Sample-Efficient Learning of Stackelberg Equilibria in General-Sum Games

Yu Bai  
Salesforce Research  
yu.bai@salesforce.com

Chi Jin  
Princeton University  
chij@princeton.edu

Huan Wang  
Salesforce Research  
huan.wang@salesforce.com

Caiming Xiong  
Salesforce Research  
cxiong@salesforce.com

Abstract

Real world applications such as economics and policy making often involve solving multi-agent games with two unique features: (1) The agents are inherently asymmetric and partitioned into leaders and followers; (2) The agents have different reward functions, thus the game is general-sum. The majority of existing results in this field focuses on either symmetric solution concepts (e.g. Nash equilibrium) or zero-sum games. It remains open how to learn the Stackelberg equilibrium—an asymmetric analog of the Nash equilibrium—in general-sum games efficiently from noisy samples. This paper initiates the theoretical study of sample-efficient learning of the Stackelberg equilibrium, in the bandit feedback setting where we only observe noisy samples of the reward. We consider three representative two-player general-sum games: bandit games, bandit-reinforcement learning (bandit-RL) games, and linear bandit games. In all these games, we identify a fundamental gap between the exact value of the Stackelberg equilibrium and its estimated version using finitely many noisy samples, which can not be closed information-theoretically regardless of the algorithm. We then establish sharp positive results on sample-efficient learning of Stackelberg equilibrium with value optimal up to the gap identified above, with matching lower bounds in the dependency on the gap, error tolerance, and the size of the action spaces. Overall, our results unveil unique challenges in learning Stackelberg equilibria under noisy bandit feedback, which we hope could shed light on future research on this topic.

1 Introduction

Real-world problems such as economic design and policy making can often be modeled as multi-agent games that involves two levels of thinking: The policy maker—as a player in this game—needs to reason about the other player’s optimal behaviors given her decision, in order to inform her own optimal decision making. Consider for example the optimal taxation problem in the AI Economist [53], a game modeling a real-world social-economic system involving a leader (e.g. the government) and a group of interacting followers (e.g. citizens). The leader sets a tax rate which determines an economics-like game for the followers; the followers then play in this game with the objective to maximize their own reward (such as individual productivity). However, the goal of the leader is to maximize her own reward (such as overall equality) which is in general different from the followers’ rewards, making these games general-sum [38]. Such two-level thinking appears broadly in other applications as well such as in automated mechanism design [11, 12], optimal auctions [10, 14], security games [43], reward shaping [25], and so on.

Another key feature in such games is that the players are asymmetric, and they act in turns: the leader first plays, then the follower sees the leader’s action and then adapts to it. This makes symmetric solution concepts such as Nash equilibrium [30] not always appropriate. A more natural solution concept for these games is the Stackelberg equilibrium: the leader’s optimal strategy, assuming the followers play their best response to the leader [42, 13]. The Stackelberg equilibrium is often the desired solution concept in many of the aforementioned applications. Furthermore, it is of compelling interest to understand the learning of Stackelberg equilibria from samples, as it is often the case that we can only learn about the game through interactively deploying policies and observing the (noisy) feedback from the game [53]. This may be the case even when the game rules are perfectly known but not yet represented in a desired form, as argued in the line of work on empirical game theory [50, 48, 20].

Despite the motivations, theoretical studies of learning Stackelberg equilibria in general-sum games remain open, in particular when we can only learn from noisy samples of the rewards. A line of work provides guarantees for finding Stackelberg equilibria in general-sum games, but restricts attention to either the full observation setting (so that the exact game is observable) or with an exact best-response oracle [13, 27, 47, 34]. These results lay out a foundation for analyzing the Stackelberg equilibrium, but do not generalize to the bandit feedback setting in which the game can only be learned from random samples of the rewards. Another line of work considers the sample complexity of learning the Nash equilibrium in Markov games [35, 4, 5, 28, 51, 52], which also do not imply algorithms for finding the Stackelberg equilibrium in these games as the Nash is in general different from the Stackelberg equilibrium in general-sum games.

In this work, we study the sample complexity of learning Stackelberg equilibrium in general-sum games. We focus on general-sum games with two players (one leader and one follower), in which we wish to learn an approximate Stackelberg equilibrium for the leader from random samples. Our contributions can be summarized as follows.

- As a warm-up, we consider bandit games in which the two players play an action in turns and observe their own rewards. We identify a fundamental gap between the exact Stackelberg value and its estimated version from finite samples, which cannot be closed information-theoretically regardless of the algorithm (Section 3.1). We then propose a rigorous definition gapε for this gap, and show that it is possible to sample-efficiently learn the (gapε+ε)-approximate Stackelberg equilibrium with \( O(AB/\varepsilon^2) \) samples, where \( A, B \) are the number of actions for the two players. We further show a matching lower bound \( \Omega(AB/\varepsilon^2) \) (Section 3.2). We also establish similar results for learning Stackelberg in simultaneous matrix games (Appendix B).

- We consider bandit-RL games in which the leader’s action determines an episodic Markov Decision Process (MDP) for the follower. We show that a (gapε+ε) approximate Stackelberg equilibrium for the leader can be found in \( O(HS^2AB/\varepsilon^2) \) episodes of play, where \( H, S \) are the horizon length and number of states for the follower’s MDP, and \( A, B \) are the number of actions for the two players (Section 4). Our algorithm utilizes recently developed reward-free reinforcement learning techniques to enable fast exploration for the follower within the MPDs.

- Finally, we consider linear bandit games in which the action spaces for the two players can be arbitrarily large, but the reward is a linear function of a \( d \)-dimensional feature representation of the actions. We design an algorithm that achieves \( \tilde{O}(d^2/\varepsilon^2) \) sample complexity upper bound for linear bandit games (Section 5). This only depends polynomially on the feature dimension instead of the size of the action spaces, and has at most an \( \tilde{O}(d) \) gap from the lower bound.

1.1 Related work

Since the seminal paper of [46], notions of equilibria in games and their algorithmic computation have received wide attention [see, e.g., 9, 41]. For the scope of this paper, this section focuses on reviewing results that related to learning Stackelberg equilibria.

Learning Stackelberg equilibria in zero-sum games The first category of results study two-player zero-sum games, where the rewards of the two players sum to zero. Most results along this line focus on the bilinear or convex-concave setting [see, e.g., 21, 32, 31, 37, 16], where the Stackelberg equilibrium coincide with the Nash equilibrium due to Von Neumann’s minimax theorem [46]. Results for learning Stackelberg equilibria beyond convex-concave setting are much more recent,
with Rafique et al. [36], Nouiehed et al. [33] considering the nonconvex-concave setting, and Fiez et al. [15], Jin et al. [19], Marchesi et al. [29] considering the nonconvex-nonconcave setting. Marchesi et al. [29] provide sample complexity results for learning Stackelberg with infinite strategy spaces, using discretization techniques that may scale exponentially in the dimension without further assumptions on the problem structure.

We remark that a crucial property of zero-sum games is that any two strategies giving similar rewards for the follower will also give similar rewards for the leader. This is no longer true in general-sum games, and prevents most statistical results for learning Stackelberg equilibria in the zero-sum setting from generalizing to the general-sum setting.

Learning Stackelberg equilibria in general-sum games

The computational complexity of finding Stackelberg equilibria in games with simultaneous play (“computing optimal strategy to commit to”) is studied in [13, 26, 47, 22, 1, 7]. These results assume full observation of the payoff function, and show that several versions of matrix games and extensive-form (multi-step) games admit polynomial time algorithms. Vasal [45] designs computationally efficient algorithms for computing Stackelberg in certain “conditionally independent controlled” Markov games.

Another line of work considers learning Stackelberg with a “best response oracle” [27, 6, 34], that returns the follower’s exact best response strategy when a leader’s strategy is queried. This oracle and the noisy reward oracle we assume are in general incomparable (cannot simulate each other regardless of the number of queries), and thus our sample complexity results do not imply each other. The recent work of Sessa et al. [39] proposes the StackelUCB algorithm to sample-efficiently learn a Stackelberg game where the opponent’s response function has a linear structure in a certain kernel space, and the observation noise is added in the action space instead of the reward (thus a different noisy feedback model from ours).

Lastly, Fiez et al. [15] study the local convergence of first-order algorithms for finding Stackelberg equilibria in general-sum games. Their result also assumes exact feedback and do not allow sampling errors. The AI Economist [53] studies the optimal taxation problem by learning the Stackelberg equilibrium via a two-level reinforcement learning approach.

Learning equilibria in Markov games

A recent line of results [4, 5, 51, 52] consider learning Markov games [40]—a generalization of Markov decision process to the multi-agent setting. We remark that all three settings studied in this paper can be cast as special cases of general-sum Markov games, which is studied by [28]. In particular, Liu et al. [28] provides sample complexity guarantees for finding Nash equilibria, correlated equilibria, or coarse correlated equilibria of the general-sum Markov games. These Nash-finding algorithms are related to our setting, but do not imply results for learning Stackelberg (see Section 3.2 and Appendix C.5 for detailed discussions).

2 Preliminaries

Bandit games

A general-sum two-player bandit game can be described by a tuple \( M = (A, B, r_1, r_2) \), which defines the following game played by two players, a leader and a follower:

- The leader plays an action \( a \in A \), with \(|A| = A\).
- The follower sees the action played by the leader, and plays an action \( b \in B \), with \(|B| = B\).
- The follower observes a (potentially random) reward \( r_2(a, b) \in [0, 1] \). The leader also observes her own reward \( r_1(a, b) \in [0, 1] \).

Note that this is a special case of a general-sum turn-based Markov game with two steps [40, 4]. This game is also a turn-based variant of the simultaneous matrix game considered in [13, 27] (for which we also provide results in Appendix B).

Best response, Stackelberg equilibrium

Let \( \mu_i(a, b) := \mathbb{E}[r_i(a, b)] \) (\( i = 1, 2 \)) denote the mean rewards. For each leader action \( a \), the best response set \( \text{BR}_0(a) \) is the set of follower actions that maximize \( \mu_2(a, \cdot) \):

\[
\text{BR}_0(a) := \left\{ b : \mu_2(a, b) = \max_{b' \in B} \mu_2(a, b') \right\}.
\] (1)
Given the best-response set \( BR_0(a) \), we define the function \( \phi_0 : A \to [0, 1] \) as the leader’s value function when the follower plays the worst-case best response (henceforth the “exact \( \phi \)-function”):

\[
\phi_0(a) := \min_{b \in BR_0(a)} \mu_1(a, b),
\]

This is the value function for the leader action \( a \), assuming the follower plays the best response to \( a \) and breaks ties in the best response set against the leader’s favor. This is known as pessimistic tie breaking and provides a worst-case guarantee for the leader [13]. We remark that here restricting \( b \) to pure strategies (deterministic actions) is without loss of generality, as there is at least one pure strategy that maximizes \( \mu_2(a, \cdot) \) and (among the maximizers) minimize \( \mu_1(a, \cdot) \), among all mixed strategies.

