The PCP theorem and the complexity of 2 prover games

A game G is described four finite nonempty sets $\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}$, a probability distribution $\mu : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}_+$ (we assume that for all x, y, $\mu(x, y)$ can be represented by abitstring of length at most $\lceil \log(|\mathcal{X}||\mathcal{Y}|) \rceil$) and a table $V : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0, 1\}$. To see it as the input of a computational problem which should represent G using a finite bitstring. One way to represent such a G is by the following string:

$$\mathrm{repr}(G) := \mathrm{bin}(|\mathcal{X}|) \mid \mathrm{bin}(|\mathcal{Y}|) \mid \mathrm{bin}(|\mathcal{A}|) \mid \mathrm{bin}(|\mathcal{B}|) \mid \mathrm{bin}_{\lceil \log(|\mathcal{X}||\mathcal{Y}|) \rceil}(\mu(x, y))_{x,y \in \mathcal{X},\mathcal{Y}} \mid (V(x, y, a, b))_{x,y,a,b \in \mathcal{X},\mathcal{Y},\mathcal{A},\mathcal{B}}$$

where $\mathrm{bin}(n)$ is the binary representation of the integer n, $\mathrm{bin}_k(\alpha)$ for $\alpha \in (0, 1)$ is the binary representation of α truncated after k bits, $|$ is a separator symbol. To represent the lists for μ and V, we have implicitly chosen a fixed orders on $\mathcal{X} \times \mathcal{Y}$ and $\mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B}$ and the list is represented as a separated sequence of bitstrings in the corresponding order. Note that the size of the string representing G contains $O(|\mathcal{X}||\mathcal{Y}||\mathcal{A}||\mathcal{B}|)$ symbols.

Given a game G, we can define its value

$$\mathrm{val}(G) = \sup_{p,q} \sum_{x,y} \mu(x, y) \sum_{a,b} V(x, y, a, b) p(a|x) q(b|y) \ ,$$

where p, q are such that $p(.|x), q(.|y)$ are probability distributions for every x, y. As the function is linear in p and q, we can restrict the optimization to p, q satisfying $p(a|x), q(b|y) \in \{0, 1\}$, i.e., deterministic strategies. We can then define the promise problem ρ-GapGameVal as follows: for any G as above if $\mathrm{val}(G) = 1$, then $\mathrm{repr}(G)$ is a YES instance and if $\mathrm{val}(G) \leq \rho$, then $\mathrm{repr}(G)$ is a NO instance

Proposition 0.1. *There exists a constant $\rho < 1$ such that promise problem ρ-GapGameVal is NP-hard in the sense that for any $L \in NP$, there is a polynomial time function f such that if $x \in L$, then $f(x)$ is a YES instance of ρ-GapGameVal and if $x \notin L$, $f(x)$ is a NO instance of ρ-GapGameVal.*

Proof We are going to use the NP-hardness of ρ-Gap3Sat (see the chapter on PCP theorem in the Arora-Barak book https://theory.cs.princeton.edu/complexity/book.pdf). An instance of Gap3Sat is given by a set of variables labeled by $[n]$, and a set of constraints labeled by $[m]$. A constraint $i \in [m]$ contains three variables $v_1(i), v_2(i), v_3(i) \in [n]$ and each variable appears with a negation or not we represent this with $w_1(i), w_2(i), w_3(i) \in \{0, 1\}$. For example, a constraint $x_1 \vee \bar{x}_{10} \vee x_{12}$ is represented by $v_1 = 1, v_2 = 10, v_3 = 12$ and $w_1 = 0, w_2 = 1, w_3 = 0$. The game we construct is as follows: $\mathcal{X} = [n], \mathcal{Y} = [m], \mathcal{A} = \{0, 1\}, \mathcal{B} = \{0, 1\}^3$. Then $\mu(v, i) = \frac{1}{3m}$ if variable $v \in \{v_1(i), v_2(i), v_3(i)\}$ and otherwise 0. Also we set $V(v, i, a, (b_1, b_2, b_3)) = 1$ when b_1, b_2, b_3 satisfies the constraint i (i.e., $\bar{b}_1^{w_1(i)} \vee \bar{b}_2^{w_2(i)} \vee \bar{b}_3^{w_3(i)} = 1$, where the notation $\bar{b}^w$ refers to b if $w = 0$ and $\bar{b}$ if $w = 1$) and $a = b_j$ where $v = v_j(i)$. And V is set to 0 otherwise. Note that all the operations take a time which is polynomial in n and m so this is a valid reduction.

Now assume that the instance of Gap3Sat is satisfiable. Then the game has a strategy than wins with probability 1: just take a satisfying assignment and both players answer according to this. Conversely, assume the game has a winning probability $1 - \delta$. Then let us construct an assignment of the variables. We may assume that the strategy achieving $1 - \delta$ is deterministic. Thus, the first player's strategy is described by a function $\sigma : [n] \to \{0, 1\}$ and we interpret this as an assignment to the variables. Then the probability of losing the game can be written as

$$\frac{1}{3m} \sum_{i \in [m]} \sum_{j=1}^{3} \mathbf{1}_{\sigma(v_j(i)) \neq b_j(i) \text{ OR } \bar{b}_1(i)^{w_1(i)} \vee \bar{b}_2(i)^{w_2(i)} \vee \bar{b}_3(i)^{w_3(i)} = 0}$$

We know that this quantity is $\leq \delta$. We are on the other hand interested in

$$\begin{aligned}\frac{1}{m}\sum_{i\in[m]}\mathbf{1}_{\overline{\sigma(v_1(i))}^{w_1(i)}\vee\overline{\sigma(v_2(i))}^{w_2(i)}\vee\overline{\sigma(v_3(i))}^{w_3(i)}=0} &\leq \frac{1}{m}\sum_{i\in[m]}\mathbf{1}_{\bar{b}_1(i)^{w_1(i)}\vee\bar{b}_2(i)^{w_2(i)}\vee\bar{b}_3(i)^{w_3(i)}=0}\mathbf{1}_{\sigma(v_j(i))=b_j(i)\forall j\in\{1,2,3\}} \\ &+\frac{1}{m}\sum_{i\in[m]}\sum_{j=1}^{3}\mathbf{1}_{\sigma(v_j(i))\neq b_j(i)} \\ &\leq 6\delta\ .\end{aligned}$$

So the formula si $(1-6\delta)$-satisfiable and this concludes the proof of the converse. □

Note that we can even obtain the NP-hardness for any constant $\rho < 1$. This follows immediately from the parallel repetition theorem. In fact, we will give a reduction from ρ-GapGameVal to ϵ-GapGameVal for any $\epsilon > 0$. Take an instance G for ρ-GapGameVal and then consider the game G' obtained by parallel repetition G a constant $c(\rho, \epsilon)$ number of times. Then G' can be obtained in polynomial time from G, and if G had a value of 1, then so does G', and if G had a value $\leq \rho$, then G' has a value $\leq \epsilon$ if $c(\rho, \epsilon)$ is chosen appropriately.