Problem Set 5: Average Case Complexity
Due: Monday, May 27th

Worst-case to average-case reductions

Definition 1 (Discrete Log problem)**.**

Input: A cyclic group G, generator $g \in G$, and element $x \in G$.

Output: d such that $g^d = x$.

1. (**Easier-than-medium**) Fix G, g. Prove that if finding the discrete log of a worst case x is hard (i.e. no poly-time randomized algorithm), then it is also hard w.h.p. for a uniformly random x.

   Hint: Multiplying x by a uniformly random element gives a uniformly random element.

Average-case to worst-case reductions

Definition 2 (Planted Clique problem)**.**

Input: A graph G sampled either from $\mathcal{G}(n, 1/2)$, or from $\mathcal{G}(n, 1/2)$ plus a k-clique.

Output: Decide if G has a k-clique

Definition 3 (ε-best ε-Nash problem)**.**

Input: Payoff matrices $A, B \in [0,1]^{n \times n}$.

Output: Approximate, to within additive $\pm\varepsilon$, the maximum total payoff in any ε-Nash equilibrium.

(Note that unlike finding any Nash equilibrium, this is a decision problem.)

2. (**Guided**) Let $\varepsilon > 0$ be a sufficiently small constant and $k = O(\log(n))$ be sufficiently large. Prove that if the Planted Clique problem (with parameter k) is hard, then the ε-best ε-Nash problem is hard.

   (a) **From a graph to a game**

   Given graph G (input to the Planted Clique problem), construct a two-player identical interest[1] $|V| \times |V|$ game with payoffs in $\{0, 1\}$ that satisfies the following:

   Completeness If G has a k-clique, then the game has a mixed Nash equilibrium with expected payoff 1 for both players, and such that Alice's (respectively Bob's) mixed strategy is uniform over a subset S_A of her actions (resp. S_B of his actions) of size $|S_A|, |S_B| = k$.

   Soundness If G is sampled from $\mathcal{G}(|V|, 1/2)$, then with high probability for any mixed strategy profile where Alice and Bob draw their actions uniformly from subsets of size $|S_A|, |S_B| \geq k$, the expected payoff to each player is at most 0.6.

   (b) **Forcing a large support**

   Let $m = \text{poly}(|V|)$ be sufficiently large. Show how to construct in (possibly randomized) polynomial time a zero-sum $|V| \times m$ game, where Alice's payoffs are in $\{-1.5, 0\}$ (and Bob's payoffs are in $\{0, 1.5\}$) that satisfies the following, with high probability:

   Completeness If Alice's strategy is uniform over a random subset $|S_A| = k$ of her actions, then her expected payoff (regardless of Bob's strategy) is at least -0.8.

   Soundness If Alice's strategy has support $\leq \log(|V|)$, then Bob can guarantee an expected payoff of 1.5.

   (c) **Putting it all together**

   The desiderata for the soundness guarantees in the previous two parts are incompatible. It is possible to make them match by strengthening both to hold assuming that Alice's strategy assigns δ probability on a subset of size $c\log(|V|)$ (for appropriate choice of constants $\delta, c > 0$). Namely, if Alice and Bob both assign at most δ probability on any subset of size $c\log(|V|)$, then their expected payoff in the first game is at most 0.6. If Alice assigns at least δ probability on a subset of size $c\log(|V|)$ in the second game[2], then Bob can guarantee an expected payoff of at least 1.5.

   Use the above strengthening of what you proved in the previous two parts to show that if the Planted Clique problem is hard, then the ε-best ε-Nash problem is hard.

[1] A game is called *identical interests* if for any choice of actions all players receive the same utility.

[2] Making this actually work requires modifying the game to so that Bob can have larger (but at most a constant) payoffs. They're still always non-negative.