Parallel Repetition Using de Finetti Reductions

QIS @ MIT | June 23, 2015

arXiv:1308.0312 | de Finetti reductions for correlations
arXiv:1411.1582 | Non-signalling parallel repetition using de Finetti reductions

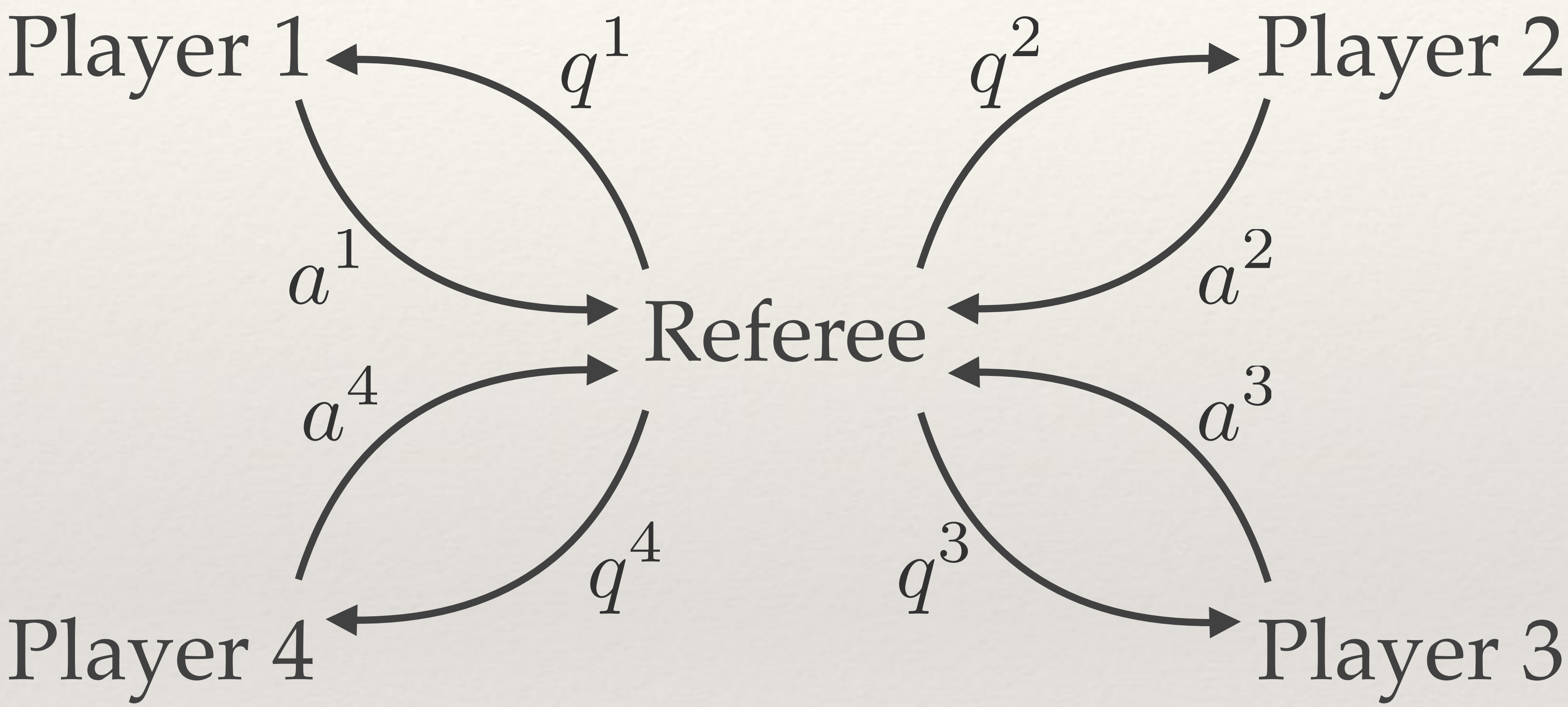
Rotem Arnon-Friedman (ETH), Renato Renner (ETH) & Thomas Vidick (Caltech)

