left.\begin{array}{r}\sqrt{2\varepsilon_Q(\mathcal{E})}+\nu_P(\mathcal{E})\\ \varepsilon_Q(\mathcal{E})+\sqrt{2\nu_Q(\mathcal{E})}\end{array}\right\}\geq$$

$$\sqrt{2\varepsilon_Q(\mathcal{E})}+\eta_P(\mathcal{E})\geq$$



Consider approximate position measurement of an approximate momentum state, followed by approximate momentum measurement

$$\sigma_P^{\text{in}} \longrightarrow \sigma_Q \longrightarrow \sigma_P^{\text{out}}$$

by uncertainty principle, expect change in momentum $\sim 1/\sigma_Q$

to detect change in momentum, need $\sigma_P^{\text{out}} \ll \sigma_P^{\text{in}} + 1/\sigma_Q$

for measurement disturbance

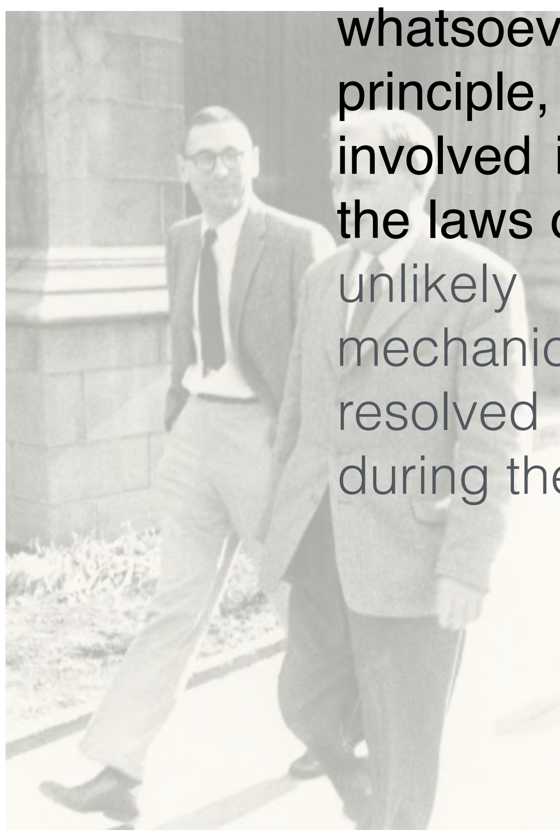
$$\sigma_P^{\text{out}} = 2/\sigma_Q$$ ✗

for preparation disturbance

$$\sigma_P^{\text{in}} = 2/\sigma_Q$$ ✓

Proof technique

A brief calculation after my return to the Institute showed that one could indeed represent such situations mathematically, and that the approximations are governed by what would later be called the uncertainty principle of quantum mechanics: the product of the uncertainties in the measured values of the position and momentum (i.e., the product of mass and velocity) cannot be smaller than Planck's constant. This formulation, I felt, established the much-needed bridge between the cloud chamber observations and the mathematics of quantum mechanics. **True, it had still to be proved that any experiment whatsoever was bound to set up situations satisfying the uncertainty principle, but this struck me as plausible a priori, since the processes involved in the experiment or the observation had necessarily to satisfy the laws of quantum mechanics.** On this presupposition, experiments are unlikely to produce situations that do not accord with quantum mechanics. “It is the theory which decides what we can observe.” I resolved to prove this by calculations based on simple experiments during the next few days.



- Heisenberg, “Physics and Beyond”