The Stackelberg Equilibrium (henceforth also “Stackelberg”) for the leader is the “best response to a pure strategies” problem of [13]). We also remark that, while we consider pessimistic tie breaking and provides a worst-case guarantee for the leader [13]. We remark that here restricting pessimistic tie breaking (definition (2)) in this paper, similar results hold in the optimistic setting as well in which the follower breaks ties in favor of the leader. We defer the statements and proofs of these results to Appendix A.

**Real-world example (AI Economist):** Consider the following (simplified) optimal taxation problem in the AI Economist [53] as an example of a bandit game. The government (leader) determines the tax rate \( \alpha \in A \) for the follower. The citizen (follower) then chooses the amount of labor \( b \in B \) she wishes to perform. The rewards for the two players are different in general: For example, the citizen’s reward \( r_2(a, b) \) can be her post-tax income per labor, and the government’s reward \( r_1(a, b) \) can be a weighted average of its tax income and some measure of the citizen’s welfare (e.g. not too much labor). We remark that the actual AI Economist is more similar to a bandit-RL game where the follower plays sequentially in an MDP determined by the leader, which we study in Section 4.

**Sample-efficient learning with bandit feedback** In this paper we consider the bandit feedback setting, that is, the algorithm cannot directly observe the mean rewards \( \mu_1(\cdot, \cdot) \) and \( \mu_2(\cdot, \cdot) \), and can only query \((a, b)\) and obtain random samples \((r_1(a, b), r_2(a, b))\). Our goal is to determine the number of samples in order to find an approximate maximizer of \( \phi_0(a) \).

Note that the bandit feedback setting assumes observation noise in the rewards. As we will see in Section 3, this noise turns out to bring in a fundamental challenge for learning Stackelberg equilibria that is not present in (and thus not directly solved by) existing work on learning Stackelberg, which assumes either exact observation of the mean rewards [13, 26], or the best-response oracle that can query \( a \) and obtain the exact best response set \( BR_0(a) \) [27, 34].

**Markov decision processes** We also present the basics of a Markov Decision Processes (MDPs), which will be useful for the bandit-RL games in Section 4. We consider episodic MDPs defined by a tuple \((H, S, B, d, \mathbb{P}, r)\), where \( H \) is the horizon length, \( S \) is the state space, \( B \) is the action space, \( \mathbb{P} = \{P_h(\cdot|s, b) : h \in [H], s \in S, b \in B\} \) is the transition probabilities, and \( r = \{r_h : S \times B \to [0, 1], h \in [H]\} \) are the (potentially random) reward functions. A policy \( \pi = \{\pi_h(\cdot|s) \in \Delta_B : h \in [H], s \in S\} \) for the player is a set of probability distributions over actions given the state.

In this paper we consider the exploration setting as the protocol of interacting with MDPs, similar as in [3, 17]. The learning agent is able to play episodes repeatedly, where in each episode at step \( h \in \{1, \ldots, H\} \), the agent observes state \( s_h \in S \), takes an action \( b_h \sim \pi_h(\cdot|s_h) \), observes her reward \( r_h = r_h(s_h, b_h) \in [0, 1] \), and transits to the next state \( s_{h+1} \sim P_h(\cdot|s_h, b_h) \). The initial state is received from the MDP: \( s_1 \sim d(\cdot) \). The overall value function (return) of a policy \( \pi \) is defined as

\[
V(\pi) := \mathbb{E}_\pi \left[ \sum_{h=1}^{H} r_h(s_h, b_h) \right].
\]

1The notation \( B \) indicates that the MDP is played by the follower (cf. Section 4); we reserve \( A \) as the leader’s action space in this paper.
3 Warm-up: bandit games

3.1 Hardness of maximizing $\phi_0$ from samples

Given the exact $\phi$-function $\phi_0$ (2), a natural notion of approximate Stackelberg equilibrium is to find an action $\hat{a}$ that is $\varepsilon$ near-optimal for maximizing $\phi_0$:

$$\phi_0(\hat{a}) \geq \max_{a \in A} \phi_0(a) - \varepsilon. \quad (4)$$

However, the following lower bound shows that, in the worst case, it is hard to find such $\hat{a}$ from finite samples.

**Theorem 1** ($\Omega(1)$ lower bound for maximizing $\phi_0$). For any sample size $n$ and any algorithm for maximizing $\phi_0$ that outputs an action $\hat{a} \in A$, there exists a bandit game with $A = B = 2$ on which the algorithm must suffer from $\Omega(1)$ error with probability at least $1/3$:

$$\phi_0(\hat{a}) \leq \max_{a \in A} \phi_0(a) - 1/2.$$

Theorem 1 shows that, no matter how large the sample size $n$ is, any algorithm in the worst-case have to suffer from an $\Omega(1)$ lower bound for maximizing $\phi_0$ (i.e. determining the Stackelberg equilibrium for the leader). This result stems from a hardness of determining the best response $\text{BR}_0(a)$ exactly from samples. (See Table 2 for the construction of the hard instance and Appendix C.1 for the full proof of Theorem 1.) This is in stark contrast to the standard $1/\sqrt{n}$ type learning result in finding other solution concepts such as the Nash equilibrium [4, 28], and suggests a new fundamental challenge to learning Stackelberg equilibrium from samples.

3.2 Learning Stackelberg with value optimal up to gap

The lower bound in Theorem 1 shows that approximately maximizing $\phi_0$ is information-theoretically hard. Motivated by this, we consider in turn a slightly relaxed notion of optimality, in which we consider maximizing $\phi_0$ only up to the gap between $\phi_0$ and its counterpart using $\varepsilon$-approximate best responses. More concretely, define the $\varepsilon$-approximate versions of the best response set and $\phi$-function as

$$\phi_\varepsilon(a) := \min_{b \in \text{BR}_\varepsilon(a)} \mu_1(a, b),$$

$$\text{BR}_\varepsilon(a) := \left\{ b \in B : \mu_2(a, b) \geq \max_{b'} \mu_2(a, b') - \varepsilon \right\}.$$

These definitions are similar to the vanilla $\text{BR}_0$ and $\phi_0$ in (1) and (2), except that we allow any $\varepsilon$-approximate best response to be considered as a valid response to the leader action. Observe we always have $\text{BR}_\varepsilon(a) \supseteq \text{BR}_0(a)$ and $\phi_\varepsilon(a) \leq \phi_0(a)$. We then define the gap of the game for any $\varepsilon \in (0, 1)$ as

$$\text{gap}_\varepsilon := \max_{a \in A} \phi_0(a) - \max_{a \in A} \phi_\varepsilon(a) \geq 0. \quad (5)$$

This gap is discontinuous in $\varepsilon$ in general, and can be as large as $\Theta(1)$ for any $\varepsilon > 0$ without additional assumptions on the relation between $\mu_1$ and $\mu_2$. See Figure 1 for an illustration for a typical $\max_{a \in A} \phi_\varepsilon(a)$ against $\varepsilon$.

With the definition of the gap, we are now ready to state our main result, which shows that it is possible to sample-efficiently learn Stackelberg Equilibria with value up to $(\text{gap}_\varepsilon + \varepsilon)$. The proof can be found in Appendix C.3.

---

2This gap could be small when $\mu_1$ and $\mu_2$ have certain relations, such as zero-sum or cooperative structure. See Appendix C.6 for more discussions.
Algorithm 1 Learning Stackelberg in bandit games

**Require:** Target accuracy $\varepsilon > 0$.

1. Query each $(a, b) \in A \times B$ for $N$ times and obtain $\{r_1^{(j)}(a, b), r_2^{(j)}(a, b)\}_{j=1}^N$.
2. Construct empirical estimates of the means $\hat{\mu}_1(a, b) = \frac{1}{N} \sum_{j=1}^N r_1^{(j)}(a, b)$ for $i = 1, 2$.
3. Construct approximate best response sets and values for all $a \in A$:
   \[
   \hat{\phi}_{3\varepsilon/4}(a) := \min_{b \in BR_{3\varepsilon/4}(a)} \hat{\mu}_1(a, b), \quad \text{where} \quad \hat{BR}_{3\varepsilon/4}(a) := \left\{ b : \hat{\mu}_2(a, b) \geq \max_{b' \in B} \hat{\mu}_2(a, b') - 3\varepsilon/4 \right\}.
   \]
4. Output $(\hat{a}, \hat{b})$, where $\hat{a} = \arg\max_{a \in A} \hat{\phi}_{3\varepsilon/4}(a), \quad \hat{b} = \arg\min_{b \in \hat{BR}_{3\varepsilon/4}(\hat{a})} \hat{\mu}_1(\hat{a}, b)$.

**Theorem 2** (Learning Stackelberg in bandit games). For any bandit game and $\varepsilon \in (0, 1)$, Algorithm 1 outputs $(\hat{a}, \hat{b})$ such that with probability at least $1 - \delta$,

\[
\phi_0(\hat{a}) \geq \phi_{\varepsilon/2}(\hat{a}) \geq \max_{a \in A} \phi_0(a) - \text{gap}_\varepsilon - \varepsilon,
\]

\[
\mu_2(\hat{a}, \hat{b}) \geq \max_{b' \in B} \mu_2(\hat{a}, b') - \varepsilon
\]

with $n = \tilde{O}(AB/\varepsilon^2)$ samples, where $\tilde{O}(\cdot)$ hides log factors. Further, the algorithm runs in $O(n) = \tilde{O}(AB/\varepsilon^2)$ time.

**Implications; Overview of algorithm** Theorem 2 shows that it is possible to learn $\hat{a}$ that maximizes $\phi_0(a)$ up to $(\text{gap}_\varepsilon + \varepsilon)$ accuracy, using $\tilde{O}(AB/\varepsilon^2)$ samples. The quantity $\text{gap}_\varepsilon$ is not bounded and can be as large as $\Theta(1)$ for any $\varepsilon$ (see Lemma C.1 for a formal statement); however the gap is non-increasing as we decrease $\varepsilon$. In the situation where for every $a$ the best follower action for $\mu_2(\cdot, \cdot)$ is at least $\varepsilon_0$-better than the second best action, then for $\varepsilon < \varepsilon_0$ we have $\text{gap}_\varepsilon = 0$ and Theorem 2 implies an $\varepsilon$-optimal Stackelberg guarantee. In general, Theorem 2 presents a “best-effort” positive result for learning Stackelberg under this relaxed notion of optimality. To the best of our knowledge, this is the first result for sample-efficient learning of Stackelberg equilibrium in general-sum games with noisy bandit feedbacks. We remark that Theorem 2 also provides a near-optimality guarantee for $\phi_{\varepsilon/2}(\hat{a})$ which is slightly stronger than $\phi_0$ (since $\phi_{\varepsilon/2}(\hat{a}) \leq \phi_0(\hat{a})$), and guarantees the learned $\hat{b}$ is indeed an $\varepsilon$-approximate best response of $\hat{a}$.