Outline

1. Games and parallel repetition
2. de Finetti theorems in the context of games
3. Results
4. Proof ideas

Games & Parallel Repetition

Multiplayer games

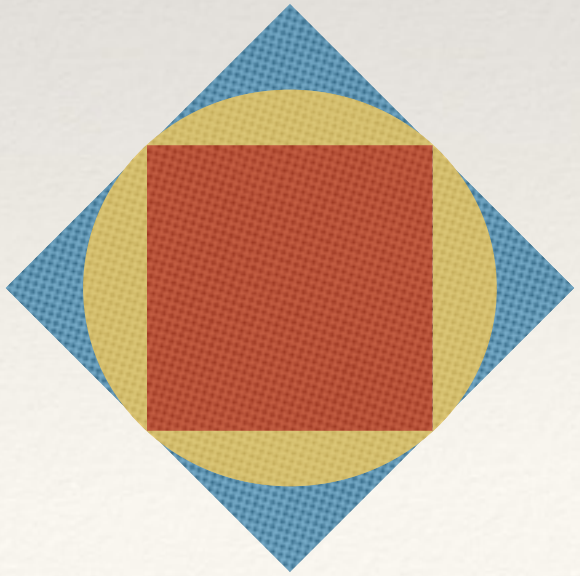


Game: $G = (\mathcal{Q}, \mathcal{A}, Q, R)$

Winning condition: $R : \mathcal{Q} \times \mathcal{A} \to \{0, 1\}$

Strategies

- Players decide on a strategy to optimally win the game
- Modelled by a conditional prob. dist. $O_{A|Q}$
- Allowed resources:
  - Classical — local functions + shared randomness
  - Quantum — shared quantum state
  - **Non-signalling**



Non-signalling conditions

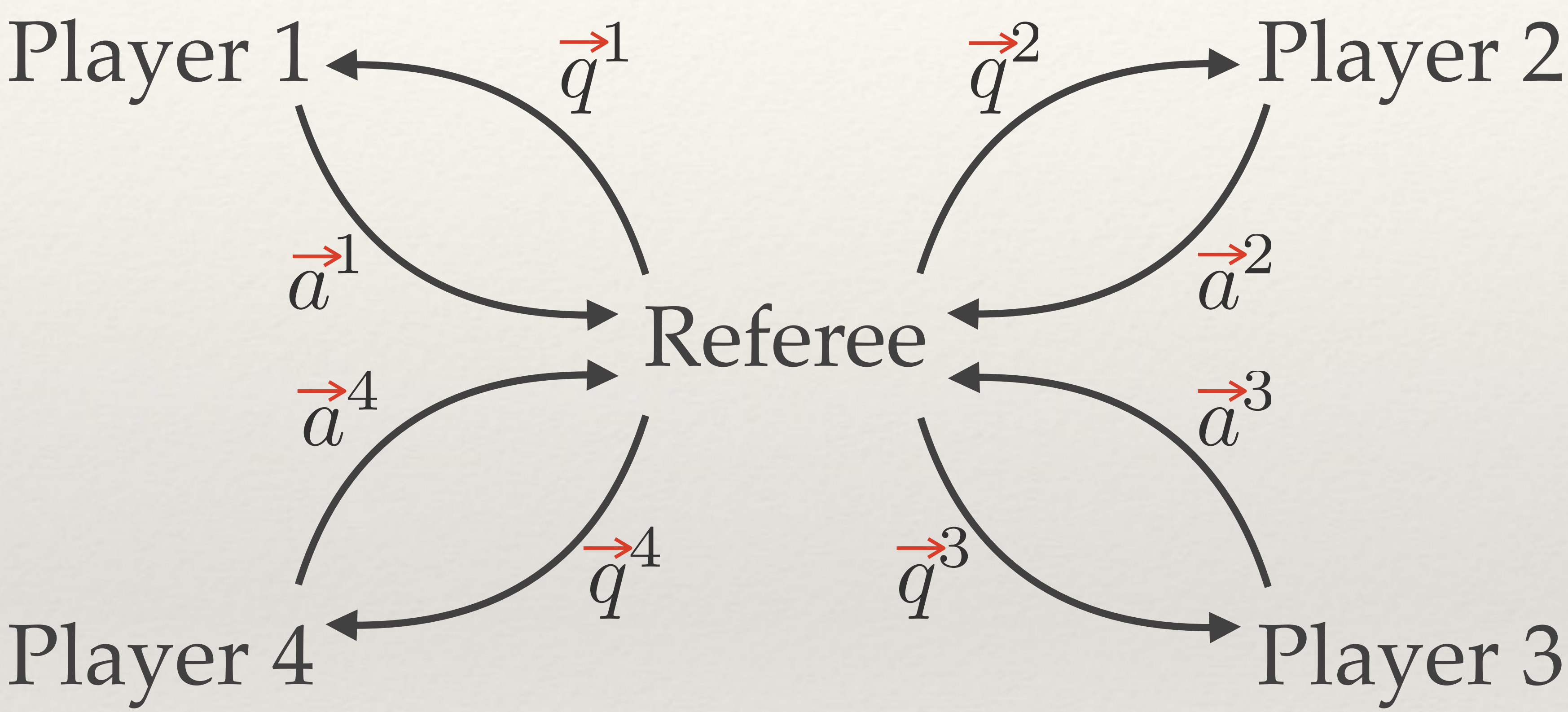
- For every subset of players I, the marginals of the other players $\bar{I}$ is independent of the questions to I
- Formally:

