Consequences and Limits of Nonlocal Strategies

Richard Cleve (Calgary)

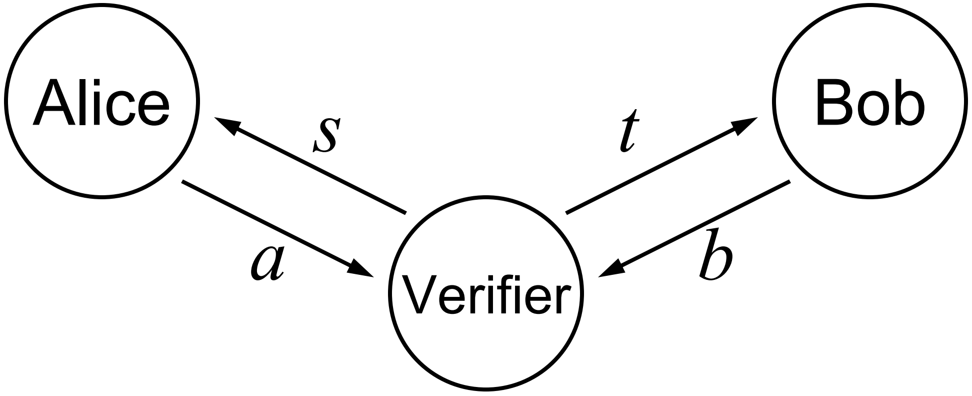
joint work with:

Peter Høyer (Calgary)

Benjamin Toner (Caltech)

John Watrous (Calgary)

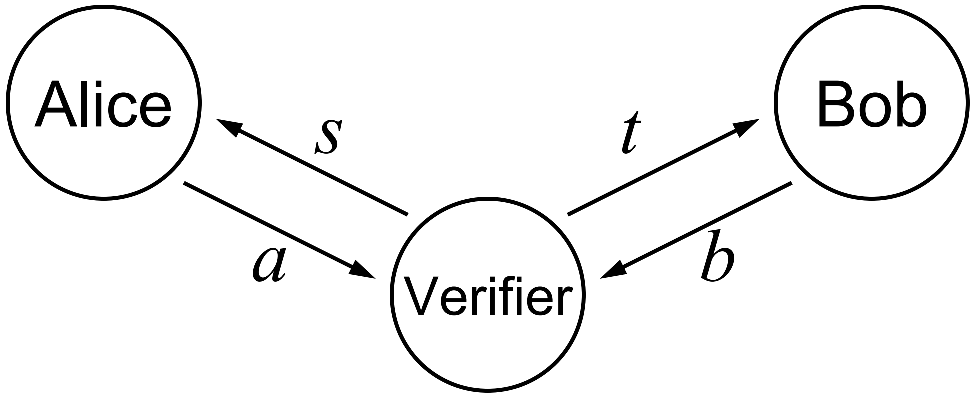
Bell Nonlocality à la CHSH



No communication between Alice and Bob during the game

- The Verifier chooses two random bits, s and t, and sends them to Alice and Bob, respectively
- Alice and Bob return bits a and b, respectively
- The Verifier ***accepts*** iff $a \oplus b = s \wedge t$
  (Alice and Bob ***win*** iff Verifier accepts)

CHSH Game



For any ***classical*** strategy, Alice and Bob's success probability is at most 3/4

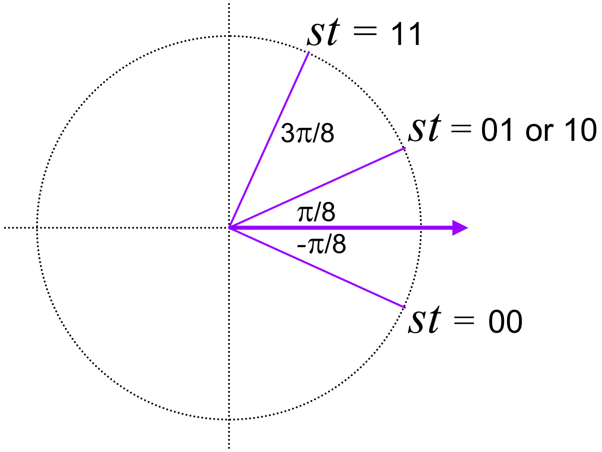
Winning conditions: $a_s \oplus b_t = s \wedge t$

$$a_0 \oplus b_0 = 0$$
$$a_0 \oplus b_1 = 0$$
$$a_1 \oplus b_0 = 0$$
$$a_1 \oplus b_1 = 1$$

