de Finetti Theorems
Quantum and Beyond

IQI seminar | June 17 2014

arXiv:1308.0312 | de Finetti reductions beyond quantum theory

Rotem Arnon-Friedman & Renato Renner

ETH Zurich

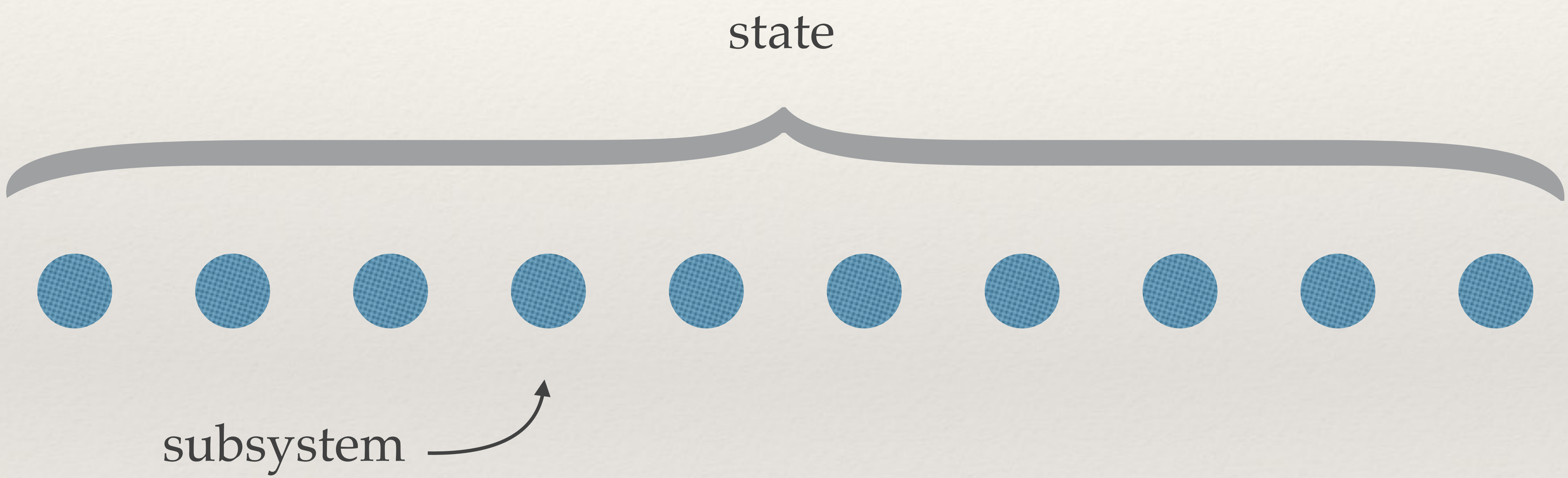
Outline

- The basics
- Quantum family tree
- Device independent de Finetti reductions
  - Motivation
  - Results
  - “Open issues”

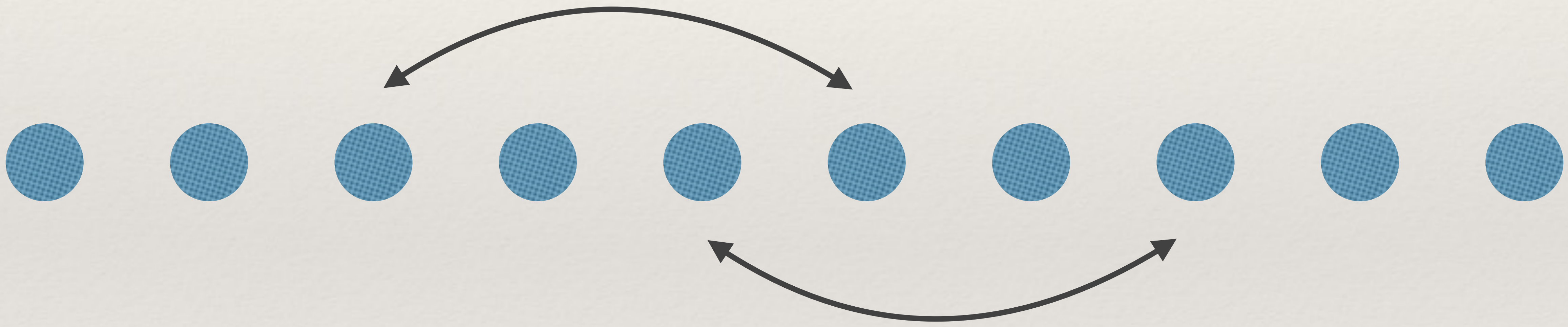
The basics

- Two ingredients:
    1. Permutation invariant states
    2. de Finetti state
- de Finetti theorem — a tool that "connects" the two

