Hi! Want to come for a beer? It’s late!

No... I’m still working on my security proof...

I have to prove that it works for every possible state of Alice and Bob...
By now I only checked 2...

I will never finish my PhD!!

Did you try to use a de Finetti reduction? Instead of checking every possible state you only need to check one special state!

I can’t use it...

Alice Bob
\[
X \sim P_{AB|XY} \leftrightarrow Y \quad A \sim P_{AB|XY} \rightarrow B
\]

My protocol is device independent. I don’t have a bound on the dimension.

Oh... Then you should check this poster out!

---

**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 \( P_{A|X} \)
- \( X \) - measurements
- \( A \) - outcomes
- Describes a larger set of systems than quantum systems

---

**Theorem:**

There exists a de Finetti system, \( \tau_{A|X} \), such that for every permutation invariant system \( P_{A|X} \)

\[
\forall a, x \quad P_{A|X}(a|x) \leq (n + 1)^{m(l-1)} \tau_{A|X}(a|x).
\]

\( \tau_{A|X} \) - 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 \( P_{A|X} \) and outputs “success” or “fail” with some probabilities. Then for every system \( P_{A|X} \)

\[
P_{\text{fail}}(P_{A|X}) \leq (n + 1)^{m(l-1)} P_{\text{fail}}(\tau_{A|X}).
\]

---

**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

---

QCrypt, August 5-9, 2013, Waterloo

| rotema, renner | @phys.ethz.ch |