CHSH Game

There is a ***quantum*** strategy that succeeds with probability $\cos^2(\pi/8) \approx 0.853$

- Alice and Bob start with entanglement $|\phi\rangle = |00\rangle - |11\rangle$
- If Alice applies rotation θ_A and Bob applies rotation θ_B:
  $\cos(\theta_A - \theta_B)\,(|00\rangle - |11\rangle) + \sin(\theta_A - \theta_B)\,(|01\rangle + |10\rangle)$
- Alice and Bob can organize their rotations so that $\theta_A - \theta_B$ takes on the following values for input st :

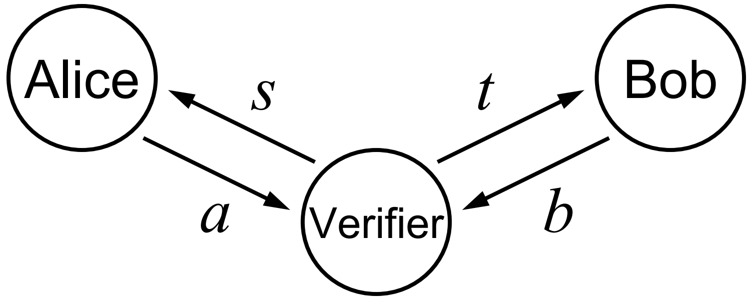


(Bell, 1964; Clauser, Horne, Shimony, Holt, 1969)

CHSH Game

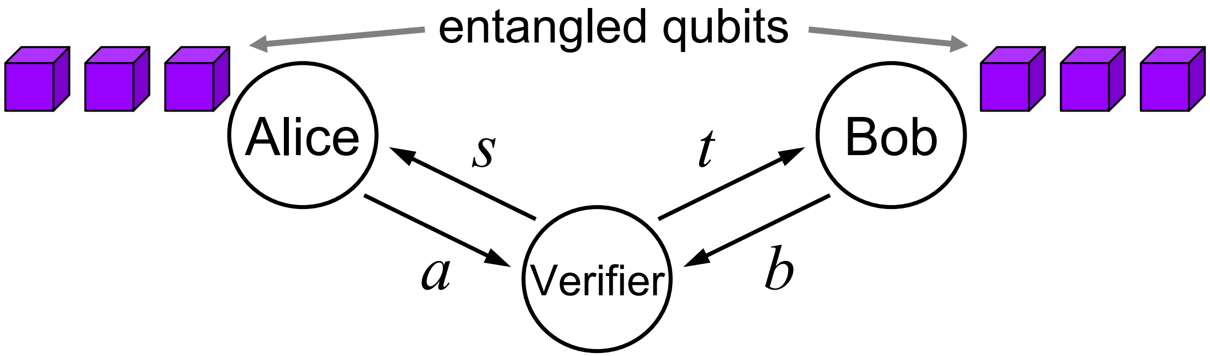
Tsirelson (1980): For ***any*** quantum strategy, the success probability is at most $\cos^2(\pi/8)$

Nonlocality Game Framework



- A ***nonlocality game*** G consists of four sets A, B, S, T, a probability distribution π on $S \times T$, and a predicate $V : A \times B \times S \times T \rightarrow \{0,1\}$
- Verifier chooses $(s,t) \in S \times T$ according to π and, after receiving (a,b), ***accepts*** iff $V(a,b,s,t) = 1$
- The ***classical value*** of G, denoted as $\omega_c(G)$, is the maximum acceptance probability, over all classical strategies of Alice and Bob

Quantum Strategies



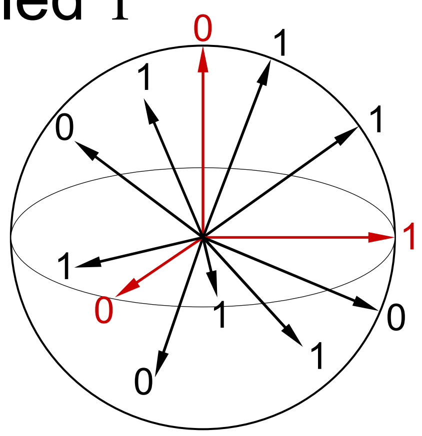
- The ***quantum value*** of G, denoted as $\omega_q(G)$, is the maximum acceptance probability of quantum strategies
- An upper bound on $\omega_c(G)$ is a ***Bell inequality***
- A quantum strategy with success probability greater than $\omega_c(G)$ is a ***Bell inequality violation***
- An upper bound on $\omega_q(G)$ is a ***Tsirelson inequality***