Permutation invariance



Permutation invariance



Permutation invariance

- More formally:
  - Quantum: $\rho = \pi \rho \pi^{\dagger}$
  - Probability distribution (PD): $\mathrm{P}\left(a\right) = \mathrm{P}\left(\pi(a)\right)$
  - Conditional PD (CPD): $\mathrm{P}\left(a|x\right) = \mathrm{P}\left(\pi(a)|\pi(x)\right)$

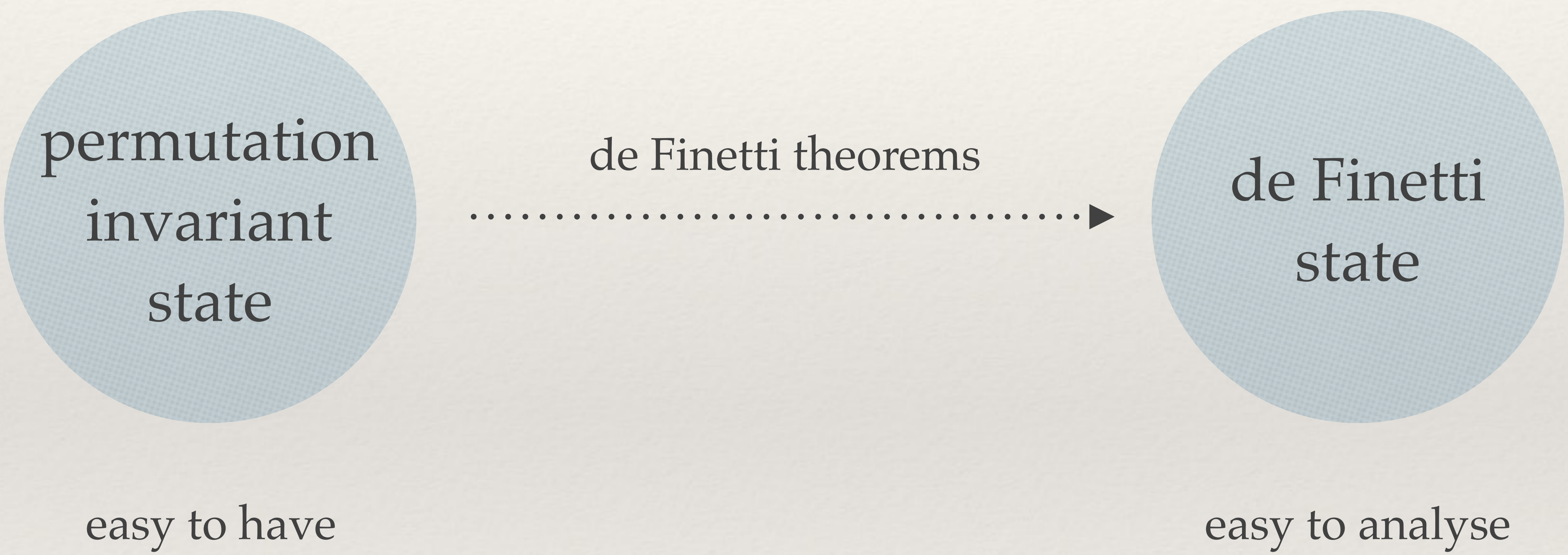
Why permutation invariance?

- Relevant in physics
- Easy to enforce — choose a random permutation

de Finetti state

- Convex combination of i.i.d. states
  - Quantum: $\tau = \int \sigma^{\otimes n} \mathrm{d}\sigma$
  - CPD: $\tau_{A|X} = \int \mathrm{Q}_{A_1|X_1}^{\otimes n} \mathrm{dQ}_{A_1|X_1}$
- Simple structure — easy to handle

de Finetti type theorems



Applications: cryptography, tomography, channel coding, quantum field theory, thermodynamics?