From a more practical point of view, Theorem 2 (and our later results on bandit-RL games and linear bandit games) spells out concretely the sample size required to learn an $\varepsilon$-approximate Stackelberg, in terms of the scaling with problem parameters. For instance, in the AI Economist example, $A$ is the number of tax rate choices for the government, and $B$ is the number of actions for the citizen, and our results show that there exist an algorithm with sample complexity polynomial in $A$, $B$, and $1/\varepsilon$.

The main step in Algorithm 1 is to construct approximate best response sets $\hat{BR}_{3\varepsilon/4}(a)$ for all $a \in A$ based on the empirical estimates of the rewards. Through concentration, we argue that $\hat{BR}_{3\varepsilon/4}(a)$ is a good approximation of the true best response sets in the sense that $BR_{\varepsilon/2}(a) \subseteq \hat{BR}_{3\varepsilon/4}(a) \subseteq BR_{\varepsilon}(a)$ holds for all $a \in A$, from which the Stackelberg guarantee follows.

**Irreducibility to Nash-finding algorithms** We also remark that our bandit game is equivalent to a turn-based general-sum Markov game with two steps, $A$ states, and $(A, B)$ actions [4]. Further, the Stackelberg equilibrium $\alpha_a$, along with a follower policy that plays the best response (with pessimistic tie-breaking) constitutes a Nash equilibrium for that Markov game (see Appendix C.5 for a formal statement and proof). However, existing Nash-finding algorithms for general-sum Markov games such as Multi1-Nash-VI [28] do not imply an algorithm for finding the Stackelberg equilibrium. This is because general-sum games have multiple Nash equilibria (with different values) in general [38], and these existing Nash-finding algorithms cannot pre-specify which Nash to output.

**Lower bound** We accompany Theorem 2 by an $\Omega(AB/\varepsilon^2)$ sample complexity lower bound, showing that Theorem 2 achieves the optimal sample complexity up to logarithmic factors.
Theorem 3 (Lower bound for bandit games). There exists an absolute constant $c > 0$ such that the following holds. For any $\varepsilon \in (0, c)$, $g \in [0, c)$, any $A, B \geq 3$, and any algorithm that queries $N \leq c[AB/\varepsilon^2]$ samples and outputs an estimate $\hat{a} \in A$, there exists a bandit game $M$ on which $\text{gap}_\varepsilon = g$ and the algorithm suffers from $(g + \varepsilon)$ error:

$$\phi_{g/2}(\hat{a}) \leq \phi_0(\hat{a}) \leq \max_{a \in A} \phi_0(a) - g - \varepsilon$$

with probability at least $1/3$.

This lower bound shows the tightness of Theorem 2, and suggests that $(\text{gap}_\varepsilon + \varepsilon)$ suboptimality is perhaps a sensible learning goal, as for any algorithm and any value of $g \geq 0$ there exists a game with $\text{gap}_\varepsilon = g$, on which the algorithm has to suffer from $(g + \varepsilon)$ error, if the number of samples is at most $O(AB/\varepsilon^2)$. The proof of Theorem 3 is deferred to Appendix C.4.

4 Bandit-RL games

In this section, we investigate learning Stackelberg equilibrium in bandit-RL games, in which each leader’s action determines an episodic Markov Decision Process (MDP) for the follower. This setting extends the two-player bandit games by allowing the follower to play sequentially, and has strong practical motivations in particular in policy making problems involving sequential plays for the follower, such as the optimal taxation problem in the AI Economist [53].

**Setting** A bandit-RL game is described by the leader’s action set $A$ (with $|A| = A$), and a family of MDPs $M = \{M^a : a \in A\}$. Each leader action $a \in A$ determines an episodic MDP $M^a = (H, S, B, \mathbb{P}^a, r_{1,h}(a, \cdot), r_{2,h}(a, \cdot))$ that contains $H$ steps, $S$ states, $B$ actions, with two reward functions $r_1$ and $r_2$. In each episode of play,

- The leader plays action $a \in A$.
- The follower sees this action and enters the MDP $M^a$. She observes the deterministic $^3$ initial state $s_1$, and plays in $M^a$ with exploration feedback for one episode.
- While the follower plays in the MDP, she observes reward $r_{2,h}(a, s_h, b_h)$, whereas the leader also observes her own reward $r_{1,h}(a, s_h, b_h)$.

We let $\pi^b$ denote a policy for the follower, and let $V_1(a, \pi^b)$ and $V_2(a, \pi^b)$ denote its value functions (in $M^a$) for the leader and the follower respectively.

Similar as in bandit games, we define the $\varepsilon$-approximate best-response set $\text{BR}_\varepsilon(a)$ and the $\varepsilon$-approximate $\phi$-function $\phi_\varepsilon(a)$ for all $\varepsilon \geq 0$ as

$$\phi_\varepsilon(a) := \min_{\pi^b \in \text{BR}_\varepsilon(a)} V_1(a, \pi^b), \quad \text{where} \quad \text{BR}_\varepsilon(a) := \left\{ \pi^b : V_2(a, \pi^b) \geq \max_{\pi^b} V_2(a, \pi^b) - \varepsilon \right\}.$$

Define $\text{gap}_\varepsilon = \max_{a \in A} \phi_0(a) - \max_{a \in A} \phi_\varepsilon(a)$ similarly as in (5). We are interested in the number of episodes in order to find a $(\text{gap}_\varepsilon + \varepsilon)$ near-optimal Stackelberg equilibrium.

4.1 Algorithm description

At a high level, our algorithm for bandit-RL games is similar as for bandit games – query each leader action $a \in A$ sufficiently many times, let the follower learn the best response (i.e. best policy for the MDP $M^a$) for each $a \in A$, and then choose the leader action that maximizes the best response value function. This requires solving

$$\arg \max_{a \in A} \phi_{3\varepsilon/4}(a) := \arg \max_{a \in A} \min_{\pi^b \in \text{BR}_{3\varepsilon/4}(a)} \hat{V}_1(a, \pi^b), \quad \text{where} \quad \text{BR}_{3\varepsilon/4}(a) := \left\{ \pi^b : \hat{V}_2(a, \pi^b) \geq \max_{\pi^b} \hat{V}_2(a, \pi^b) - 3\varepsilon/4 \right\}. \quad (6)$$

$^3$The general case where $s_1$ is stochastic reduces to the deterministic case by adding a step $h = 0$ with a single deterministic initial state $s_{i_0}$, which only increases the horizon of the game by 1.
We now state our theoretical guarantee for Algorithm 2. The proof can be found in Appendix D.2.

Two technical challenges emerge as we instantiate (6). First, the follower not only needs to find her own best policy during the exploration phase, but also has to accurately estimate both her own and the leader’s reward over the entire approximate best response set $\hat{\text{BR}}_{3\epsilon/4}$ so as to make sure the estimates $\hat{V}_1(a, \pi^b)$ (i = 1, 2) are reliable. Standard fast PAC-exploration algorithms such as those in [3, 17] do not provide such guarantees. We resolve this by applying the reward-free learning algorithm of Jin et al. [18] for the follower to explore the environment efficiently while providing value concentration guarantees for multiple rewards and policies. We remark that we slightly generalize the guarantees of [18] to the situation where the rewards are random and have to be estimated from samples.

Second, the problem $\min_{\pi^b \in \text{BR}_{3\epsilon/4}(a)} \hat{V}_1(a, \pi^b)$ in (6) requires minimizing a value function over the near-optimal policy set of another value function. We build on the linear programming reformulation in the constrained MDP literature [2] to translate (6) into a linear program $\text{WorstCaseBestResponse}(\hat{M}^a, \hat{V}_2(a) - 3\epsilon/4)$. The description of this subroutine can be found in Algorithm 8 in Appendix D.1). Our full algorithm is described in Algorithm 2.

4.2 Main result

We now state our theoretical guarantee for Algorithm 2. The proof can be found in Appendix D.2.

**Theorem 4** (Learning Stackelberg in bandit-RL games). For any bandit-RL game and sufficiently small $\epsilon \leq O(1/H^2S^2)$, Algorithm 2 with $n = \tilde{O}(H^5S^2AB/\epsilon^2 + H^7S^4AB/\epsilon)$ episodes of play can return $(\hat{\alpha}, \hat{\pi}^b)$ such that with probability at least $1 - \delta$, 

$$\phi_0(\hat{\alpha}) \geq \phi_{\epsilon/2}(\hat{\alpha}) \geq \max_{a \in A} \phi_0(a) - \text{gap}_{\epsilon},$$

$$V_2(\hat{\alpha}, \hat{\pi}^b) \geq \max_{\pi^b} V_2(\hat{\alpha}, \pi^b) - \epsilon,$$

where $\tilde{O}(\cdot)$ hides $\log(HSAB/\delta\epsilon)$ factors. Further, the algorithm runs in $\text{poly}(HSAB/\delta\epsilon)$ time.

**Sample complexity, relationship with reward-free RL.** Theorem 4 shows that for bandit-RL games, the approximate Stackelberg Equilibrium (with value optimal up to $\text{gap}_{\epsilon} + \epsilon$) can be efficiently found with polynomial sample complexity and runtime. In particular, (for small $\epsilon$) the leading term in the sample complexity scales as $O(H^5S^2AB/\epsilon^2)$. Since bandit-RL games include bandit games as a special case, the $\Omega(AB/\epsilon^2)$ lower bound for bandit games (Theorem 3) apply here and implies that the $A, B$ dependence in Theorem 4 is tight, while the $H$ dependence may be slightly suboptimal.

We also remark the learning goal for the follower in our bandit-RL game is a new RL setting in which the single-reward setting and the full reward-free setting, for which the optimal $S$ dependence is currently unclear. In the single-reward setting, existing fast exploration algorithms such as UCBVI [3] only require linear in $S$ episodes for finding a near-optimal policy. In contrast, in the full reward-free
We now state our main guarantee for Algorithm 3. The proof can be found in Appendix E.1.