Stinespring dilation and its continuity

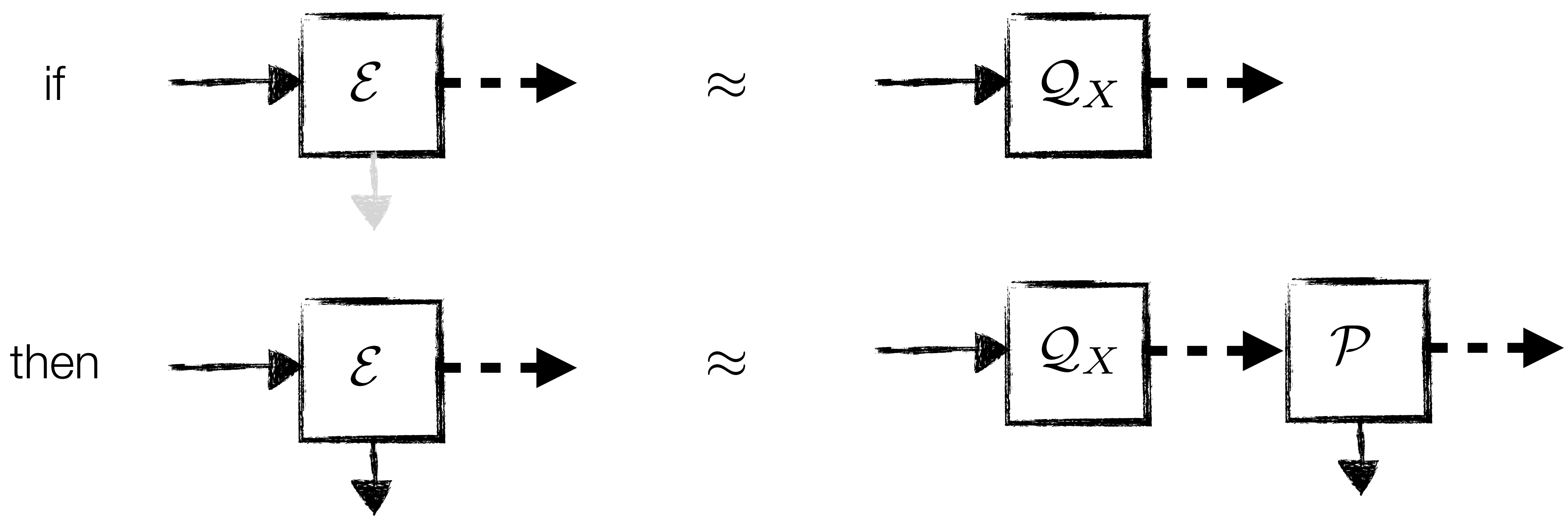
dilate any channel to an isometry

isometries close if channels indistinguishable

$$\mathcal{E} \approx \mathcal{F} \quad \Leftrightarrow \quad UW_{\mathcal{E}} \approx W_{\mathcal{F}}$$

diamond norm — infinity norm

using this we can infer behavior of quantum output from behavior of classical output



Lemma 2. *For any apparatus $\mathcal{E}_{A \to YB}$ there exists a channel $\mathcal{F}_{XA \to YB}$ such that $\delta(\mathcal{E}, \mathcal{Q}'_X \mathcal{F}) \leq \sqrt{2\varepsilon_X(\mathcal{E})}$, where $\mathcal{Q}'_X$ is a quantum instrument associated with the measurement $\mathcal{Q}_X$. Furthermore, if $\mathcal{Q}_X$ is a projective measurement, then there exists a state preparation $\mathcal{P}_{X \to YB}$ such that $\delta(\mathcal{E}, \mathcal{Q}_X \mathcal{P}) \leq \sqrt{2\varepsilon_X(\mathcal{E})}$.*

Now use triangle inequality

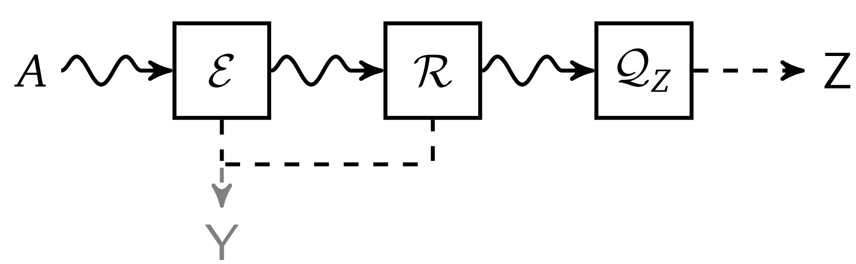
want to show

$$\sqrt{2\varepsilon_X(\mathcal{E})} + \nu_Z(\mathcal{E}) \geq c_M(X,Z) \quad and$$
$$\varepsilon_X(\mathcal{E}) + \sqrt{2\nu_Z(\mathcal{E})} \geq c_M(Z,X)\,.$$

$$\begin{aligned}\delta(\mathcal{Q}_Z, \mathcal{Q}_X\mathcal{P}\mathcal{R}\mathcal{Q}_Z) &\leq \delta(\mathcal{Q}_Z, \mathcal{E}\mathcal{R}\mathcal{Q}_Z) + \delta(\mathcal{E}\mathcal{R}\mathcal{Q}_Z, \mathcal{Q}_X\mathcal{P}\mathcal{R}\mathcal{Q}_Z)\\ &\leq \delta(\mathcal{Q}_Z, \mathcal{E}\mathcal{R}\mathcal{Q}_Z) + \delta(\mathcal{E}, \mathcal{Q}_X\mathcal{P})\\ &= \delta(\mathcal{Q}_Z, \mathcal{E}\mathcal{R}\mathcal{Q}_Z) + \sqrt{2\varepsilon_X(\mathcal{E})}\,.\end{aligned}$$

take infimum over R to get the first inequality

make a joint measurement out of optimal R's in error and disturbance



decompose into Z measurement first
to get the other inequality

position/momentum same,
but harder to evaluate bound

use representation of covariant measurements
and Kennard uncertainty relation

Summary and open questions

- New error-disturbance tradeoff
- formulated using easy-to-interpret quantities;
- applicable to information processing

- tightness in general?
- POVMs?
- precision in P and Q distinguishability