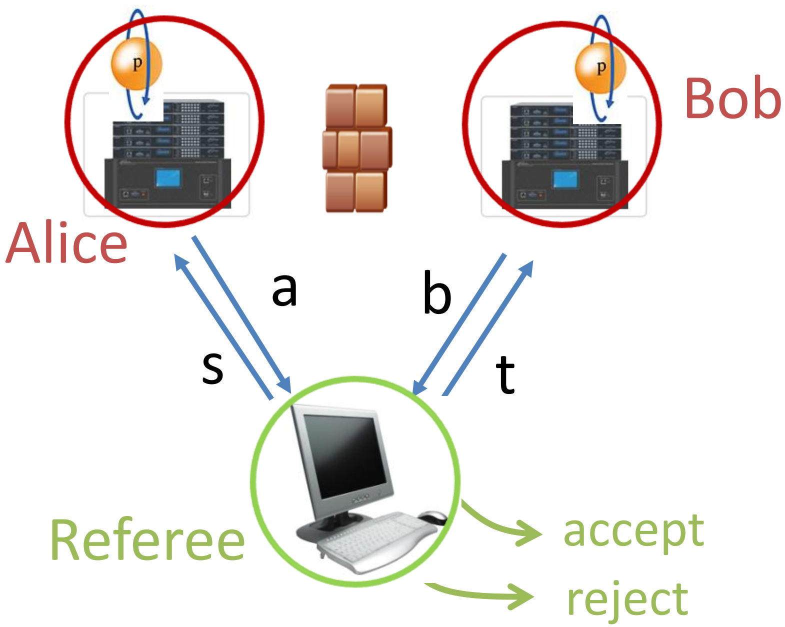
Parallel repetition of nonlocal games

Thomas Vidick
UC Berkeley

Joint work with Julia Kempe (LRI, Paris)

Nonlocal games



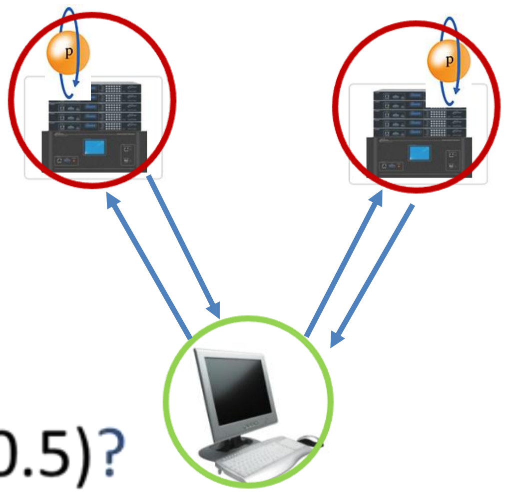
- Referee picks (s,t) ~ π and sends them to the players
- Players provide answers a,b
- No communication allowed, but can share |ψ>

Classical value ω(G) = Max. Winning Prob.

(over all *classical* strategies)

- Framework to study Bell, Tsirelson inequalities
- Also arise in cryptography (device-independent QKD), testing, complexity theory (PCPs)....

Parallel repetition



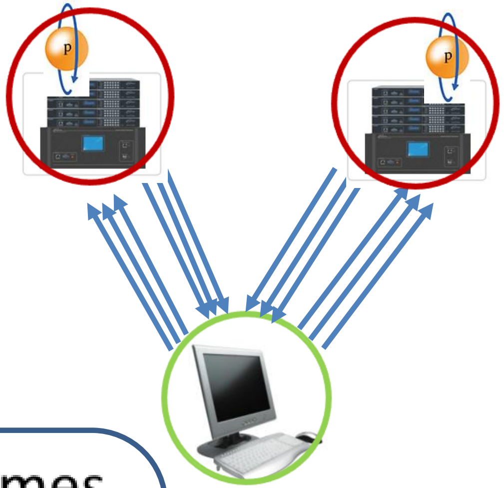
- Suppose given G such that either
  - $\omega^*(G) = 1$ ("honest case"), or
  - $\omega^*(G) < 0.999$ ("dishonest case")

  Can we amplify the difference (to, say, 1 vs 0.5)?

- Sequential repetition works
  - $\omega^*\left(G^{seq-l}\right) = \omega^*(G)^l$
  - Drives us outside the model of one-round games

- Parallel repetition…?
  - Send l pairs of questions simultaneously, receive l pairs of answers, accept iff all correct
  - It works: the rounds are independent! [FRS'88]
  - Not quite: [F,W]: game G, $\omega^*(G^{par-2}) = \omega^*(G) = 2/3$