Kochen-Specker Game

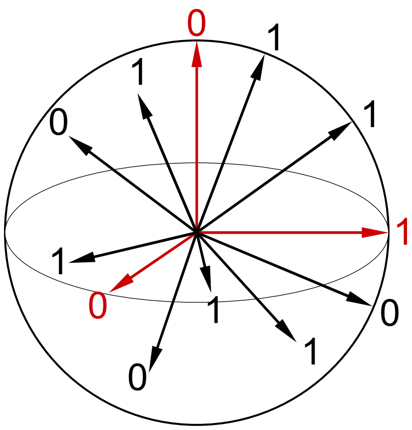
Based on the

Kochen-Specker Theorem (1967)**:** there exists a finite set of vectors $v_1, v_2, \ldots, v_n$ in $\mathbf{R}^3$ that ***cannot*** be assigned labels from $\{0,1\}$ simultaneously satisfying:

- For any two orthogonal vectors, they are not both labeled 1
- For any three mutually orthogonal vectors, at least one of them is labeled 1



Kochen-Specker Game



- The Verifier sends Alice a triple of vectors $s = (v_i, v_j, v_k)$ and Bob one vector $t = v_m$ from that triple
- Alice returns a, a valid labeling for (v_i, v_j, v_k), and Bob returns b, a label for v_m
- The verifier accepts iff the labels are consistent
- By the Kochen-Specker Theorem, $\omega_c(G) < 1$
- There is a perfect quantum strategy using entanglement $|\psi\rangle = |00\rangle + |11\rangle + |22\rangle$, therefore $\omega_q(G) = 1$

Our Goal

- Investigate general relationships between $\omega_q(G)$ and $\omega_c(G)$ for various nonlocality games

- **Motivation #1:** broaden understanding of what entanglement can and cannot do

- **Motivation #2:** determine the expressive power of ***multi-prover interactive proof systems*** with entangled provers

Computational Proof Systems

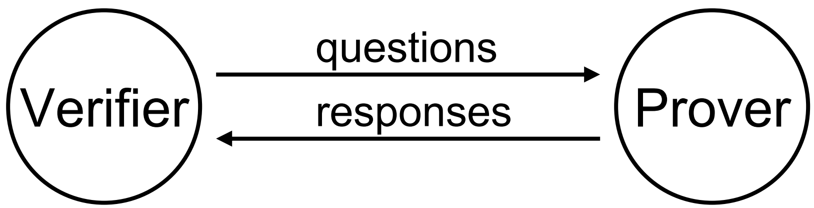
General question: what is the computational cost of the process of being ***convinced*** of something?

- Consider an instance of 3SAT:
  $$f(x_1,\ldots,x_n) = (x_1 \vee \bar{x}_3 \vee x_4) \wedge (\bar{x}_2 \vee x_3 \vee \bar{x}_5) \wedge \Lambda \wedge (\bar{x}_1 \vee x_5 \vee \bar{x}_n)$$
- Its satisfiability is easy to ***verify***—if one is supplied with, say, a satisfying assignment for it
- NP denotes the class of languages L whose positive instances have such “witnesses” that can be verified in polynomial-time

Interactive Proof Systems

If one can carry out a "dialog" with a prover then the expressive power increases from NP to PSPACE

is $x \in L$?