$$\forall a^{\bar{I}}, q^{\bar{I}}, q^{I}, r^{I} \quad \mathrm{O}_{A|Q}(\circ, a^{\bar{I}}|q^{I}, q^{\bar{I}}) = \mathrm{O}_{A|Q}(\circ, a^{\bar{I}}|r^{I}, q^{\bar{I}})$$

where

$$\mathrm{O}_{A|Q}(\circ, a^{\bar{I}}|q^{I}, q^{\bar{I}}) = \sum_{a_i|i\in I} \mathrm{O}_{A|Q}(a|q^{I}, q^{\bar{I}})$$

Repeated game



Repeated game: $G^n = \left(\mathcal{Q}^{\otimes n}, \mathcal{A}^{\otimes n}, Q^{\otimes n}, R^{\otimes n}\right)$

Goal: win as many coordinates as possible

The big question

- Trivial i.i.d. strategy $\mathrm{O}_{A|Q}^{\otimes n}$
- The players get all the questions together
- Can use a correlated strategy (between the rounds) $\mathrm{P}_{\vec{A}|\vec{Q}}$
- Known games where this is useful
- Can they do significantly better than i.i.d. for a large number of repetitions?

The big question

- Optimal winning prob. in one game $1-\alpha$
- Questions 1 (parallel repetition):
  - What is the prob. to win all games?
  - Can it be higher than $(1-\alpha)^n$?
- Question 2 (**threshold**):
  - What is the prob. to win more than a fraction $1-\alpha+\beta$ of the games?

Related work

Raz, 98: Classical two-player games exponential parallel repetition

Holenstein, 07: Classical two-player + non-signalling parallel repetition

Rao, 11: Classical two-player parallel repetition + threshold theorem

Buhrman, Fehr & Schaffner, 13: Non-signalling multiplayer parallel repetition + threshold theorem (complete-support)