**Algorithm 3** Learning Stackelberg in linear bandit games

**Require** Target accuracy $\varepsilon > 0$.

1. Find $(K, \rho) \leftarrow \text{CoreSet}(\Phi)$ (cf. (10)). Let $K = \{(a_j, b_j) : 1 \leq j \leq K\}$ where $K = |K|$.
2. Query each $(a_j, b_j)$ for $N = O(d \log(d/\delta)/\varepsilon^2)$ times. Let $(\hat{\mu}_{1,j}, \hat{\mu}_{2,j})$ denote the empirical mean of the observed rewards over the $N$ queries.
3. Estimate $(\hat{\theta}_1^2, \hat{\theta}_2^2)$ via weighted least squares
   \[
   \hat{\theta}_i := \arg\min_{\theta \in \mathbb{R}^d} \sum_{i=1}^{K} \rho(a_j, b_j)(\phi(a_j, b_j)\top \theta_i - \hat{\mu}_{i,j})^2, \quad i = 1, 2.
   \] (9)
4. Construct approximate best response sets and values for all $a \in A$
   \[
   \hat{\text{BR}}_{3\varepsilon/4}(a) := \left\{ b : \phi(a, b)\top \hat{\theta}_2 \geq \max_{b' \in B} \phi(a, b')\top \hat{\theta}_2 - 3\varepsilon/4 \right\},
   \]
   \[
   \hat{\phi}_{3\varepsilon/4}(a) := \min_{b \in \hat{\text{BR}}_{3\varepsilon/4}(a)} \phi(a, b)\top \hat{\theta}_1.
   \]
5. Output $(\hat{a}, \hat{b})$, where $\hat{a} = \arg\max_{a \in A} \hat{\phi}_{3\varepsilon/4}(a), \hat{b} = \arg\min_{b \in \hat{\text{BR}}_{3\varepsilon/4}(\hat{a})} \phi(\hat{a}, b)\top \hat{\theta}_1$.

**Setting**

We consider a bandit game with action space $A, B$ that are finite but potentially arbitrarily large, and assume in addition that the reward functions has a linear form

\[
r_1(a, b) = \phi(a, b)\top \theta_1^* + z_1, \quad r_2(a, b) = \phi(a, b)\top \theta_2^* + z_2,
\] (8)

where $\phi : A \times B \to \mathbb{R}^d$ is a $d$-dimensional feature map, $\theta_1^*, \theta_2^* \in \mathbb{R}^d$ are unknown ground truth parameters for the rewards, and $z_1, z_2$ are random noise which we assume are mean-zero and 1-sub-Gaussian. Let $\Phi := \{\phi(a, b) : (a, b) \in A \times B\}$ denote the set of all possible features. For linear bandit games, we define $\text{gap}_\varepsilon$ same as definition (5) for bandit games.

**Algorithm and guarantee**

We present our algorithm for linear bandit games in Algorithm 3. Compared with our Algorithm 1 for bandit games, Algorithm 3 takes advantage of the linear structure through the following important modifications: (1) Rather than querying every action pair, we only query $(a, b)$ in a core set $K$ found through the following subroutine

\[
\text{CoreSet}(\Phi) := (K, \rho) \quad \text{where} \quad K \subset A \times B, \quad \rho \in \Delta_K, \quad \text{such that}
\]

\[
\max_{\phi \in \Phi} \phi\top \left( \sum_{(a, b) \in K} \rho(a, b)\phi(a, b)\phi(a, b)\top \right)^{-1} \phi \leq 2d \quad \text{and} \quad K = |K| \leq 4d \log \log d + 16. \tag{10}
\]

Such a core set is guaranteed to exist for any finite $\Phi$ [24, Theorem 4.4], and can be found efficiently in $O(ABd^2)$ steps of computation [44, Lemma 3.9]. (2) Rather than estimating the reward at every $(a, b)$ in a tabular fashion, we use a weighted least-squares (9) to obtain estimates $(\hat{\theta}_1, \hat{\theta}_2)$ which are then used to approximate the true reward for all $(a, b)$.

We now state our main guarantee for Algorithm 3. The proof can be found in Appendix E.1.

**Theorem 5** (Learning Stackelberg in linear bandit games). For any linear bandit game, Algorithm 3 outputs a $(\text{gap}_\varepsilon + \varepsilon)$-approximate Stackelberg equilibrium $(\hat{a}, \hat{b})$ with probability at least $1 - \delta$:

\[
\phi_0(\hat{a}) \geq \phi_{\varepsilon/2}(\hat{a}) \geq \max_{a \in A} \phi_0(a) - \text{gap}_\varepsilon - \varepsilon,
\]

in at most $n = \tilde{O}(d^2/\varepsilon^2)$ queries.
Sample complexity; computation Theorem 5 shows that Algorithm 3 achieves $\tilde{O}(d^2/\varepsilon^2)$ sample complexity for learning Stackelberg equilibria in linear bandit games. This only depends polynomially on the feature dimension $d$ instead of the size of the action spaces $A, B$, which improves over Algorithm 1 when $A, B$ are large and is desired given the linear structure (8). This sample complexity has at most a $\tilde{O}(d)$ gap from the lower bound: An $\Omega(d/\varepsilon^2)$ lower bound for linear bandit games can be obtained by directly adapting $\Omega(AB/\varepsilon^2)$ lower bound for bandit games in Theorem 3 (see Appendix E.2 for a formal statement and proof). We also note that, while the focus of Theorem 5 is on the sample complexity rather than the computation, Algorithm 3 is guaranteed to run in $\text{poly}(A, B, d, 1/\varepsilon^2)$ time, since the CoreSet subroutine, the weighted least squares step (9), and the final optimization step in approximate best-response sets can all be solved in polynomial time.

6 Conclusion

This paper provides the first line of sample complexity results for learning Stackelberg equilibria in general-sum games with bandit feedback of the rewards and sampling noise. We identify a fundamental gap between the exact and estimated versions of the Stackelberg value, and design sample-efficient algorithms for learning Stackelberg with value optimal up to this gap, in several representative two-player general-sum games. We believe our results open up a number of interesting future directions, such as the optimal sample complexity for bandit-RL games and linear-bandit games, learning Stackelberg in more general Markov games, or further characterizations on what kinds of games admit a small gap.

Acknowledgment

The authors would like to thank Alex Trott and Stephan Zheng for the inspiring discussions on the AI Economist. The authors also thank the Theory of Reinforcement Learning program at the Simons Institute (Fall 2020) for hosting the authors and incubating our initial discussions.

Funding transparency statement

YB, HW, CX are funded through employment with Salesforce.

References


We now state our sample complexity upper bound for learning Stackelberg in bandit games under Algorithm 4 Learning Stackelberg in bandit games with optimistic tie-breaking

**Theorem A.1**

The setting is exactly the same as in Section 3, except that now we consider optimistic versions of the \( \psi \)-equilibrium. However, their true set \( \text{BR}_{\text{best}} \) measures the max gap between \( \psi \) in Section 3—our sample complexity depends on this newly defined

\[
\hat{\psi}_{3\varepsilon/4}(a) := \max_{b \in \hat{\text{BR}}_{3\varepsilon/4}(a)} \hat{\mu}_1(a, b).
\]

\[
\hat{\psi}_{3\varepsilon/4}(a) := \max_{b \in \hat{\text{BR}}_{3\varepsilon/4}(a)} \hat{\mu}_1(a, b).
\]

**Algorithm 4** Learning Stackelberg in bandit games with optimistic tie-breaking

**Require:** Target accuracy \( \varepsilon > 0 \).

**set** \( N \leftarrow C \log(AB/\delta)/\varepsilon^2 \) for some constant \( C > 0 \).

1. Query each \( (a, b) \in A \times B \) for \( N \) times and obtain \( \{r_1(j)(a, b), r_2(j)(a, b)\}_{j=1}^N \).
2. Construct empirical estimates of the means \( \hat{\mu}_1(a, b) = \frac{1}{N} \sum_{j=1}^N r_1(j)(a, b) \) for \( i = 1, 2 \).
3. Construct approximate best response sets and values for all \( a \in A \):

\[\hat{\text{BR}}_{3\varepsilon/4}(a) := \left\{ b : \hat{\mu}_2(a, b) \geq \max_{b' \in B} \hat{\mu}_2(a, b') - \varepsilon/4 \right\},\]

\[\hat{\psi}_{3\varepsilon/4}(a) := \max_{b \in \hat{\text{BR}}_{3\varepsilon/4}(a)} \hat{\mu}_1(a, b)\]

4. Output \( (\tilde{a}, \tilde{b}) \) where \( \tilde{a} = \arg \max_{a \in A} \hat{\psi}_{3\varepsilon/4}(a), \tilde{b} = \arg \max_{b \in \hat{\text{BR}}_{3\varepsilon/4}(\tilde{a})} \hat{\mu}_1(\tilde{a}, b)\).

**A Results with optimistic tie-breaking**

In this section, we present alternative versions of our main results where the Stackelberg equilibrium is defined via *optimistic tie-breaking*.

**A.1 Bandit games**

The setting is exactly the same as in Section 3, except that now we consider optimistic versions of the \( \phi \)-functions that take the \( \max \) over best-response sets (henceforth the \( \psi \)-functions):

\[
\psi_\varepsilon(a) := \max_{b \in \text{BR}_\varepsilon(a)} \mu_1(a, b),
\]

for all \( \varepsilon \geq 0 \). Notice that now \( \psi_\varepsilon \geq \psi_0 \), and we consider the following new definition of gap:

\[
\overline{\text{gap}}_\varepsilon := \max_{a \in A_\varepsilon} (\psi_\varepsilon(a) - \psi_0(a)), \quad \text{where}
\]

\[
A_\varepsilon := \left\{ a \in A : \psi_\varepsilon(a) \geq \max_{a \in A} \psi_0(a) - \varepsilon \right\}.
\]

Our desired optimality guarantee is

\[
\psi_0(\tilde{a}) \geq \max_{a \in A_\varepsilon} \psi_0(a) - \overline{\text{gap}}_\varepsilon - \varepsilon.
\]

We now state our sample complexity upper bound for learning Stackelberg in bandit games under optimistic tie-breaking. The proof can be found in Section F.1.

**Theorem A.1** (Bandit games with optimistic tie-breaking). For the two-player bandit game and any \( \varepsilon \in (0, 1) \), Algorithm 4 outputs \( (\tilde{a}, \tilde{b}) \) such that with probability at least 1 - \( \delta \),

\[
\psi_0(\tilde{a}) \geq \max_{a \in A_\varepsilon} \psi_0(a) - \overline{\text{gap}}_\varepsilon - \varepsilon,
\]

\[
\mu_2(\tilde{a}, \tilde{b}) \geq \max_{b' \in B} \mu_2(\tilde{a}, b') - \varepsilon
\]

with \( n = \tilde{O}(AB/\varepsilon^2) \) samples, where \( \tilde{O}(\cdot) \) hides log factors. Further, the algorithm runs in \( O(n) = \tilde{O}(AB/\varepsilon^2) \) time.