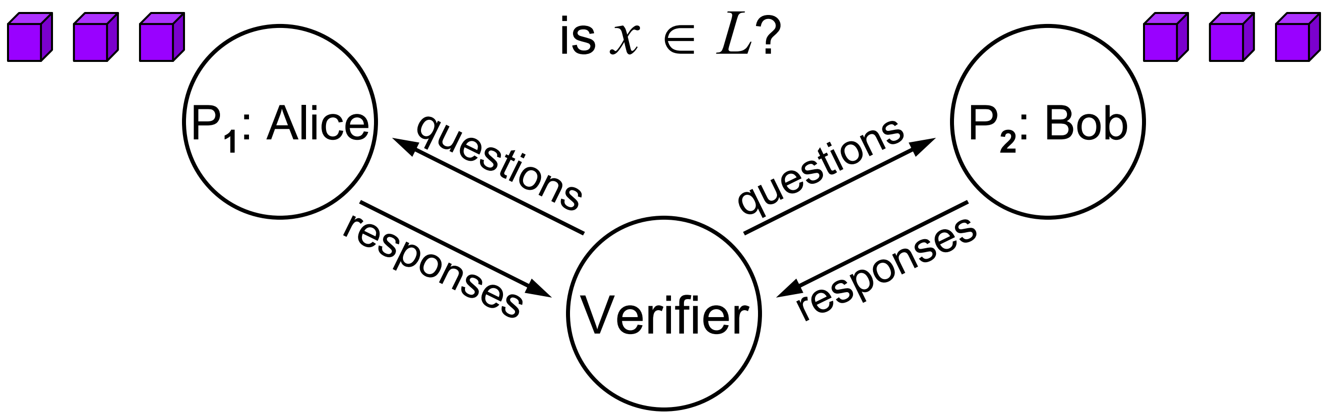


- The Verifier must be efficient (polynomial-time), but the Prover is computationally unbounded
- **Soundness:** if $x \notin L$, no Prover causes the Verifier to accept (small error probability is okay)
- **Completeness:** if $x \in L$, there exists a Prover that causes the Verifier to accept (small error is okay)

(Lund, Fortnow, Karloff, Nisan 1990; Shamir 1990)

Two Provers

With ***two*** provers, who cannot communicate with each other, the expressive power increases to NEXP (nondeterministic exponential-time)



- Again, the Verifier must be efficient (polynomial-time), and the Provers are computationally unbounded
- The NEXP result assumes the Provers are ***classical***
- With ***quantum*** strategies, Provers can sometimes "cheat"

(Babai, Fortnow, Lund, 1991)

Cheating a Protocol for 3SAT

Instance: $(x_1 \vee \overline{x}_3 \vee x_4) \wedge (\overline{x}_2 \vee x_3 \vee \overline{x}_5) \wedge (\overline{x}_1 \vee x_5 \vee \overline{x}_n)$

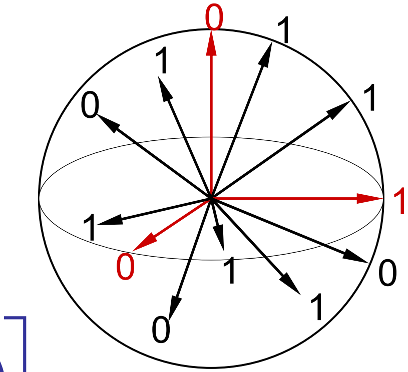
1. The Verifier randomly chooses a clause and a variable from that clause, and then sends the clause to Alice and the variable to Bob
2. Alice returns a valid truth assignment for the clause, and Bob must return a consistent value for the variable

E.g., for the above instance, the Verifier might send Alice "$(\overline{x}_2 \vee x_3 \vee \overline{x}_5)$" and send Bob "$x_5$"

… and a valid response is Alice sends 1, 0, 0 (values for x_2, x_3, x_5 respectively), and Bob sends 0 (value for x_5)

Cheating a Protocol for 3SAT

For an instance of the Kochen-Specker Theorem, the orthogonality conditions can be expressed by the formula



$$f(x_1,\ldots,x_n) = \left[\bigwedge_{v_i \perp v_j} \left(\overline{x}_i \vee \overline{x}_j\right)\right] \wedge \left[\bigwedge_{v_i \perp v_j \perp v_k} \left(x_i \vee x_j \vee x_k\right)\right]$$

- By the Kochen-Specker Theorem, this formula is unsatisfiable—therefore, for classical Provers, the Verifier accepts with probability ***less than one***
- But, using the quantum strategy for the KS game, the Provers can cause the Verifier to ***always*** accept

Quantum vs. Classical MIP

- MIP: class of languages accepted by ***classical*** two-prover interactive proof systems
- MIP*: class of languages accepted by ***quantum*** two-prover interactive proof systems
- **Theorem** (Fortnow, Rompel, Sipser, 1988)**:** MIP $\subseteq$ NEXP
- **Theorem** (Babai, Fortnow, Lund, 1991)**:** MIP $\supseteq$ NEXP
  And this holds for one-round proof systems (Feige, Lovász)
- **Open questions:** is MIP* $\supseteq$ NEXP? is MIP* $\subseteq$ NEXP?
- **Note:** one-round quantum two-prover interactive proof systems correspond to nonlocality games …