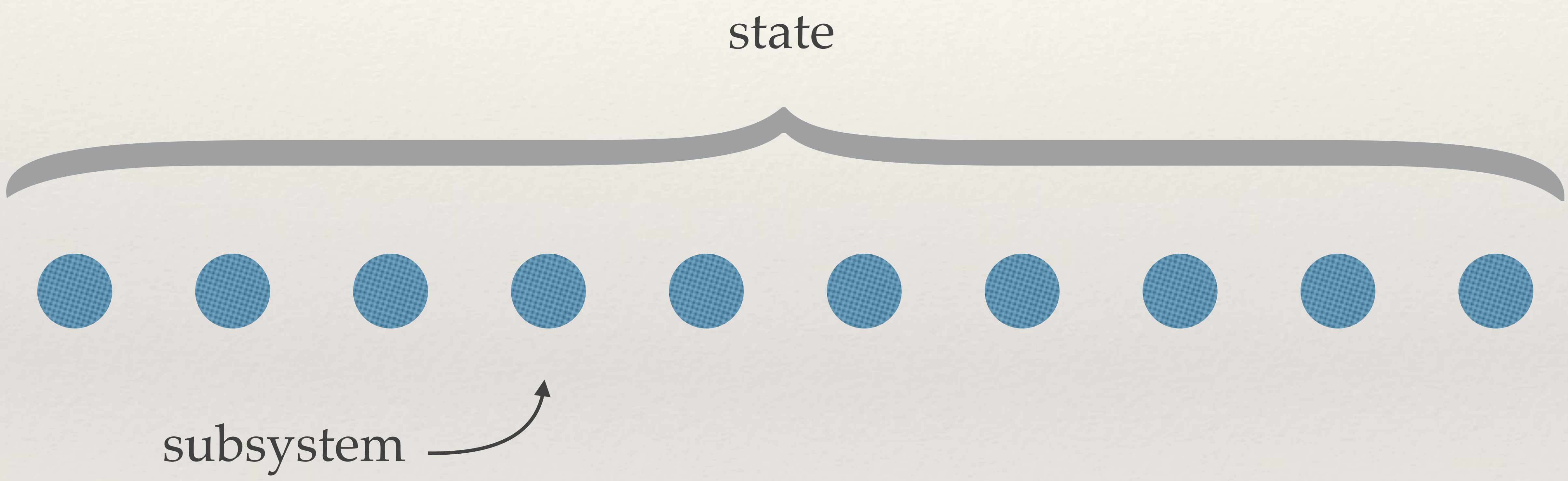
Quantum: exponential parallel repetition for restricted sets of games

de Finetti Theorems in the Context of Games

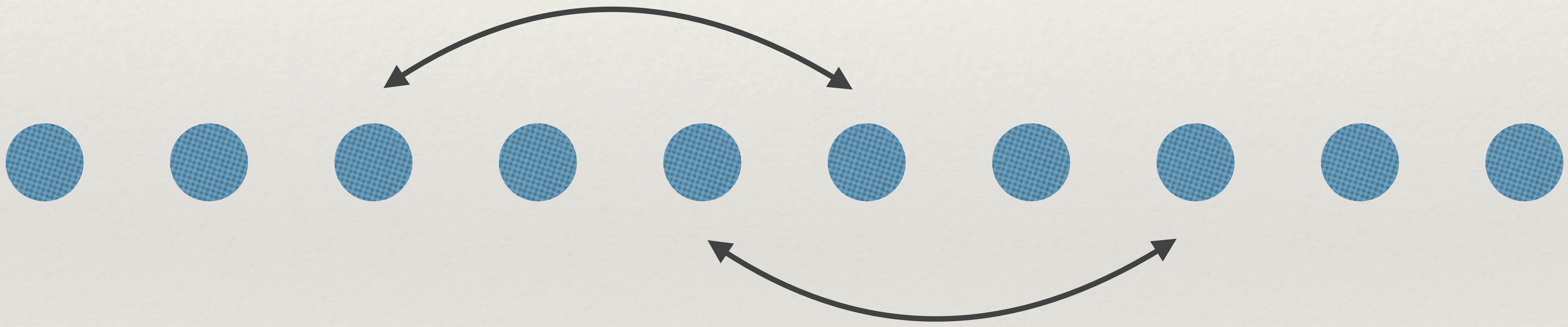
The basics

- 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: $\forall \pi \quad \rho = \pi \rho \pi^\dagger$
  - Conditional probability distribution (CPD):

$$\forall \pi, \vec{a}, \vec{q} \quad \mathrm{P}_{\vec{A}|\vec{Q}}(\vec{a}|\vec{q}) = \mathrm{P}_{\vec{A}|\vec{Q}}(\pi(\vec{a})|\pi(\vec{q}))$$

permuting the questions and answers
for all players together

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: $\tau_{\vec{A}|\vec{Q}} = \int \mathrm{O}_{A|Q}^{\otimes n} \, \mathrm{d}\mathrm{O}_{A|Q}$
- Simple structure — easy to handle