**Intuitions about new gap** We provide some intuitions about why—in contrast to the gap, defined in Section 3—our sample complexity depends on this newly defined \( \overline{\text{gap}}_\varepsilon \). Here. Observe that, \( \overline{\text{gap}}_\varepsilon \) measures the max gap between \( \psi_\varepsilon(a) - \psi_0(a) \), over all possible \( a \)'s whose \( \psi_\varepsilon \) can compete with the best \( \psi_0 \). For any of these \( a \)'s, statistically (if we only have \( O(AB/\varepsilon^2) \) samples), the best response set \( \text{BR}_\varepsilon(a) \) is indistinguishable from \( \text{BR}_0(a) \), and we may well pick these \( a \)'s as the Stackelberg equilibrium. However, their true \( \psi_0 \) can be (much) lower than the \( \psi_\varepsilon \), and thus picking one of these \( a \)'s we may have to suffer from the so-defined \( \overline{\text{gap}}_\varepsilon \) in the worst case.
We now state our sample complexity upper bound for learning Stackelberg in bandit-RL games under Algorithm 5 

**Learning Stackelberg in bandit-RL games with optimistic tie-breaking**

<table>
<thead>
<tr>
<th>Theorem A.2</th>
<th>(Learning Stackelberg in bandit-RL games with optimistic tie-breaking)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The setting is exactly the same as in Section 4, except the definition of the $\psi$-functions takes the max over best-response sets: $\psi_\varepsilon(a) := \max_{\pi \in \text{BR}<em>\varepsilon(a)} V_1(a, \pi^b)$, for all $\varepsilon \geq 0$. Similar as in Section A.1, we consider the following new definition of gap: $\tilde{\text{gap}}</em>\varepsilon := \max_{a \in A} {\psi_\varepsilon(a) - \psi_0(a)}$, where $\text{BR}<em>\varepsilon(a) := {a \in A : \psi</em>\varepsilon(a) \geq \max_{a \in A} \psi_0(a) - \varepsilon}$.</td>
<td></td>
</tr>
</tbody>
</table>

We now state our sample complexity upper bound for learning Stackelberg in bandit-RL games under optimistic tie-breaking. The proof is analogous to Theorem 4, and can be found in Section F.2.

**Theorem A.2** (Learning Stackelberg in bandit-RL games with optimistic tie-breaking). For any bandit-RL game and sufficiently small $\varepsilon \leq O(1/H^2S^2)$, Algorithm 5 with $n = \tilde{O}(H^5S^2AB/\varepsilon^2 + H^7S^4AB/\varepsilon)$ episodes of play can return $(\hat{a}, \hat{\pi}^b)$ such that with probability at least $1 - \delta$, $\psi_0(\hat{a}) \geq \max_{a \in A} \psi_0(a) - \tilde{\text{gap}}_\varepsilon - \varepsilon$, $V_2(\hat{a}, \hat{\pi}^b) \geq \max_{\pi \in \hat{\pi}} V_2(\hat{a}, \hat{\pi}^b) - \varepsilon$, where $\tilde{O}(\cdot)$ hides $\log(HSAB/\delta\varepsilon)$ factors. Further, the algorithm runs in $\text{poly}(HSVAB/\delta\varepsilon)$ time.

**B Matrix game with simultaneous play**

In this section, we consider a variant of the two-player bandit game, in which the leader and follower instead play a matrix game simultaneously, and the follower cannot see the leader’s action. The problem of finding Stackelberg in this setting is also known as learning the “optimal strategy to commit to” [13].

**Setting** A general-sum matrix game with simultaneous play can be described as $M = (A, B, r_1, r_2)$ with $|A| = A, |B| = B$, and $r_1, r_2 : A \times B \rightarrow [0, 1]$, which defines the following game:

- The leader pre-specifies a policy $\pi^a \in \Delta_A$ and reveals this policy to the follower.
Theorem B.1

The main difference between this setting and bandit games is that now the Stackelberg equilibrium φ value results on learning Nash equilibria in general-sum matrix games. On the one hand, when we have complexity assuming a best response oracle (can query BR to gap) Stackelberg equilibrium in simultaneous games. Also, as we assumed bandit feedback, (outputs simultaneous play, Algorithm 6 queries for n samples, with only a gap results suffice for learning the Stackelberg up to gap) Let B.1 Main result

• The leader plays a ∼ πa, and the follower plays an action b ∈ B simultaneously without seeing a.
• The leader receives reward r1(a, b) and the follows receives reward r2(a, b).

(Above, ΔA denotes the probability simplex on A.) Let μi(πa, b) = ∑a′∈A πa(a′)E[r_i(a′, b)], i = 1, 2 denote the mean rewards (for mixed policies), and

φε(πa) := min b∈BRε(πa) μ1(πa, b),

BRε(πa) := \{b ∈ B : μ2(πa, b) ≥ max_{b′} μ2(πa, b′) − ε\}

denote the ε-approximate best response sets and best response values for any ε ≥ 0, similar as in bandit games. We also overload notation to let φε(a1) := φε(δa1) to denote the φε value at pure strategies (δa is the pure strategy of always taking a).

The main difference between this setting and bandit games is that now the Stackelberg equilibrium for the leader may be achieved at mixed strategies only, so that we can no longer restrict attention to pure strategies a ∈ A for the leader. To see why this is true, consider 2x2 game of [13] shown in Table 1. In this game, the two pure strategies {a1, a2} achieve φ0(a1) = 2 (since the best response is b1) and φ0(a2) = 3 (since the best response is b2). However, if we take πa = pδa1 + (1 − p)δa2, then the follower’s best response is b2 whenever p < 1/2. Taking p → (1/2)−, the leader can achieve value φ0(πa) = 4p + 3(1 − p) → 3.5, which is higher than both pure strategies. For p ≥ 1/2, the follower’s best response is b1, and φ0(πa) ≤ 2. Therefore the Stackelberg equilibrium for the leader is to take πa with p → (1/2)−.

Table 1: Example of matrix game with simultaneous play, where the Stackelberg strategy for the leader is mixed.

<table>
<thead>
<tr>
<th>μ1, μ2</th>
<th>b1</th>
<th>b2</th>
</tr>
</thead>
<tbody>
<tr>
<td>a1</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>a2</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

B.1 Main result

Let gapε := supπa∈ΔA φ0(πa) − supπa∈ΔA φε(πa) denote the gap. The following result shows that $O(AB/\varepsilon^2)$ samples suffice for learning the Stackelberg up to (gapε + ε) in simultaneous matrix games, similar as in bandit games. The proof can be found in Appendix G.1.

Theorem B.1 (Learning Stackelberg in simultaneous matrix games). For any matrix game with simultaneous play, Algorithm 6 queries for n = O(AB log(AB/δ)/ε^2) = $O(AB/\varepsilon^2)$ samples, and outputs $(\hat{\pi}^a, \hat{b})$ such that with probability at least 1 − δ,

$\phi_0(\hat{\pi}^a) \geq \phi_0(\hat{\pi}^a) \sup_{\pi^a \in \Delta_A} \phi_0(\pi^a) - \text{gap}_\varepsilon - \varepsilon,$

$\mu_2(\hat{\pi}^a, \hat{b}) \geq \max_{b' \in B} \mu_2(\hat{\pi}^a, b') - \varepsilon.$

Theorem B.1 implies that $O(AB/\varepsilon^2)$ samples is also enough for determining the approximate (up to gap) Stackelberg equilibrium in simultaneous games. Also, as we assumed bandit feedback, Theorem B.1 extends the results of Letchford et al. [27], Peng et al. [34] which studied the sample complexity assuming a best response oracle (can query BR0(πa) for any πa ∈ Δ_A).

Comparison between learning Stackelberg and Nash. We compare Theorem B.1 with existing results on learning Nash equilibria in general-sum matrix games. On the one hand, when we have $O(AB/\varepsilon^2)$ samples, with only a (gapε + ε) near-optimal Stackelberg equilibrium, but we can learn

\footnote{The reason why the optimal policy can only be approached instead of exactly achieved is because of the pessimistic tie-breaking at p = 1/2, and is resolved if we take optimistic tie-breaking.}
We also study simultaneous matrix games with optimistic tie-breaking. The setting is exactly the same except the definition of the \( \psi \)-functions takes the max over best-response sets:

\[
\psi_{\epsilon}(\pi^a) := \max_{b \in \bar{BR}_\epsilon(\pi^a)} \mu_1(\pi^a, b),
\]

for all \( \epsilon \geq 0 \). Similar as in bandit games (Section A.1), we consider the following new definition of gap:

\[
\text{gap}_\epsilon := \max_{\pi^a \in \Delta_A} \left[ \psi_{\epsilon}(\pi^a) - \psi_0(\pi^a) \right], \quad \text{where}
\]

\[
A_\epsilon := \left\{ \pi^a \in \Delta_A : \psi_{\epsilon}(\pi^a) \geq \max_{\pi^a \in \Delta_A} \psi_0(\pi^a) - \epsilon \right\}.
\]

\[\text{Algorithm 6} \quad \text{Learning Stackelberg in matrix games with simultaneous play}\]

**Require:** Target accuracy \( \varepsilon > 0 \).

**set** \( N \leftarrow C \log(AB/\delta)/\varepsilon^2 \) for some constant \( C > 0 \).

1. Query each \( (a, b) \in A \times B \) for \( N \) times and obtain \( \{r_1^{(j)}(a, b), r_2^{(j)}(a, b)\}_{j=1}^N \).
2. Construct empirical estimates \( \hat{\mu}_1(\pi^a, b) = \sum_{a' \in A} \pi^a(a') \sum_{j=1}^N r_1^{(j)}(a', b) \) for \( i = 1, 2 \).
3. Construct approximate best response sets and values for all \( \pi^a \in \Delta_A \):

\[
\hat{BR}_{3\epsilon/4}(\pi^a) := \left\{ b : \hat{\mu}_2(\pi^a, b) \geq \max_{b' \in B} \hat{\mu}_2(\pi^a, b') - 3\epsilon/4 \right\},
\]

\[
\hat{\phi}_{3\epsilon/4}(\pi^a) := \min_{b \in \hat{BR}_{3\epsilon/4}(\pi^a)} \hat{\mu}_1(\pi^a, b).
\]

4. Output \( (\hat{\pi}^a, \hat{b}) \) such that

\[
\hat{\phi}_{3\epsilon/4}(\hat{\pi}^a) \geq \sup_{\pi^a \in \Delta_A} \hat{\phi}_{3\epsilon/4}(\pi^a) - \epsilon/2, \tag{13}
\]

\[
\hat{\phi}_{3\epsilon/4}(\hat{\pi}^a, \hat{b}) = \arg \min_{b \in \hat{BR}_{3\epsilon/4}(\hat{\pi}^a)} \hat{\mu}_1(\hat{\pi}^a, b).
\]

an \( \varepsilon \)-approximate Nash equilibrium [28]. On the other hand, the Stackelberg value is uniquely defined (as the max of \( \hat{\phi}_0 \)), whereas there can be multiple Nash values [38] for general-sum games. Additionally, at the Stackelberg equilibrium, the leader’s payoff is guaranteed to be at least as good as any Nash value (the leader can pre-specify any Nash policy). This makes Stackelberg a perhaps better solution concept in asymmetric games where the learning goal focuses more on the leader.