Quantum family tree

de Finetti type theorems

de Finetti reductions

(a.k.a post selection)

- $\rho^k = \pi \rho^k \pi^\dagger$

$\Rightarrow \rho^k \leq (k+1)^{d^2-1} \tau^k$

standard de Finetti theorems

n-exchangeable

- $\rho^k = \pi \rho^k \pi^\dagger$
- $\exists \rho^n :$

$$\rho^n = \pi \rho^n \pi^\dagger$$
$$\rho^k = \mathrm{tr}_{n-k} \rho^n$$

infinitely exchangeable

- $\rho^k = \pi \rho^k \pi^\dagger$
- $\forall n > k, \ \ \exists \rho^n :$

$$\rho^n = \pi \rho^n \pi^\dagger$$
$$\rho^k = \mathrm{tr}_{n-k} \rho^n$$

$\Rightarrow \rho^k = \tau^k$

exact

(poly. error)

$\Rightarrow \|\rho^k - \tau^k\|_1 \leq d^2 k/n$

almost de Finetti

(exp. error)

$\Rightarrow \|\rho^k - \tilde{\tau}^k\|_1 \leq e^{-\Omega(n-k)}$

$\tilde{\tau}^k$ almost de Finetti state

The younger brother

- de Finetti reduction: $\rho \leq (n+1)^{d^2-1}\tau$
- How to apply (intuition):
  - $\mathrm{P}_{\text{fail}}(\rho)$ — failure prob. of the protocol when acting on ρ
  - Reduction: $\mathrm{P}_{\text{fail}}(\rho) \leq (n+1)^{d^2-1}\mathrm{P}_{\text{fail}}(\tau)$