Example:

$$\frac{3}{4}\mathrm{O}_1^{\otimes n} + \frac{1}{4}\mathrm{O}_2^{\otimes n}$$

de Finetti type theorems

permutation invariant state $\xrightarrow{\text{de Finetti theorems}}$ de Finetti state

easy to have

easy to analyse

Applications in quantum info. theory: cryptography, tomography, channel coding, …

de Finetti for games

permutation invariant **strategy**

de Finetti theorems

de Finetti **strategy**

easy to have

easy to analyse

G^n is permutation invariant

trivial behaviour under parallel repetition

de Finetti for games

- Natural, how come this was never done before?
- Recent de Finetti reduction for correlations fits!

Advantages

- No dimension dependency
  - Instead: # of measurements and outcomes
- No non-signalling assumptions between subsystems (without tracing out systems)
- $\Rightarrow$ Applicable to parallel repetition and the study of correlations in general!

de Finetti reduction for correlations

- Permutation invariance $\mathrm{P}_{\vec{A}|\vec{Q}}(\vec{a}|\vec{q}) = \mathrm{P}_{\vec{A}|\vec{Q}}(\pi(\vec{a})|\pi(\vec{q}))$
- de Finetti strategy $\tau_{\vec{A}|\vec{Q}} = \int \mathrm{O}_{A|Q}^{\otimes n} \, \mathrm{dO}_{A|Q}$
- de Finetti reduction

number of questions / measurements (per subsystem)

number of answers / outcomes (per subsystem)

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

number of repetitions / subsystems

How to apply

- de Finetti reduction:

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

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

increasing poly. with n

decreasing exp. with n

Challenges in parallel repetition

- Trivial application:

$$w\left(\mathrm{P}_{\vec{A}|\vec{Q}}\right) \leq (n+1)^{m(l-1)} w\left(\tau_{\vec{A}|\vec{Q}}\right)$$

Not useful!

- Signalling de Finetti strategy

$$\tau_{\vec{A}|\vec{Q}} = \int \mathrm{O}_{A|Q}^{\otimes n} \, \mathrm{dO}_{A|Q}$$

not necessarily non-signalling

measure over CPD

Signalling de Finetti strategy

- Wishful thinking:

$$\cancel{\forall \vec{a}, \vec{q} \quad \mathrm{P}^{\mathrm{ns}}_{\vec{A}|\vec{Q}}(\vec{a}|\vec{q}) \leq (n+1)^{m(l-1)} \tau^{\mathrm{ns}}_{\vec{A}|\vec{Q}}(\vec{a}|\vec{q})}$$

- Counter example: no strong parallel repetition
  [Kempe & Regev, 2009]
- Same for quantum and classical!

Signalling de Finetti strategy

- Have to deal with the signalling de Finetti strategy
- General intuition:

$$\mathrm{P}_{\vec{A}|\vec{Q}} \approx \int \mathrm{O}_{A|Q}^{\otimes n} \, \mathrm{dO}_{A|Q}$$

- If the total strategy is non-signalling then the weight of signalling strategies is exponentially small

Parallel Repetition Results

Theorem 1

- For
  - any complete-support non-signalling game with optimal winning probability $1-\alpha$
  - any $0 < \beta \leq \alpha$
  - and large enough number of repetitions n

$$\Pr\left[f > 1-\alpha+\beta\right] \leq \mathcal{C}_1\left(G,n\right)\exp\left[-\mathcal{C}_2\left(G\right)n\beta^2\right]$$

winning frequency

polynomial

optimal

Theorem 2

- Theorem 1 also holds for 2-player games without complete supports
- For other games without complete support — similar result for a modified version of parallel repetition

