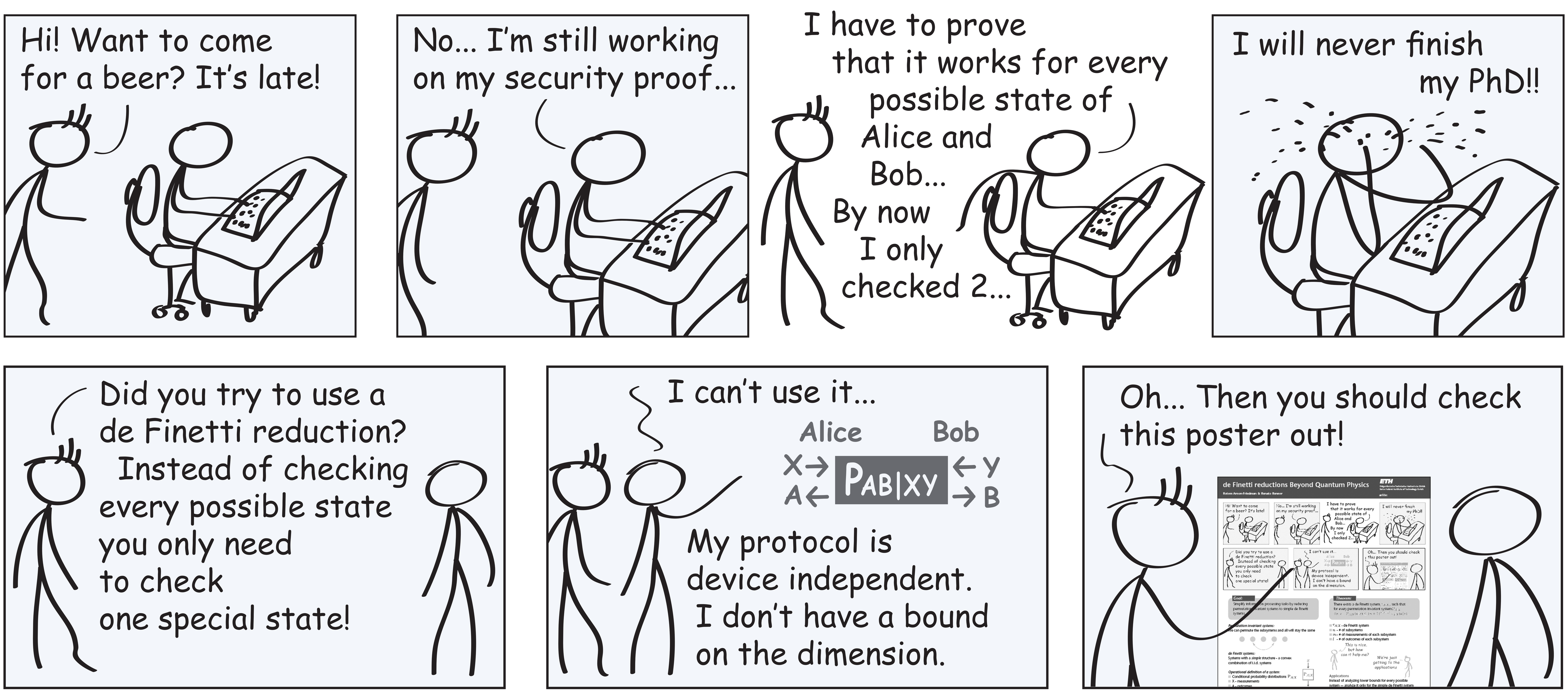
de Finetti Reductions Beyond Quantum Physics

Rotem Arnon-Friedman & Renato Renner

ETH Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

arXiv: 1308.0312

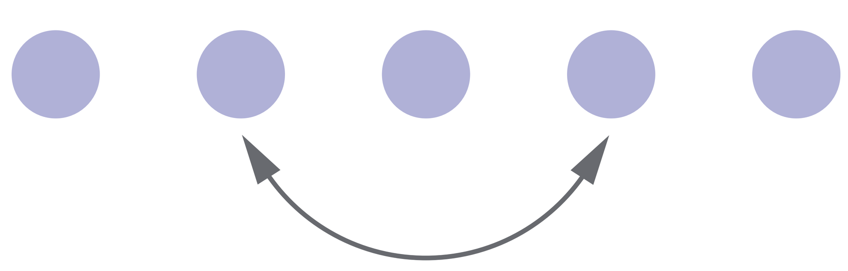


Goal:

Simplify information processing tasks by reducing permutation invariant systems to simple de Finetti systems.

Permutation invariant systems:

We can permute the subsystems and all will stay the same

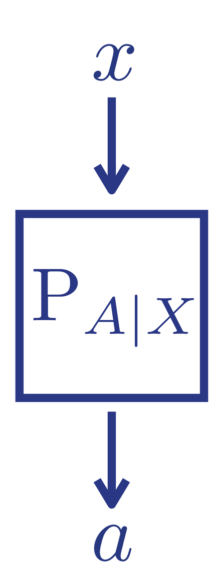


de Finetti systems:

Systems with a ***simple*** structure - a convex combination of i.i.d. systems

Operational definition of a system:

- Conditional probability distributions $\mathrm{P}_{A|X}$
- X - measurements
- A - outcomes
- Describes a larger set of systems than quantum systems



de Finetti reductions for conditional probablitiy distributions

- Reduction from permutation invariant conditional probability distributions to a de Finetti system
- Independent of the *dimension* of the underlying space
- Depends on the *number of measurements and outcomes*
- ***Useful for device independent tasks***

Theorem:

There exists a de Finetti system, $\tau_{A|X}$, such that for every permutation invariant system $\mathrm{P}_{A|X}$

$$\forall a,x \quad \mathrm{P}_{A|X}(a|x) \leq (n+1)^{m(l-1)}\ \tau_{A|X}(a|x)\ .$$

- $\tau_{A|X}$ - de Finetti system
- n - # of subsystems
- m - # of measurements of each subsystem
- l - # of outcomes of each subsystem

Applications

Instead of analyzing lower bounds for every possible system — analyze it only for the simple de Finetti system and "pay" for it with a polynomial factor

Lemma:

Consider a permutation invariant test which interacts with a system $\mathrm{P}_{A|X}$ and outputs "success" or "fail" with some probabilities. Then for every system $\mathrm{P}_{A|X}$

$$\mathrm{Pr}_{\text{fail}}(\mathrm{P}_{A|X}) \leq (n+1)^{m(l-1)}\mathrm{Pr}_{\text{fail}}(\tau_{A|X})\ .$$

More on the arXiv:

- Similar lower bounds on the diamond norm — useful for cryptography
- Better bounds in the presence of symmetries
- ***Example application — simplifying the analysis of CHSH based protocols***

{rotema,renner}@phys.ethz.ch