A brief summary of a long history



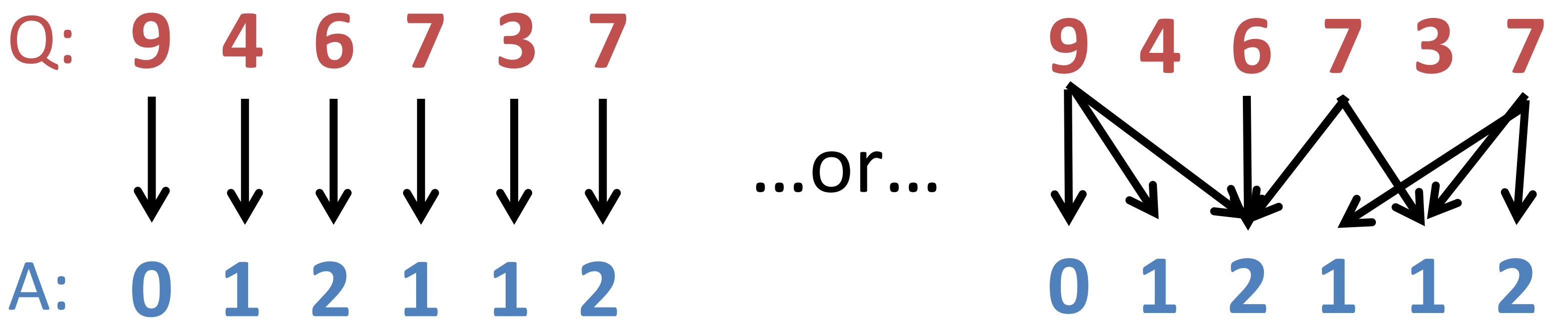
- [FK’94]: polynomial-rate decrease for projection games

- Modify the repeated game in order to facilitate analysis

  → Mostly interested in performing amplification

Feige-Kilian repetition

- Repeated (classical deterministic) strategies



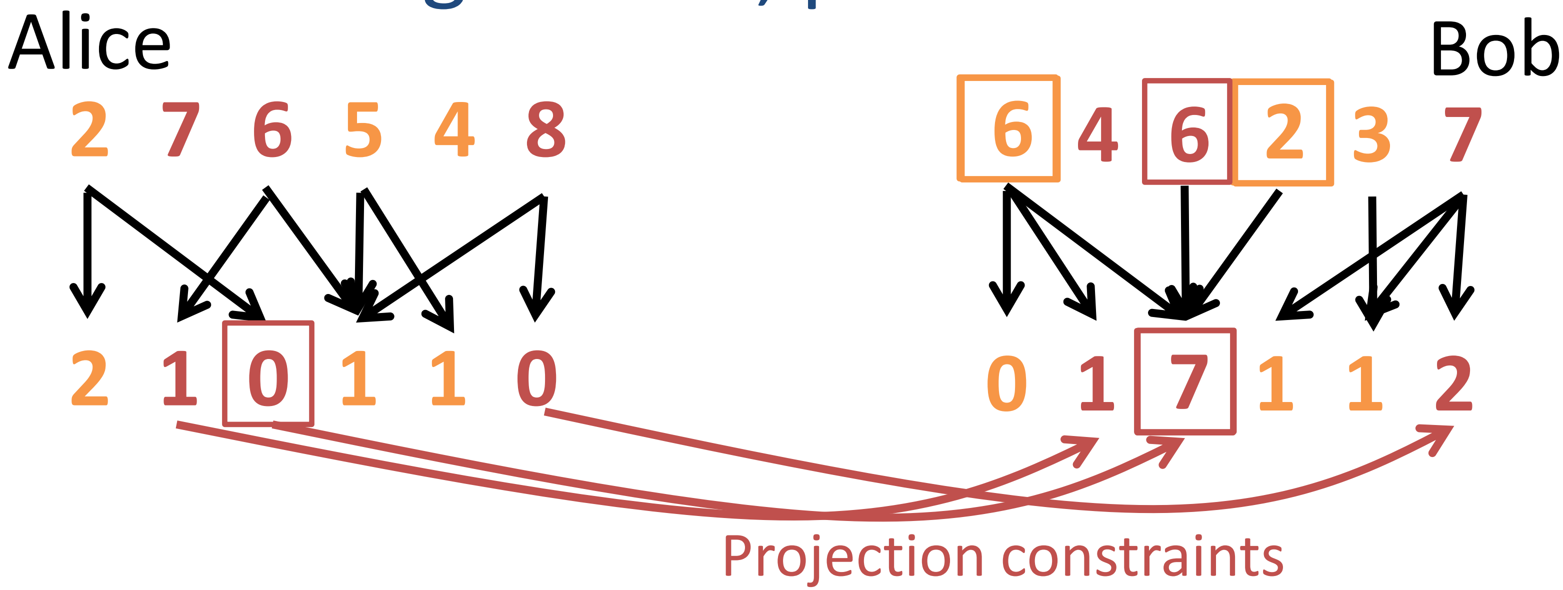
- Goal: fail strategies very far from independent repetitions
- G a projection game. Game FK(G,l):

For every pair of questions and answer from Alice, there is a unique valid answer for Bob

  – $(l - \sqrt{l})$ rounds are "confuse" rounds: send random questions, accept any answer.