Proof Ideas & Techniques

Main ideas

$$\mathrm{P}_{\vec{A}|\vec{Q}} \approx \int \mathrm{O}_{A|Q}^{\otimes n} \, \mathrm{dO}_{A|Q}$$

non-signalling

can still have signalling parts

- Step 0: define a signalling measure (distance)
- Step 1: bound the weight of the $\mathrm{O}_{A|Q}$'s which are far from non-signalling strategies
- Step 2: bound the winning probability of all other parts

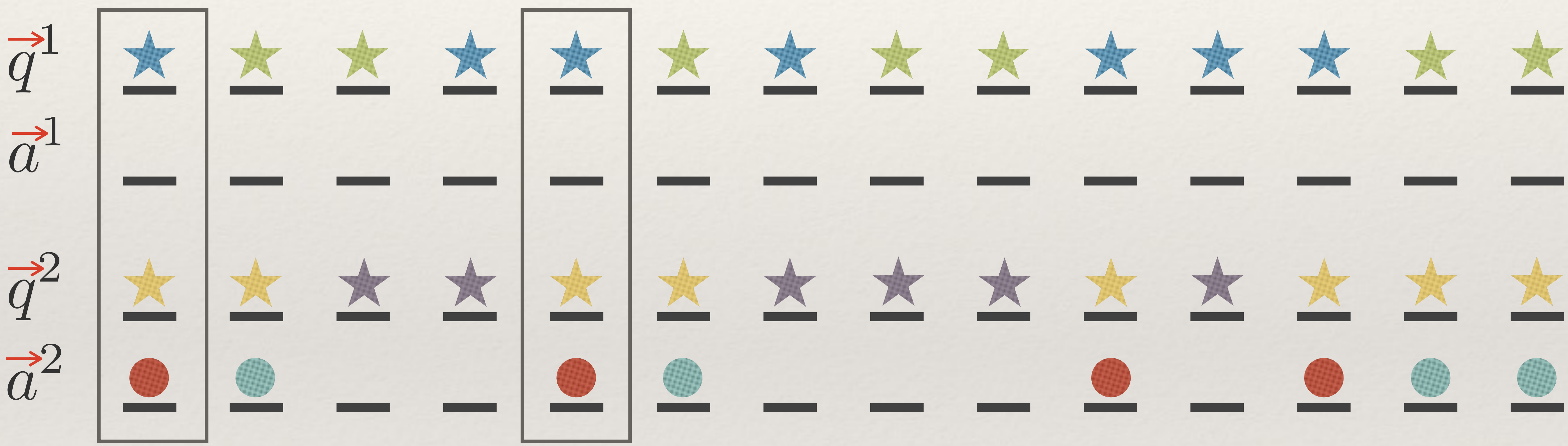
Step 1: low signalling weight

- Reduction to a guessing game

- Goal: Player 2 needs to guess an index in which the question they got is (★,★)

Step 1: low signalling weight

- Reduction to a guessing game



choose questions using shared randomness

player 2 can estimate the signalling locally

and make a better guess!

Step 1: low signalling weight

- The important part: signalling can be estimated **locally**!
- In contrast to the standard proofs of parallel repetition, we only need to condition on local events (detecting signalling)

Step 2: signalling to winning

- Most of the weight is on strategies which only signal a bit
- Small signalling value $\Rightarrow$ small advantage in the game
- Winning probability close to $1 - \alpha$
- Formally: sensitivity analysis of linear programs

Summary & open questions

- New proof technique for non-signalling parallel repetition using de Finetti reductions for correlations
  - What about classical and quantum parallel repetition?
- First (new) application for the de Finetti reduction
  - What more can we do with it?
    - Device independent crypto?
    - Complexity?

Thank you!

arXiv:1308.0312 | de Finetti reductions for correlations

arXiv:1411.1582 | Non-signalling parallel repetition using de Finetti reductions