increasing poly. with n

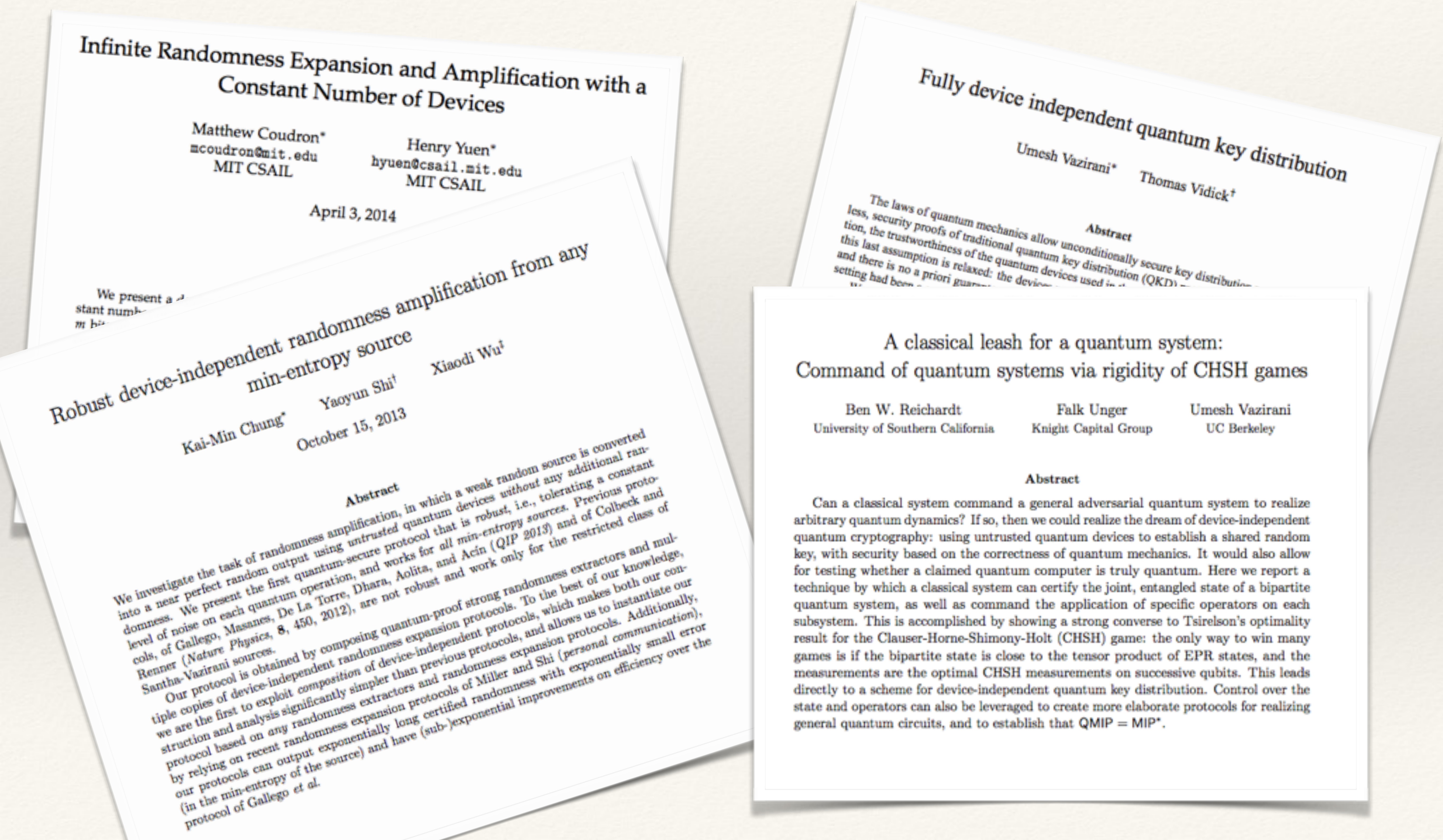
decreasing exp. with n

Well, if it is so useful in QIP protocols…

why don’t we use it in

device independent QIP?

Goal – simplify DI QIP



Infinite Randomness Expansion and Amplification with a Constant Number of Devices

Matthew Coudron*
mcoudron@mit.edu
MIT CSAIL

Henry Yuen*
hyuen@csail.mit.edu
MIT CSAIL

April 3, 2014

Robust device-independent randomness amplification from any min-entropy source

Kai-Min Chung* Yaoyun Shi† Xiaodi Wu‡

October 15, 2013

Abstract

We investigate the task of randomness amplification, in which a weak random source is converted into a near perfect random output using untrusted quantum devices *without* any additional randomness. We present the first quantum-secure protocol that is *robust*, i.e., tolerating a constant level of noise on each quantum operation, and works for *all min-entropy sources*. Previous protocols, of Gallego, Masanes, De La Torre, Dhara, Aolita, and Acín (*QIP 2013*) and of Colbeck and Renner (*Nature Physics*, **8**, 450, 2012), are not robust and work only for the restricted class of Santha-Vazirani sources.

Our protocol is obtained by composing quantum-proof strong randomness extractors and multiple copies of device-independent randomness expansion protocols. To the best of our knowledge, we are the first to exploit *composition* of device-independent protocols, which makes both our construction and analysis significantly simpler than previous protocols, and allows us to instantiate our protocol based on *any* randomness extractors and randomness expansion protocols. Additionally, by relying on recent randomness expansion protocols of Miller and Shi (*personal communication*), our protocols can output exponentially long certified randomness with exponentially small error (in the min-entropy of the source) and have (sub-)exponential improvements on efficiency over the protocol of Gallego *et al.*

Fully device independent quantum key distribution

Umesh Vazirani* Thomas Vidick†

Abstract

A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games

Ben W. Reichardt
University of Southern California

Falk Unger
Knight Capital Group

Umesh Vazirani
UC Berkeley

Abstract

Can a classical system command a general adversarial quantum system to realize arbitrary quantum dynamics? If so, then we could realize the dream of device-independent quantum cryptography: using untrusted quantum devices to establish a shared random key, with security based on the correctness of quantum mechanics. It would also allow for testing whether a claimed quantum computer is truly quantum. Here we report a technique by which a classical system can certify the joint, entangled state of a bipartite quantum system, as well as command the application of specific operators on each subsystem. This is accomplished by showing a strong converse to Tsirelson's optimality result for the Clauser-Horne-Shimony-Holt (CHSH) game: the only way to win many games is if the bipartite state is close to the tensor product of EPR states, and the measurements are the optimal CHSH measurements on successive qubits. This leads directly to a scheme for device-independent quantum key distribution. Control over the state and operators can also be leveraged to create more elaborate protocols for realizing general quantum circuits, and to establish that QMIP = MIP*.