**Runtime** In Algorithm 6, the step of approximately maximizing \( \hat{\phi}_{3\epsilon/4}(\pi^a) \) in (13) requires optimizing a discontinuous function over a continuous domain. It is unclear whether this program can be reformulated to be solved efficiently in polynomial time\(^5\). However, we remark that this is special to the pessimistic tie-breaking we assumed [27]. Learning the Stackelberg equilibrium with optimistic tie-breaking has the same \( \tilde{O}(AB/\varepsilon^2) \) sample complexity while admitting an efficient polynomial-time algorithm via linear programming (see Section B.2 for the formal statement and proof).

**B.2 Optimistic tie-breaking**

We also study simultaneous matrix games with optimistic tie-breaking. The setting is exactly the same as above except the definition of the \( \psi \)-functions takes the max over best-response sets:

\[
\psi_{\epsilon}(\pi^a) := \max_{b \in \bar{BR}_\epsilon(\pi^a)} \mu_1(\pi^a, b),
\]

This program has a finite-time solution by the following strategy (which utilizes the specific structure of this program): First partition \( \Delta_A \) according to which subsets of \( B \) are \( 3\epsilon/4 \) best response, and then within each partition solve an linear program (over \( \pi^a \)) to a fixed accuracy (e.g. \( \varepsilon/10 \)). However, the runtime is exponential because there are \( 2^{|B|} \) subsets induced by the partition.

\(^5\)We also remark that [47, Theorem 9 & Proposition 10] provides an efficient reformulation of the pessimistic Stackelberg problem in simultaneous matrix games. However, their reformulation relies crucially on the best response set being \( \text{exact} \), and does not generalize to our setting which requires to solve the pessimistic Stackelberg problem with \( \text{approximate} \) best response sets.
For any matrix game with simultaneous play, Algorithm 7 queries for poly(n) time. Further, the algorithm runs in $\text{poly}(n)$ time. We can now first maximize over $\pi$ instead of a max-min problem, for which we can exchange the order of maximization. Concretely, the optimistic version is that it is guaranteed to have a polynomial runtime.

Algorithm 7: Learning Stackelberg in matrix games with simultaneous play (optimistic tie-breaking version)

**Require:** Target accuracy $\varepsilon > 0$.

**set** $N \leftarrow C \log(AB/\delta)/\varepsilon^2$ for some constant $C > 0$.

1: Query each $(a, b) \in A \times B$ for $N$ times and obtain $\{r^{(j)}_1(a, b), r^{(j)}_2(a, b)\}_{j=1}^N$.

2: Construct empirical estimates $\hat{\mu}_1(a^a, b) = \sum_{a' \in A} a^a(a') N \sum_{j=1}^N r^{(j)}_1(a^a, b)$ for $i = 1, 2$.

3: Construct approximate best response sets and values for all $\pi^a \in \Delta_A$:

$$\text{BR}_{3\varepsilon/4}(\pi^a) := \left\{ b : \hat{\mu}_2(\pi^a, b) \geq \max_{b' \in B} \hat{\mu}_2(\pi^a, b') - 3\varepsilon/4 \right\},$$

$$\hat{\phi}_{3\varepsilon/4}(\pi^a) := \max_{b \in \text{BR}_{3\varepsilon/4}(\pi^a)} \hat{\mu}_1(\pi^a, b).$$

4: Output

$$\hat{\pi}^a = \arg\max_{\pi^a \in \Delta_A} \hat{\phi}_{3\varepsilon/4}(\pi^a),$$

$$\hat{b} = \arg\max_{b \in \text{BR}_{3\varepsilon/4}(\hat{\pi}^a)} \hat{\mu}_1(\hat{\pi}^a, b).$$

By calling the subroutine $(\hat{\pi}^a, \hat{b}) \leftarrow \text{BestMixedLeaderStrategy}(\hat{\mu}_1, \hat{\mu}_2)$.

**Theorem B.2** (Learning Stackelberg in simultaneous matrix games with optimistic tie-breaking).

*For any matrix game with simultaneous play, Algorithm 7 queries for $n = O(AB \log(AB/\delta)/\varepsilon^2) = O(AB/\varepsilon^2)$ samples, and outputs $(\hat{\pi}^a, \hat{b})$ such that with probability at least $1 - \delta$,

$$\psi_0(\hat{\pi}^a) \geq \max_{\pi^a \in \Delta_A} \psi_0(\pi^a) - \delta \mu_2(\hat{\pi}^a, \hat{b}) - \varepsilon,$$

$$\mu_2(\hat{\pi}^a, \hat{b}) \geq \max_{b' \in B} \mu_2(\hat{\pi}^a, b') - \varepsilon.$$

Further, the algorithm runs in $\text{poly}(n)$ time.

The proof can be found in Section G.2.

**Efficient runtime** Theorem B.2 shares the same sample complexity $\tilde{O}(AB/\varepsilon^2)$ as its pessimistic tie-breaking counterpart (Theorem B.1), albeit with a slightly different definition of the gap. However, an additional advantage of the optimistic version is that it is guaranteed to have a polynomial runtime. The core reason behind this is that with optimistic tie-breaking now $(\hat{\pi}^a, \hat{b})$ solves a *max-max problem* (instead of a max-min problem), for which we can exchange the order of maximization. Concretely, we can now first maximize over $\pi^a$ for each $b$, which admits a linear programming formulation (cf. the BestMixedLeaderStrategy subroutine in Algorithm 10, also in [13]).

### C Proofs for Section 3

#### C.1 Proof of Theorem 1

To prove Theorem 1, we will construct a pair of hard instances, and use Le Cam’s method [49, Section 15.2] to reduce the estimation error into a testing problem between the two hard instances. Consider the following two games $M_1$ and $M_{-1}$, where the rewards follow Bernoulli distributions: $r_i(a, b) \sim \text{Ber}(\mu_i(a, b))$ with means shown in Table 2, where $\delta \in (0, 1)$ is a parameter to be determined.

Based on Table 2, it is straightforward to check that $\phi^0_{M_1}(a_1) = 1, \phi^0_{M_{-1}}(a_1) = 0$, and $\phi^M_{M_{-1}}(a_2) = \phi^M_{M_{-1}}(a_2) = 1/2$. Further, $a^M_{M_1} = a_1$ and $a^M_{M_{-1}} = a_2$.

For any algorithm that outputs a (possibly randomized) estimator $\hat{a} \in A$ of the Stackelberg equilibrium, let $\pi$ denote its querying policy, that is, given prior queries and observations
where choosing the problem class to be $M$. Therefore, Lemma C.1 and C.2 A Lemma on the gap yields $\max \phi_{\epsilon_1}(a) - \max \phi_{\epsilon_2}(a) \geq \frac{1}{2}$. The next query $\pi^{(k)}(a,b) \{ a(i), b(i), r_1(i), r_2(i) \}_{i=1}^{k-1}$ denotes the distribution of the next query. Let $P_{M,\pi}$ and $P_{M-1,\pi}$ denote the distribution of all $n$ observations generated by the querying policy $\pi$. For these two instances, we have

$$\sup_{M \in \{M_1, M_{-1}\}} \mathbb{P}(\max \phi^M_0(a) - \hat{\phi}^M_0(\hat{a}) \geq \frac{1}{2})$$

$$= \sup_{M \in \{M_1, M_{-1}\}} \mathbb{P}(\hat{a} \neq \arg \max_{a \in A} \phi^M_0(a))$$

$$\geq \frac{1}{2} (\mathbb{P}(\hat{a} \neq a_1) + \mathbb{P}(\hat{a} \neq a_2))$$

$$\geq \frac{1}{2} \left( 1 - \text{TV}(P_{M_1,\pi}, P_{M_{-1},\pi}) \right)$$

$$\geq \frac{1}{2} \left( 1 - \frac{1}{2} \text{KL}(P_{M_1,\pi} \| P_{M_{-1},\pi}) \right),$$

where the second-to-last step used Le Cam’s inequality, and the last step used Pinsker’s inequality. To upper bound the KL distance between $P_{M,\pi}$ and $P_{M-1,\pi}$, we apply the divergence decomposition of [23, Lemma 15.1] and obtain that

$$\text{KL}(P_{M_1,\pi} \| P_{M_{-1},\pi}) \leq \sum_{(a,b) \in A \times B} E_{M_1,\pi} [T_{a,b}(n)] \cdot \text{KL}(P_{a,b}^{M_1} \| P_{a,b}^{M_{-1}}) \leq n \cdot \max_{(a,b) \in A \times B} \text{KL}(P_{a,b}^{M_1} \| P_{a,b}^{M_{-1}}),$$

where $T_{a,b}(n)$ denotes the number of queries to $(a,b)$ among the $n$ queries, and $P_{a,b}^{M_i}$ denote the distribution of the observation $(r_1(a,b), r_2(a,b))$ in problem $M_i$, $i = 1, 2$. We have $\text{KL}(P_{a,b}^{M_1} \| P_{a,b}^{M_{-1}}) = 0$ for $(a,b) = (a_2, b_1)$ and $(a,b) = (a_2, b_2)$. For $(a,b) = (a_1, b_1)$ and $(a,b) = (a_1, b_2)$, using the bound $\text{KL}(\text{Ber}(\frac{1+\delta}{2}) \| \text{Ber}(\frac{1-\delta}{2})) = \delta \log \frac{1+\delta}{1-\delta} \leq 3\delta^2$ for $\delta \leq 1/2$ (and the same bound for $\text{KL}(\text{Ber}(\frac{1-\delta}{2}) \| \text{Ber}(\frac{1+\delta}{2}))$). Therefore, we get

$$\text{KL}(P_{M_1,\pi} \| P_{M_{-1},\pi}) \leq 3n\delta^2.$$

Choosing $\delta = 1/\sqrt{(27/2)n}$, the above is upper bounded by $2/9$, and thus plugging back to the preceding bound yields

$$\sup_{M \in \{M_1, M_{-1}\}} \mathbb{P}(\hat{a} \neq \arg \max_{a \in A} \phi^M_0(a)) \geq \frac{1}{2} \left( 1 - \frac{1}{2} \text{KL}(P_{M_1,\pi} \| P_{M_{-1},\pi}) \right) \geq \frac{1}{3}.$$

Therefore, choosing the problem class to be $\mathcal{M}_n = \{M_1, M_{-1}\}$ with $\delta = 1/\sqrt{(27/2)n}$, the above is the desired lower bound.