XOR Games

- An ***XOR game*** is a nonlocality game where:
  - Alice and Bob's messages, a and b, are bits
  - The Verifier's decision is a function of s, t, $a \oplus b$
- **Example:** the CHSH game is an XOR game
- **Theorem 1:** for any XOR game, if $\omega_c(G) \leq 1 - \varepsilon$ then $\omega_q(G) \leq 1 - c\varepsilon^2$, where $c \approx \pi^2/4$
- **Note:** there exist classical XOR two-prover MIPs for NEXP

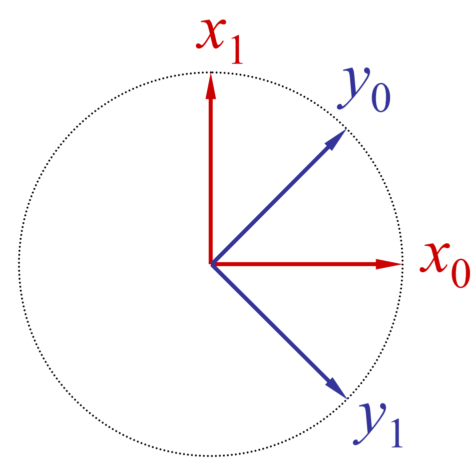
Proof of Theorem 1 (Part 1)

Makes use of

Theorem (Tsirelson, 1987)**:** quantum strategies for XOR games can be characterized by sets of vectors $\{x_s : s \in S\}$ and $\{y_t : t \in T\}$ in $\mathbf{R}^n$ such that, on input $(s,t) \in S \times T$,

$$\Pr[a \oplus b = 1] = (1 - x_s \cdot y_t)/2$$

E.g., vectors in $\mathbf{R}^2$ for the CHSH game:



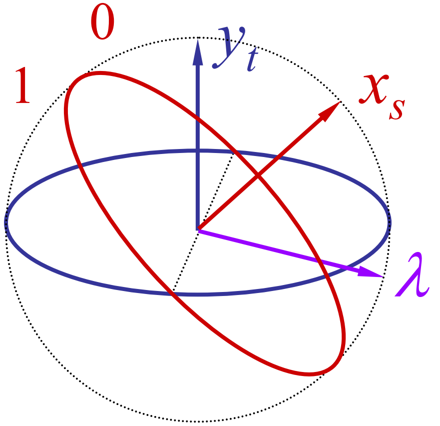
Aside: optimal strategies can be found by semidefinite programming

Proof of Theorem 1 (Part 2)

Contrapositive: $\omega_q(G) > 1 - c\varepsilon^2$ implies $\omega_c(G) > 1 - \varepsilon$

For a quantum strategy, we have $\{x_s : s \in S\}$, $\{y_t : t \in T\}$

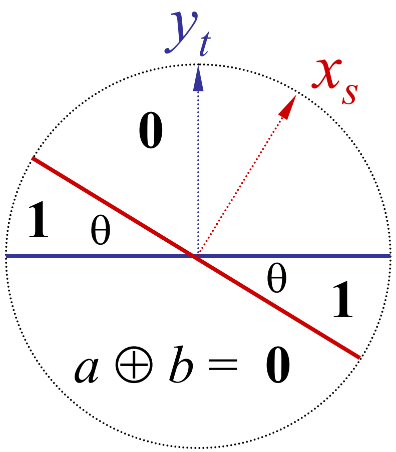
Classical strategy:



- Alice and Bob share a random vector $\lambda \in \mathbf{R}^n$
- On input s, Alice outputs 0 if $x_s \cdot \lambda \geq 0$ and 1 otherwise
- On input t, Bob outputs 0 if $y_t \cdot \lambda \geq 0$ and 1 otherwise

Proof of Theorem 1 (Part 3)

- **Classical protocol:**
  $\Pr[a \oplus b = 1] = \theta/\pi$
- **Quantum protocol:**
  $\Pr[a \oplus b = 1] = (1 - \cos(\theta))/2$
- It follows that the quantum and classical success probabilities, p_q and p_c, are related by
  $p_q \leq \sin^2(\pi\, p_c/2)$ if $p_c \geq 0.742$



