25.1 2-Prover 1-Round Game

2-Prover 1-Round Game is shown in Figure 25.1. 

\((x,y) (X,Y)\) is correlated random variables. Verifier send \(x\) to Prover1 and send \(y\) to Prover2. The answer is belong to alphabet \(\Sigma\) where \(|\Sigma| = q\). However during the game there is no communication between two provers. Verifier will accept iff \(V(x,y,a,b) = 1\), where \(V : X \times Y \times \Sigma \times \Sigma\) is the verification function. This Game is important in PCPs and inapproximability.

Here is an example of 3-SAT. Suppose \(\phi\) is a 3-SAT instance. Then \(X\) denote clauses of \(\phi\) and \(Y\) denotes variables of \(\phi\). The answer is just an assignment of variables. \(V(c_j, x_i, \alpha, \beta) = 1\) if and only if \(\alpha\) satisfies \(c_j\) and \(\alpha | x_i = \beta\).

In this example, we have the following lemma.

**Lemma 25.1** If \(\phi\) satisfiable, there exist strategies that make Verifier accept with probability 1. If every assignment fails to satisfy \(\rho\) fraction of clauses, then for any strategy Verifier rejects with probability at least \(\rho/3\).

Here is the definition of the value of game.

**Definition 25.2** We denote the maximum probability that verifier accepts among all strategies to be the value of game.

\[
\text{val}(G) = w(G) = \max_{\Pi_1 : X \rightarrow \Sigma, \Pi_2 : Y \rightarrow \Sigma} [\mathbb{Pr}_{(x,y) \sim (X,Y)} [V(x,y,\Pi_1(x),\Pi_2(y)) = 1]]
\]

Here Prover1 and Prover2 do not communicate, but we can allow shared randomness, then we have:

\[
\text{val}(G) = w(G) = \max_{\Pi_1 : X \rightarrow \Sigma, \Pi_2 : Y \rightarrow \Sigma} [\mathbb{Pr}_{(x,y) \sim (X,Y), r \sim R} [V(x,y,\Pi_1(x,r),\Pi_2(y,r)) = 1]]
\]

which will not change the value of game.

25.2 \(n\)-repeated Game

In \(n\)-repeated Game. \((x_1,x_2) \ldots, (x_n,y_n)\) are iids with distribution \((X,Y)\). Prover1 read \(x_1, \ldots, x_n\) and response answers \(a_1, \ldots, a_n\), Prover2 read questions \(y_1, \ldots, y_n\) and response answers \(b_1, \ldots, b_n\). Verifier will accept if and only if \(\land_{i=1}^{n} V(x_i, y_i, a_i, b_i) = 1\).

It is trivial that \(w(G^n) \geq w(G)^n\) since we can just set \(\Pi_1^{(n)}(x_1, \ldots, x_n) = (\Pi_1(x_1), \ldots, \Pi_1(x_n))\), and the same with \(\Pi_2\) to reach the bound. In [FRS88] they claim that \(w(G^n) = w(G)^n\). However this claim is false.
Lecture 25: Parallel Repetition Theorem

Here is a counterexample. Suppose \((x, y)\) are uniform independent random bits. \(\Sigma = \{1, 2\} \times \{0, 1\}\).

\[ V(x, y, a, b) = 1 \text{ if and only if } a = b = (i, c) \text{ and Prover } i \text{ got the bit } c. \]

In this example, \(w(G) = 1/2\). The strategy is trivial. Since at least 1 prover must guess other prover’s question for verifier to accept, the value of game can not be more than 1/2.

Now let’s consider about \(G^2\). Here we denote \(W_i\) as the verifier is right on question \(i\). Then

\[ \Pr(W_1 \cap W_2) = \Pr(W_1)\Pr(W_2|W_1) \]

Here the first term can not be improved, but we can improve second term to be more than 1/2 utilizing information in the first round. Let the strategy of Prover1 to be \(a_1 = (1, x_1), a_2 = (2, x_1)\) and the strategy of Prover2 to be \(b_1 = (1, y_2), b_2 = (2, y_2)\). Therefore \(\Pr(W_2|W_1) = 1\) and verifier accepts when \(x_1 = y_2\), so \(w(G^2) = 1/2\).

Exercise: If \(n\) is even, \(w(G^n) = 2^{-n/2}\) in this counterexample.

So the value of game does go down exponentially.

25.3 Parallel Repetition Theorem

**Theorem 25.3 (Parallel Repetition Theorem)** For all games \(G\), if \(w(G) = 1 - \delta\) then

\[ w(G^n) \leq 2^{-\Omega\left(\frac{\delta q}{\ln n}\right)} = 2^{-\Omega_{\delta,q}(n)} \]

where \(q\) is the size of answer alphabet.

Here we use the simplification proof in [Holestein’ 07].

**Lemma 25.4 (Main Lemma)** There exist \(\gamma = \gamma(q, \delta)\) such that for all \(S \subset [n]\) satisfied \(|S| \leq \gamma n, \Pr[W_S] \geq 2^{-\gamma n}\), there exist \(i\) such that

\[ \Pr[W_i|W_S] \leq 1 - \delta/2 \]

where \(W_S\) denotes verifier accepts on all coordinates in \(S\).
Proof: [Proof of Theorem 25.3] Lemma 25.4 implies the theorem directly. Because based on Lemma 25.4, we can pick \( i_1, i_2, \ldots, i_l \) with \( l \leq \gamma n \), such that

\[
\Pr[W_{i_j} | W_{i_{j-1}}, \ldots, W_{i_1}] \leq 1 - \delta/2
\]

Therefore

\[
w(G^n) \leq \max[2^{-\gamma n}, (1 - \delta/2)^{\gamma n}]
\]

To prove Lemma 25.4, the intuition is for fixed \( S \), use the strategy for \( G^n \) to deal with \( G \). Fix some \( I \), given \((x, y) \sim (X, Y)\), use shared randomness to generate \((n - 1)\) other questions such that when \((x, y)\) is placed in \( i \)-th coordinate and rest of questions are placed in other coordinates, the resulting distribution is statistically close to \(((x_1, y_1), \ldots, (x_n, y_n) | W_S)\).

There are two main obstacles in this construction.

1. We must need \( i \) to satisfy \((X_i, Y_i) \sim (X, Y)\). This is not hard to ensure.

2. We must sample remaining \( n - 1 \) coordinates without any communication.
The detailed proof of Lemma 25.4 will be mentioned in the next lecture.