- Thm [FK'94]: ω(FK(G,l)) decreases polynomially fast with l

Feige-Kilian, proof idea



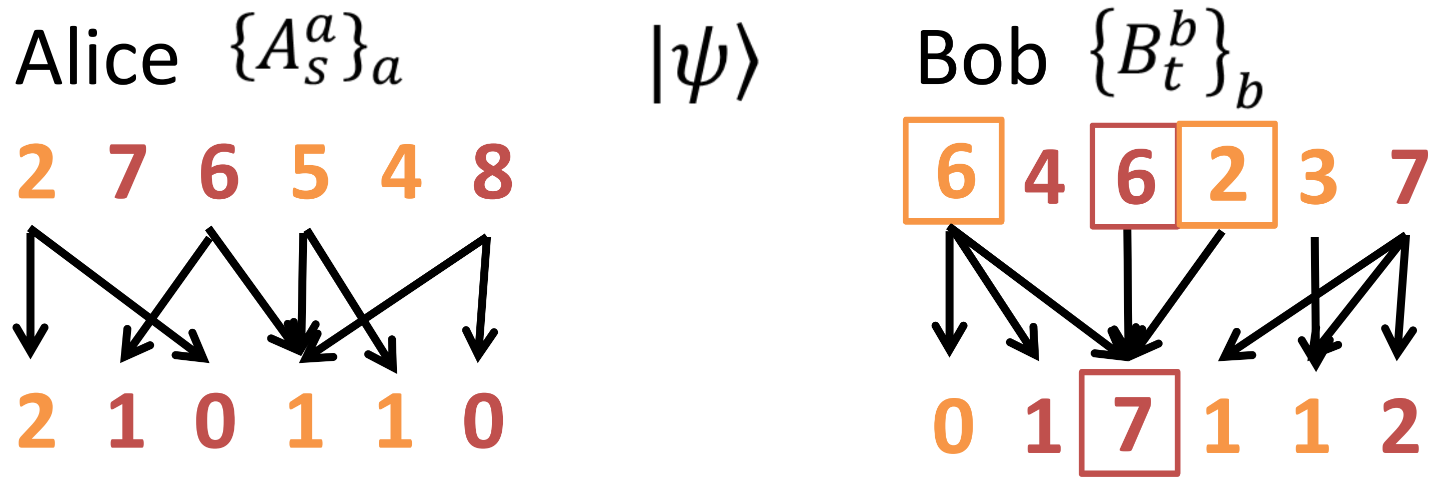
[FK] prove a “dichotomy” theorem.

Criterion: a (1-ϵ) –fraction of questions have no answer arising with probability $\geq \epsilon$ (as questions in other rounds vary)

- True: Player is using a highly correlated strategy
- False (informal): At least a subset of the game rounds are played independently of each other

In both cases we can bound the value $\omega(FK(G,l))$

Entangled strategies (1)

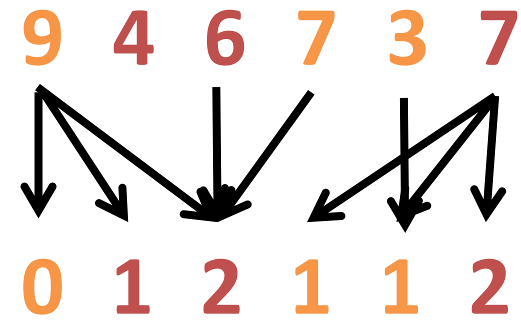


- Bob's answers can be random but still correlated with Alice's
- Need a new criterion to distinguish honest product strategies from correlated ones.
- Suppose Bob measures twice, *sequentially*
  - First as if q = (6,4,6,2,….)
  - Second as if q= (9,4,6,7,…)
- Will he obtain the same outcome (to the third question)?
  - Yes if uses honest, product, projective strategy

Entangled strategies (2)

- We prove a "quantum dichotomy theorem"

> Criterion: sequential measurement *does not* lead to same answer



  - Yes: strategy will not satisfy projection constraints
  - No (informal): can argue about strategy being independent across rounds

- In the second case, obtain almost-product form of strategy

$$B_{q_1 q_2 q_3 \dots q_l}^{a_1 a_2 a_3 \dots a_l} \approx \Pi_{q_1}^{a_1} \Pi_{q_2}^{a_2} B_{q_3 \dots q_l}^{a_3 \dots a_l}, \text{ where } \left\{\Pi_{q_i}^{a_i}\right\}_{a_i} \text{ is a POVM}$$

  - Based on "orthogonalization lemma": almost-orthogonal operators are close to perfectly orthogonal ones.

- In both cases we can bound the value $\omega^*(FK(G,l))$

Summary of results

- The value of nonlocal games can be reduced in parallel.

- Thm: If G is a projection game, FK-repetition decreases its entangled value at a polynomial rate
  - If in addition G is a free game, then direct parallel repetition works

The referee’s distribution on questions is product

- If G is a general game, need to add “consistency” rounds in addition to “game”, “confuse” rounds
  - Consistency round: same question, should give same answer
  - Again, polynomial decrease in the value
  - Value of G could go from 1 to < 1!
  - Does not happen if honest strategy does not use any entanglement, or only the maximally entangled state.

Lots of open questions!

- Can we get an exponential rate?
- Would direct parallel repetition also work?
- Can one prove “threshold” amplification?
- More players, more rounds, quantum messages?
- Can extract “direct product test”; applications?