C.2 A Lemma on the gap

Lemma C.1 (Gap can be $\Omega(1)$). For any $0 \leq \varepsilon_1 < \varepsilon_2 < 1$, there exists a two-player bandit game $M = M_{\varepsilon_1,\varepsilon_2}$ with $A = B = 2$, such that

$$\max_{a \in A} \phi_{\varepsilon_1}(a) - \max_{a \in A} \phi_{\varepsilon_2}(a) \geq \frac{1}{2},$$

$$\max_{a \in A} \phi_{\varepsilon_1}(a) - \phi_{\varepsilon_1} \left( \arg \max_{a' \in A} \phi_{\varepsilon_2}(a') \right) \geq \frac{1}{2}.$$
In particular, (taking \( \varepsilon_1 = 0 \)), for any \( \varepsilon \) there exists a game in which \( \text{gap}_\varepsilon = \max_{a \in A} \phi_0(a) - \max_{a \in A} \phi_\varepsilon(a) \geq 1/2 \).

**Proof.** Let \( 0 \leq \varepsilon_1 < \varepsilon_2 \). We construct the problem \( M = M_{\varepsilon_1, \varepsilon_2} \) as follows: \( A = \{a_1, a_2\} \) and \( B = \{b_1, b_2\} \), and the rewards \( \{r_1(a, b), r_2(a, b)\}_{a \in A, b \in B} \) are all deterministic and valued as in the following table:

<table>
<thead>
<tr>
<th>( r_1, r_2 )</th>
<th>( b_1 )</th>
<th>( b_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a_1 )</td>
<td>( \frac{\varepsilon_1 + \varepsilon_2}{2} )</td>
<td>0, 0</td>
</tr>
<tr>
<td>( a_2 )</td>
<td>( \frac{1}{2} ), 1</td>
<td>( \frac{1}{2}, 1 )</td>
</tr>
</tbody>
</table>

Table 3: Construction of \( r_1(a, b), r_2(a, b) \) for \( a \in \{a_1, a_2\}, b \in \{b_1, b_2\} \).

For the arm \( a_2 \), actions \( b_1 \) and \( b_2 \) are exactly the same, so we have \( \phi_\varepsilon(a_2) = \frac{1}{2} \) for all \( \varepsilon \). For the arm \( a_1 \), observe that \( \varepsilon_1 < \frac{\varepsilon_1 + \varepsilon_2}{2} < \varepsilon_2 \), and thus \( \text{BR}_{\varepsilon_1}(a_1) = \{b_1\} \) and \( \phi_\varepsilon(a_1) = 1 \), but \( \text{BR}_{\varepsilon_2}(a_1) = \{b_1, b_2\} \) and \( \phi_\varepsilon(a_1) = 0 \). Therefore,

\[
\max_{a \in A} \phi_\varepsilon(a) = \max \left\{ \frac{1}{2}, \frac{1}{2} \right\} = 1,
\]

\[
\max_{a \in A} \phi_\varepsilon(a) = \max \left\{ 0, \frac{1}{2} \right\} = \frac{1}{2},
\]

\[
\phi_\varepsilon \left( \arg \max_{a' \in A} \phi_\varepsilon(a') \right) = \phi_\varepsilon(a_2) = \frac{1}{2}.
\]

This shows the desired result. \( \square \)

### C.3 Proof of Theorem 2

Algorithm 1 pulled each arm \( (a, b) \) for \( N = O(\log(AB/\delta)/\varepsilon^2) \) times, and \( \hat{\mu}_1(a, b), \hat{\mu}_2(a, b) \) are the empirical means of the observed rewards. By the Hoeffding inequality and union bound over \( (a, b) \), with probability at least \( 1 - \delta \), we have

\[
\max_{(a, b) \in A \times B} \left| \hat{\mu}_i(a, b) - \mu_i(a, b) \right| \leq \varepsilon/8 \quad \text{for } i = 1, 2. \tag{15}
\]

**Properties of \( \text{BR}_{3\varepsilon/4}(a) \)** On the uniform convergence event (22), we have the following: for any \( b \in \text{BR}_{\varepsilon/2}(a) \), we have

\[
\hat{\mu}_2(a, b) \geq \mu_2(a, b) - \varepsilon/8 \geq \max_{b' \in B} \mu_2(a, b') - 5\varepsilon/8 \geq \max_{b' \in B} \hat{\mu}_2(a, b') - 3\varepsilon/4,
\]

and thus \( b \in \text{BR}_{3\varepsilon/4}(a) \). This shows that \( \text{BR}_{\varepsilon/2}(a) \subseteq \text{BR}_{3\varepsilon/4}(a) \). Similarly we can show that \( \text{BR}_{3\varepsilon/4}(a) \subseteq \text{BR}_{\varepsilon}(a) \). In other words,

\[
\text{BR}_\varepsilon(a) \supseteq \text{BR}_{3\varepsilon/4}(a) \supseteq \text{BR}_{\varepsilon/2}(a) \quad \text{for all } a \in A.
\]

Notably, this implies that \( \hat{b} \in \text{BR}_{3\varepsilon/4}(\hat{a}) \in \text{BR}_\varepsilon(\hat{a}) \), the desired near-optimality guarantee for \( \hat{b} \).

**Near-optimality of \( \hat{\alpha} \)** On the one hand, because \( \hat{\alpha} \) maximizes \( \hat{\mu}_1(\hat{a}, \hat{b}(\hat{a})) \), we have for any \( a \in A \) that

\[
\min_{b' \in \text{BR}_{3\varepsilon/4}(\hat{a})} \hat{\mu}_1(\hat{a}, b') \overset{(i)}{=} \hat{\mu}_1(\hat{a}, \hat{b}(\hat{a})) \overset{(ii)}{=} \min_{b \in \text{BR}_\varepsilon(a)} \hat{\mu}_1(a, b),
\]

where (i) is because \( \hat{b} \) minimizes \( \hat{\mu}_1(\hat{a}, \cdot) \) within \( \text{BR}_{3\varepsilon/4}(\hat{a}) \), and (ii) is because \( \hat{b}(a) \in \text{BR}_{3\varepsilon/4}(a) \subseteq \text{BR}_\varepsilon(a) \). By the uniform convergence (22), we get that

\[
\min_{b' \in \text{BR}_{3\varepsilon/4}(\hat{a})} \mu_1(\hat{a}, b') \geq \min_{b \in \text{BR}_\varepsilon(a)} \mu_1(a, b) - 2 \cdot \varepsilon/8 \geq \phi_\varepsilon(a) - \varepsilon.
\]
We define a family of games \( M \), where:

\[
\hat{\mu}_1(a, b) \leq \min_{b' \in BR_{\varepsilon/4}(\hat{a})} \mu_1(\hat{a}, b') \leq \min_{b' \in BR_{\varepsilon/2}(\hat{a})} \mu_1(\hat{a}, b') = \phi_{\varepsilon/2}(\hat{a}),
\]

where (i) is because \( BR_{\varepsilon/4}(\hat{a}) \supseteq BR_{\varepsilon/2}(a) \). This yields that:

\[
\phi_{\varepsilon/2}(\hat{a}) \geq \max_{a \in A} \phi_\varepsilon(a) - \varepsilon = \max_{a \in A} \phi_0(a) - \text{gap}_\varepsilon - \varepsilon,
\]

which is the first part of the bound for \( \hat{a} \).

On the other hand, since \( \phi_\varepsilon(a) \) is increasing as we decrease \( \varepsilon \), we directly have:

\[
\phi_{\varepsilon/2}(\hat{a}) \leq \phi_0(\hat{a}) \leq \max_{a \in A} \phi_0(a).
\]

This is the second part of the bound for \( \hat{a} \). \( \square \)

### C.4 Proof of Theorem 3

Suppose \( \varepsilon \in (0, c) \) and \( g \in [0, c) \) where \( c > 0 \) is an absolute constant to be determined. For any algorithm that outputs an estimator \( \hat{a} \in A \), let \( \pi \) denote its (sequential) querying policy, and \( P_{M, \pi} \) denote the joint distribution of the \( N \) observed rewards \( (r_1(a^{(i)}, b^{(i)}), r_2(a^{(i)}, b^{(i)}))_{i=1}^N \) under game \( M \). We will rely on the divergence decomposition of [23, Lemma 15.1]:

\[
KL(P_{M, \pi} || P_{M', \pi}) \leq \sum_{(a, b) \in A \times B} E_{M_1, \pi}[T_{a, b}(N)] \cdot KL\left(P_{M, \pi}^{a, b} || P_{M'}^{a, b}\right),
\]

where \( P_{M}^{a, b} \) denotes the distribution of observation \( (r_1(a, b), r_2(a, b)) \) under game \( M \), and \( T_{a, b}(N) \) denotes the number of queries of \( (a, b) \) using algorithm \( \pi \) (which is a random variable). We will also use the fact that:

\[
KL(\text{Ber}(1/2)||\text{Ber}(1/2 + \delta)) = \frac{1}{2} \log \frac{1/2}{1/2 + \delta} + \frac{1}{2} \log \frac{1/2}{1/2 - \delta} = \frac{1}{2} \log \frac{1}{1 - 4\delta^2} \leq \frac{1}{2} \cdot 8\delta^2 \leq 4\delta^2
\]

whenever \( 4\delta^2 \leq 1/2 \), i.e. \( |\delta| \leq 1/2\sqrt{2} \).

#### Construction of hard instance

In our construction below, the rewards follow Bernoulli distributions: \( r_i(a, b) \sim \text{Ber}(\mu_i(a, b)) \), so that it suffices to specify \( \mu_i(a, b) \). Without loss of generality assume \( B/3 \) is an integer, and let \( B = |B| = \{1, \ldots, B\} \) for notational simplicity.