The concept of DI

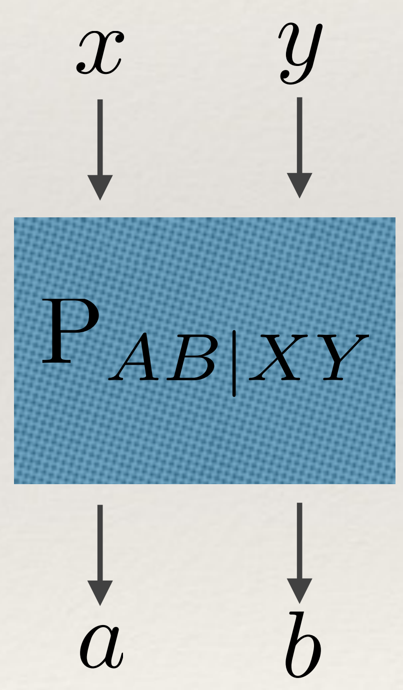
- Motivation:
  - Bridge the gap between theory and experiment
  - Assume less about the physical systems and measurements
- Extreme case: use only observed statistics
- Possible due to Bell inequalities — certificate of non-locality

Framework – CPD

- Conditional probability distributions describe the operational behaviour of a physical system under measurements
- State $\mathrm{P}_{A|X}$
- X — measurements
- A — outcomes
- $\mathrm{P}_{A|X}(a|x)$

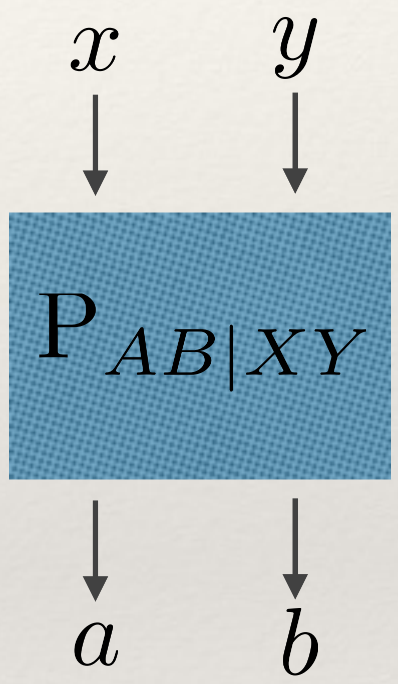
Framework – CPD

- Conditional probability distributions describe the operational behaviour of a physical system under measurements
- State $\mathrm{P}_{AB|XY}$
- X,Y — measurements
- A,B — outcomes
- $\mathrm{P}_{AB|XY}(ab|xy)$



Not much to rely on

- Black box
- Unknown dimension
- Unknown internal structure — might be signalling (memory effects)
  - ⇒ Marginals are not well defined, can't just trace out



Quantum family tree

de Finetti type theorems

standard de Finetti theorems

de Finetti reductions

(a.k.a post selection)

- $\rho^k = \pi \rho^k \pi^\dagger$

$\Rightarrow \rho^k \leq (k+1)^{d^2-1} \tau^k$

n-exchangeable

- $\rho^k = \pi \rho^k \pi^\dagger$
- $\exists \rho^n$:

$\rho^n = \pi \rho^n \pi^\dagger$

$\rho^k = \mathrm{tr}_{n-k} \rho^n$

infinitely exchangeable

- $\rho^k = \pi \rho^k \pi^\dagger$
- $\forall n > k, \quad \exists \rho^n$:

$\rho^n = \pi \rho^n \pi^\dagger$

$\rho^k = \mathrm{tr}_{n-k} \rho^n$

$\Rightarrow \rho^k = \tau^k$

exact

(poly. error)

$\Rightarrow \|\rho^k - \tau^k\|_1 \leq d^2 k/n$

almost de Finetti

(exp. error)

