Today

- 2-Prover Proof Systems
- Parallel Repetition
- Motivation: Hardness of Approximation
- Conjecture + Counterexample
- Theorem (Raz; Holenstein)
- Towards Proof

2-Prover Proof Systems Framework

2 provers + 1 verifier → 3 players in all

\[ \Phi \rightarrow P_A \rightarrow v \rightarrow v \rightarrow P_B \rightarrow x, y \rightarrow (x, y) \rightarrow \mu \rightarrow P_A \rightarrow \alpha \rightarrow x \rightarrow P_B \rightarrow y \rightarrow v \rightarrow P_A \rightarrow a \rightarrow v \rightarrow P_B \rightarrow b \rightarrow \text{Accept if } V(x, y, a, b) = 1 \]
In English

1. Prover ("Criminals") being interrogated by ("Interrogator") Verifier; Verifier randomized.
2. Provers strategize together, but can't exchange question being asked. Must answer questions without coordination.
3. Verifier determines their innocence/guilt based on answers.

Q: What is \( \max \) (over strategies) of Prover's Verifier's acceptance prob.

Formally: Game = \((U, V)\) \(\{U \text{ supported on } X \times Y\}\) \(\{V: X \times Y \times A \times B \rightarrow \{0,1\}\}\)

- Strategy = \(f: X \rightarrow A\) \(g: Y \rightarrow B\)

- Value \((f, g) = \mathbb{E}_{(x, y) \sim U} \left[ V(x, y, f(x), g(y)) \right] \)

- Value \((\text{Game}) = \max_{f, g} \{ \text{value}(f, g) \} \)
Example: **Odd-Cycle Game**

- \( G = (V, E) \), \( V = \mathbb{Z}_n \), \( E = \{ (i, i+1 \mod n) \} \)
- \( \mu = \frac{1}{2} (\text{unif}(E) + \text{unif}(i,i)) \)
- \( \text{Claim: } A = B = \{0,1\} \)
- \( V(a,y,a,b) = 1 \iff a = b \iff x = y \)

Claim: \( \text{Value}(\text{game}) = 1 - \Theta(\frac{1}{n}) \). [Exercise ?]

---

In English:

- Provers claiming \( \mathbb{Z}_n \) is 2-colorable (odd cycle is not!)

- Verifier picks edge \( e(u,v) \) & asks A for \( x(u) \) & B for \( x(v) \)
  
  - accepts if \( x(u) + x(v) \)

- Unfortunately fails if Alice always says 0 & Bob always says 1.

- So w.p. \( \frac{1}{2} \) verify consistency \( x_{\text{Alice}}(u) = x_{\text{Bob}}(u) \)
  
  - w.p. \( \frac{1}{2} \) verify edge

- Strategy: Pick one edge \( x(v) = u \mod 2 \).
Parallel Repetition Problem:

- Can interrogator reduce prob. error by asking many questions?
  - Answer: yes. \( k \)-repetition \( \Rightarrow \) Value(\( k \)) \( k \).

- But: can you what if they're interrogator can only ask a many-part question.
  [Interview vs. Written Exam]

- How does error prob. behave?

Approximation Motivation

- Prover Game \( \equiv \) Generalized Graph\#Colorability

\( \mathcal{G}_1 = (V, E) \) a function

\( \forall i \in \mathbb{Z} : E \times \{0, 1\} \times \{0, 1\} \rightarrow \mathbb{Z} \)

\((u, v) \text{ validly colored if } V((u, v), X(u), X(v)) = 1\).

- 92: Well-known: \( \exists \) \( k \) approximation \( \epsilon \) 3-Color is hard to within \( 1 + 10^{-10} \).

Can we get \( 3k \) still approximate \( \epsilon \) \( k \) Real. Do nothing \( 10^{-10} \) is hard?
Parallel Repetition: ("Tensor Product", Repeated Game ...)

\[ G^k = (U^k, V^k) \]

\[ U^k = U \times U \times U \]

Supp on \( X^k \times Y^k \).

\[ V^k((x_1, \ldots, x_k), (y_1, \ldots, y_k), (a_1, a_2), (b_1, b_2)) = \prod_{i=1}^{k} V(x_i, y_i, a_i, b_i) \]

"Repeating Questions in Parallel"

"Allows provers to "coordinate" answers"

is Value\((G^k)\) = Value\((G)\)^k ?

Feige's Example

\[ X = \{1, 2\} \quad Y = \{3, 4\} \quad A = B = \{1, 2, 3, 4\} \]

\[ M = \text{wise}(X \times Y) \]

\[ V(x, y, a, b) = 1 \quad \text{if} \quad a = b \quad \text{and} \quad a \in \{x, y\} \]

In English: Verifier Pickers tosses two coins \(x \in \{1, 2\}\)

\(y \in \{3, 4\}\)

\(x\) sends to Alice & Bob. They must guess one of the coins. Value\((G)\) = \(1/2\).
2-fold repetition

- Alice $\leftarrow \exists x_1, x_2 \exists y_1, y_2 \rightarrow Bob$

- $\exists a_1, a_2 \exists b_1, b_2 \leftarrow$

- Accept if $a_i = b_i \land a_i \in \exists x_i, y_i \exists$ for $i = 1, 2$.

- Strategy: “Hope that $a_1 = y_2 - 2 \pmod{2}$”

  $\begin{align*}
  a_1 &= x_1 \\
  a_2 &= x_1 + 2
  \end{align*}$

  $\begin{align*}
  b_1 &= y_2 - 2 \\
  b_2 &= y_{\phi 2}
  \end{align*}$

  if Hope then win
  else lose

  $Pr[\text{Hope}] = \frac{1}{2}$

  value $(G_{\boxtimes 2}) = \frac{1}{2} = \text{Value}(G_1)$ !

  Clearly does not behave as expected.

Thm [Verbitsky]: $\exists G_1$ s.t. $\text{Value}(G_1) < 1$, $\forall \varepsilon > 0 \exists k$ s.t. $\text{Value}(G_1) \leq \varepsilon$. [Very weak]

Thm [Raz]: $\exists A, B, C = 0 \exists \varepsilon > 0$ s.t. $\forall G_1$ with $\text{Value}(G_1) \leq 1 - \varepsilon$

$\forall k$, $\text{Value}(G_{\boxtimes k}) \leq (1 - \varepsilon')^k$. [does not depend on $x_1$]
Would like to say: Fix $f, g: X^k \times Y^k \rightarrow A^k \times B^k$

$s_i$: $Pr \left[ \forall (x_i, y_i), f(x_i), g(y_i) \right] = 1 | \forall (x_j, y_j), f(x_j), g(y_j) \leq 1-\epsilon$

Problem: $(x_i, y_i)$ independent of $(x_{\bar{i}}, y_{\bar{i}})$ but $f(x_i), f(y_i)$ is not independent.

More Intrinsic Lemma:

$s \in \{x\}

Notation: $W_s = \text{Winning on } s

= \text{Event that } f, g \text{ win on } s.

\[
\forall (x_i, y_i), f(x_i), g(y_i) : 1 \quad \forall i \in s
\]

Lemma:

$s \in \{x\}$

$\exists x \geq 0 \text{ s.t. } \forall s \text{ with } \text{value}(s) \leq 1-\epsilon$

either

$Pr[W_s] \leq 2^{-\epsilon k}$

or

$\exists i \in S \text{ Pr}[W_i | W_s] \leq 1 - \epsilon^2$