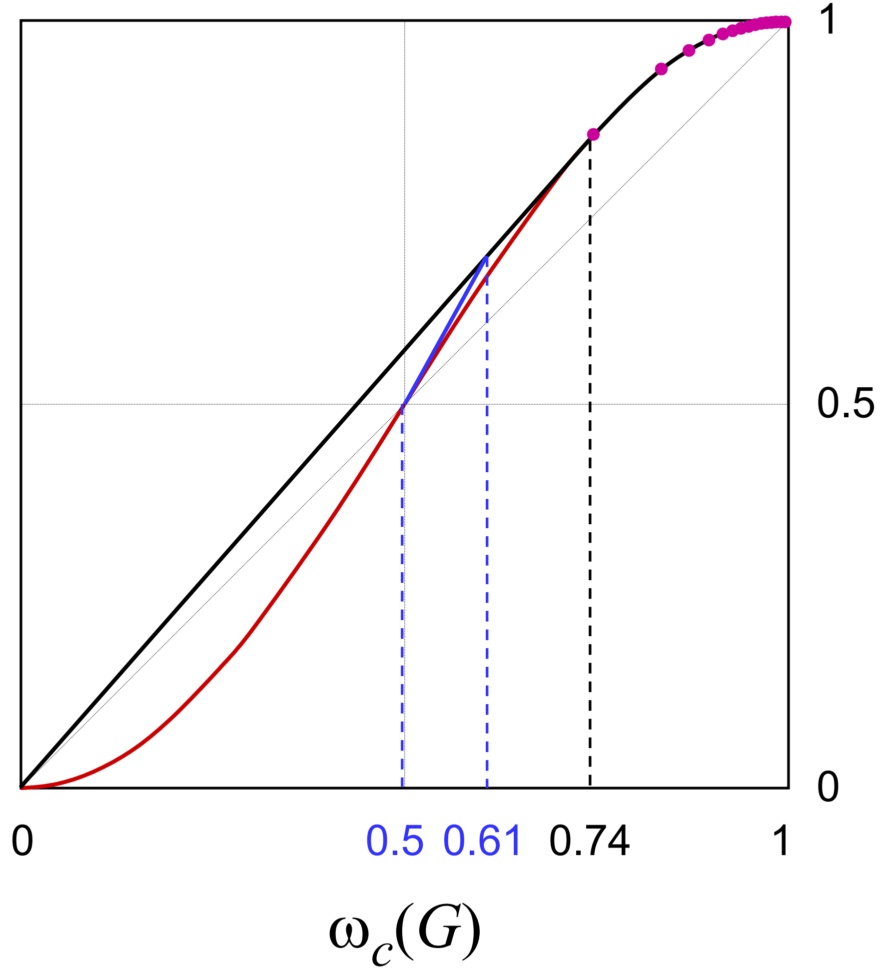
$$\cos(\theta) = x_s \cdot y_t$$

Conclusion of Theorem 1

Upper bound of $\omega_q(G)$ in terms of $\omega_c(G)$ for XOR games

Tight bound for Chained Bell Inequality games (Braunstein, Caves, 1990)

For ***nondegenerate*** XOR games, better bound when $0.5 \leq \omega_c(G) < 0.61$



Consequences for MIP*?

- For all $L \in$NEXP, there is a ***classical*** two-prover MIP that:
  - is an XOR game
  - has soundness probability $p_s \approx 0.6875$
  - has completeness probability $p_c = 0.75$

- ☹ Unfortunately, applying Theorem 1 yields a quantum upper bound on p_s of 0.7825 (greater than p_c)

- Possible remedies:
  - better classical p_s vs. p_c gap?
  - stronger ***specialized*** upper bounds for quantum p_s?
  - quantum strategy to increase quantum p_c?

Binary Nonlocality Games

Binary: $|A| = |B| = 2$ (but not necessarily XOR)

Theorem 2: for any binary game G,
if $\omega_c(G) < 1$ then $\omega_q(G) < 1$

Note: no corresponding result if "binary" is relaxed to "ternary-binary": $|A| = 3$ and $|B| = 2$

Example: the Kochen-Specker game is ternary-binary with $\omega_c(G) < 1$ and $\omega_q(G) = 1$

Bounding Entanglement

- For XOR games, $N = \max(|S|,|T|)$ entangled qubits suffice (this can be exponentially large for MIPs)
- For ***approximate*** simulations, $O(\log N)$ qubits suffice (by applying the Johnson-Lindenstrauss Theorem)
- **Theorem** (Kobayashi, Matsumoto, 2003)**:** if the provers are restricted to a ***polynomial number*** of entangled qubits then MIP* $\subseteq$ NEXP
- **Corollary:** XOR-MIP* $\subseteq$ NEXP

Open Questions

- MIP* versus NEXP?
- What happens with more than two provers?
- Quantum communication between the provers and a quantum Verifier?
- How does “parallel repetition” work for quantum strategies?

THE END