$\Rightarrow \|\rho^k - \tilde{\tau}^k\|_1 \leq e^{-\Omega(n-k)}$

$\tilde{\tau}^k$ almost de Finetti state

Wanted — new de Finetti

- We need a new de Finetti theorem, applicable to device independent protocols
- No dimension dependence
    - Instead: # of measurements and outcomes
- No non-signalling assumptions (without tracing out)
- Known "non-signalling" de Finetti theorems require additional assumptions

de Finetti reduction for CPD

- Permutation invariance $\mathrm{P}_{A|X}(a|x) = \mathrm{P}_{A|X}(\pi(a)|\pi(x))$
- de Finetti state $\tau_{A|X} = \int \mathrm{Q}_{A_1|X_1}^{\otimes n} \mathrm{dQ}_{A_1|X_1}$
- de Finetti reduction

number of measurements (per subsystem)

number of outcomes (per subsystem)

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

number of subsystems

How to apply

- de Finetti reduction:

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

- How to apply (intuition):
  - $\mathrm{P}_{\text{fail}}(\mathrm{P}_{A|X})$ — failure prob. of the protocol when acting on $\mathrm{P}_{A|X}$
  - Reduction: $\mathrm{P}_{\text{fail}}(\mathrm{P}_{A|X}) \leq (n+1)^{m(l-1)} \mathrm{P}_{\text{fail}}(\tau_{A|X})$

increasing poly. with n

decreasing exp. with n

How to apply

- de Finetti reduction:

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

- How to apply (intuition):
  - $\mathrm{P}_{\text{fail}}(\mathrm{P}_{A|X})$ — failure prob. of the protocol when acting on $\mathrm{P}_{A|X}$
  - Reduction: $\mathrm{P}_{\text{fail}}(\mathrm{P}_{A|X}) \leq (n+1)^{m(l-1)} \mathrm{P}_{\text{fail}}(\tau_{A|X})$

the "cost" of
the reduction

Variants

- Freedom in the measure $\tau_{A|X} = \int Q_{A_1|X_1}^{\otimes n} \mathrm{d}Q_{A_1|X_1}$
- Different measures give different de Finetti states
- Different de Finetti states lead to different de Finetti reductions:
  1. Applicable to different families of states
  2. Lower "cost"

Variants

- General result: including additional symmetries

$$\forall a, x \quad \mathrm{P}^{\mathcal{S}}_{A|X}(a|x) \leq (n+1)^{d} \tau^{\mathcal{S}}_{A|X}(a|x)$$

- No symmetry:

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

- CHSH symmetry:

$$\forall a, b, x, y \quad \mathrm{P}^{\mathcal{CHSH}}_{AB|XY}(ab|xy) \leq (n+1) \tau^{\mathcal{CHSH}}_{AB|XY}(ab|xy)$$

Great!!

Let’s apply it to all DI protocols!

well… I wish :)

“Open issues”

- 2 main difficulties
- de Finetti reduction beyond quantum theory
- A_1/X_1 is distributed over several parties

$$\tau_{A|X} = \int \mathrm{Q}_{A_1|X_1}^{\otimes n} \mathrm{d}\mathrm{Q}_{A_1|X_1}$$

not necessarily quantum
not necessarily non-signalling

measure
over CPD

Non-quantum de Finetti state

- In some special cases can restrict to quantum states
- All the rest: can't apply trivially
- Wishful thinking: general quantum DI reduction

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

- Counter example: no strong parallel repetition

No purifications

- When working with quantum states: $\rho_{A_1}^{\otimes n} \rightarrow \psi_{A_1 E_1}^{\otimes n}$
- In the CPD framework there is no such thing
- Wishful thinking: de Finetti system includes the purifying system

$$\cancel{\mathrm{P}_{A|X} \quad \mathrm{PI} \quad \rightarrow \quad \tau_{AE|XZ} = \int \mathrm{Q}^{\otimes n}_{A_1 E_1|X_1 Z_1} \mathrm{dQ}_{A_1 E_1|X_1 Z_1}}$$

- Counter example: impossibility of general non-signalling privacy amplification

Summary

- Many quantum de Finetti theorems
- Goal: simplify device independent protocols
- New result: device independent de Finetti reduction

$$\forall a, x \quad \mathrm{P}^{\mathcal{S}}_{A|X}(a|x) \leq (n+1)^d \tau^{\mathcal{S}}_{A|X}(a|x)$$

- Not trivial to apply, but in the right direction!
- Proof idea: happy to explain (mainly combinatorics)

Thank you!