We define a family of games \( M_{a, b_1, b_2} \) indexed by \( a_* \in A \) and \( b_1, b_2 \in B \). Each game \( M_{a, b_1, b_2} \) is defined as follows:

- \( \mu_1(a, b) = 1/2 + g + \varepsilon \) for all \( a \in A \) and \( 1 \leq b \leq B/3 \);
- \( \mu_1(a, b) = 1/2 + \varepsilon \) for all \( a \in A \) and \( B/3 + 1 \leq b \leq 2B/3 \);
- \( \mu_1(a, b) = 1/2 \) for all \( a \in A \) and \( 2B/3 + 1 \leq b \leq B \);
- \( \mu_2(a_*, b_1) = 1/2 + 2\varepsilon \), where \( b_1 \in \{1, \ldots, B/3\} \).
- \( \mu_2(a_*, b_2) = 1/2 + 5\varepsilon/4 \), where \( b_2 \in \{B/3 + 1, \ldots, 2B/3\} \).
- \( \mu_2(a, b') = 1/2 \) for all \( b' \neq b_1, b_2 \).
- \( \mu_2(a', b) = 1/2 \) for all \( a' \neq a_* \) and \( b \in B \).

For this game, we have \( \phi_0(a_*) = 1/2 + g + \varepsilon \), \( \phi_\varepsilon(a_*) = 1/2 + \varepsilon \), and \( \phi_0(a') = \phi_\varepsilon(a') = 1/2 \) for all \( a' \neq a_* \). Therefore, \( \text{gap}_\varepsilon = \max_{a \in A} \phi_0(a) - \max_{a \in A} \phi_\varepsilon(a) = g \).

Further, notice that as long as \( \hat{a} \neq a_* \), we have \( \phi_0(\hat{a}) = \max_{a \in A} \phi_0(a) - (g + \varepsilon) \).

Define \( P_M \) as the mixture of over the prior of \( M_{a_*, b_1, b_2} \) where the prior samples \( a_* \sim \text{Unif}(A) \), \( b_1 \sim \text{Unif}(\{1, \ldots, B/3\}) \), and \( b_2 \sim \text{Unif}(\{B/3 + 1, \ldots, 2B/3\}) \). Define \( M_0 \) as the “null-game” where all the \( r_2 \) are 1/2, and \( r_1 \) has the same configuration as in the above game.
Proof of lower bound  Under the mixture $P_M$, we have

$$
P_M \left( \phi_0(\tilde{a}) \leq \max_{a \in A} \phi_0(a) - (g + \varepsilon) \right) = P_M(\tilde{a} \neq a_*)
$$

$$
= \frac{1}{A(B^2/9)} \sum_{a_*} \sum_{b_1^* = 1}^{B/3} \sum_{b_2^* = B/3 + 1}^{2B/3} P_{M_{a_*, b_1^*, b_2^*}}(\tilde{a} \neq a_*)
$$

$$
\geq \frac{1}{A(B^2/9)} \sum_{a_*} \sum_{b_1^* = 1}^{B/3} \sum_{b_2^* = B/3 + 1}^{2B/3} \sqrt{\frac{1}{2} \sum_{a, b} E_{0, \pi} [T_{a, b}(N)] KL \left( P_{a, b}^{0, \pi} || P_{M_{a_*, b_1^*, b_2^*}}^{0, \pi} \right)}
$$

We now show that $(\ast) \leq 1/3$ if $N \leq c[AB/\varepsilon^2]$ for some small absolute constant $c > 0$. Using the divergence decomposition (16), we have

$$(\ast) \leq \frac{1}{A(B^2/9)} \sum_{a_*} \sum_{b_1^* = 1}^{B/3} \sum_{b_2^* = B/3 + 1}^{2B/3} \sqrt{\frac{1}{2} \sum_{a, b} E_{0, \pi} [T_{a, b}(N)] KL \left( P_{a, b}^{0, \pi} || P_{M_{a_*, b_1^*, b_2^*}}^{0, \pi} \right)}
$$

$$
\leq \frac{1}{A(B^2/9)} \sum_{a_*} \sum_{b_1^* = 1}^{B/3} \sum_{b_2^* = B/3 + 1}^{2B/3} \sqrt{\frac{1}{2} E_{0, \pi} [T_{a, b_1^*}(N)] KL \left( P_{a, b_1^*}^{0, \pi} || P_{M_{a_*, b_1^*, b_2^*}}^{0, \pi} \right)} + \sqrt{\frac{1}{2} E_{0, \pi} [T_{a, b_2^*}(N)] KL \left( P_{a, b_2^*}^{0, \pi} || P_{M_{a_*, b_1^*, b_2^*}}^{0, \pi} \right)}
$$

$$
\leq \frac{1}{A(B/3)} \sum_{a_*} \sum_{b_1^* = 1}^{B/3} \sqrt{\frac{1}{2} E_{0, \pi} [T_{a, b_1^*}(N)] \cdot 4 \cdot (2\varepsilon)^2} + \frac{1}{A(B/3)} \sum_{a_*} \sum_{b_2^* = 1}^{B/3} \sqrt{\frac{1}{2} E_{0, \pi} [T_{a, b_2^*}(N)] \cdot 4 \cdot (5\varepsilon/4)^2}
$$

$$
\leq 2 \sqrt{\frac{24 N \varepsilon^2}{AB}}
$$

Above, (i) used the fact that for the null game $M_0$ and the game $M_{a_*, b_1^*, b_2^*}$, only the actions $(a_*, b_1^*)$ and $(a_*, b_2^*)$ will lead to different observation distributions. (ii) used the fact that $r_2(a_*, b_1^*)$ has mean $1/2 + 2\varepsilon$ under $M_{a_*, b_1^*, b_2^*}$ and mean $1/2$ under $M_0$ (and the other Bernoulli means correspondingly), and the fact that $r_1(a, b)$ are equally distributed in the two games and thus do not contribute to the KL, and finally the KL bound (17) for small enough $\varepsilon$ such that $2\varepsilon < 1/2 \sqrt{2}$. (iii) used the power mean inequality and the equality $\sum_{a, b} T_{a, b}(N) = N$ for any algorithm.
The above implies that, as long as $\varepsilon < 1/4\sqrt{2}$ and $g \leq 1/4$, for $N \leq AB/(864\varepsilon^2)$, we have $(\ast) \leq 1/3$, and thus
\[
P_M \left( \phi_0(\hat{a}) \leq \max_{a \in \mathcal{A}} \phi_0(a) - (g + \varepsilon) \right) = \frac{1}{A(B^2/9)} \sum_{a, b_1, b_2} P_{M_{a, b_1, b_2}} \left( \phi_0(\hat{a}) \leq \max_{a \in \mathcal{A}} \phi_0(a) - (g + \varepsilon) \right)
\]
\[
\geq 1 - \frac{1}{A} - \frac{1}{3} \geq \frac{1}{3}.
\]
Therefore there must exist a game $M_{a, b_1, b_2}$ on which the error probability is at least $1/3$. This is the desired lower bound. \(\square\)

### C.5 Equivalence to turn-based Markov game

We consider the following general-sum turn-based Markov game with two steps and state space $S = \{s_a : a \in \mathcal{A}\}$:

- $(h = 1)$ Leader receives deterministic initial state $s_1$ and plays action $a \in \mathcal{A}$. No reward for both players.
- $(h = 2)$ The game transits deterministically to $s_a$. The follower plays action $b \in \mathcal{B}$ and observes reward $r_2(s_a, b) = r_2(a, b)$. The leader observes reward $r_1(s_a, b) = r_1(a, b)$.
- The game terminates.

It is straightforward to see that the bandit game $M = (\mathcal{A}, \mathcal{B}, r_1, r_2)$ is equivalent to the above turn-based Markov game. Note that the Markov game has $|S| = A$ states.

Now, let $a_*$ be the leader’s exact Stackelberg equilibrium (as defined in (3)). For any $a$, let $b_*(a) = \arg\min_{b \in \text{BR}_0(a)} \mu_1(a, b)$ be the best response of $a$ with the worst $\mu_1$. Define the deterministic follower policy $\pi^b_*$ as $\pi^b_*(s_a) = b_*(a)$ for all $s_a \in S$.

We claim that $(a_*, \pi^b_*)$ is a Nash equilibrium of the above Markov game. Indeed, $\pi^b_*$ is clearly $a_*$’s best response on the follower’s reward. Also, if we fix $\pi^b_*$, then $a_*$ is also the leader’s best response to $\pi^b_*$, as we have
\[
\mu_1(s_a, \pi^b_*(s_a)) = \mu_1(a, b_*(a)) = \min_{b \in \text{BR}_0(a)} \mu_1(a, b) = \phi_0(a),
\]
and thus the leader’s best response is exactly the argmax of $\phi_0(a)$, i.e. $a_*$.

### C.6 Additional discussions on the gap

Here we show that for bandit games, $\text{gap}_\varepsilon$ is small for two special kinds of games: zero-sum games and cooperative games.

**Zero-sum games** Here $r_1 \equiv -r_2$ and thus $\mu_1 \equiv -\mu_2$. In such games, by definition we have
\[
\phi_\varepsilon(a) = \min_{b \in \text{BR}_\varepsilon(a)} \mu_1(a, b),
\]
\[
\text{BR}_\varepsilon(a) = \left\{ b \in \mathcal{B} : \mu_1(a, b) \leq \min_{b'} \mu_1(a, b') + \varepsilon \right\}.
\]
Notice that now the minimum over $b \in \text{BR}_\varepsilon(a)$ is always taken at the exact minimizer of $b \mapsto \mu_1(a, b)$. Therefore we have $\phi_\varepsilon(a) = \min_{b \in \mathcal{B}} \mu_1(a, b)$ does not depend on $\varepsilon$, and thus $\text{gap}_\varepsilon = \max_{a \in \mathcal{A}} \phi_0(a) - \max_{a \in \mathcal{A}} \phi_\varepsilon(a) = 0$.

**Cooperative games** Here $r_1 \equiv r_2$ and thus $\mu_1 \equiv \mu_2$. In such games, by definition we have
\[
\phi_\varepsilon(a) = \min_{b \in \text{BR}_\varepsilon(a)} \mu_1(a, b),
\]
\[
\text{BR}_\varepsilon(a) = \left\{ b \in \mathcal{B} : \mu_1(a, b) \geq \max_{b'} \mu_1(a, b') - \varepsilon \right\}.
\]
Thus for each $a \in \mathcal{A}$, the difference between $\mu_1(a, b)$ for any $b \in \text{BR}_0(a)$ and any $b \in \text{BR}_\varepsilon(a)$ is at most $\varepsilon$. This shows that $\phi_0(a) - \phi_\varepsilon(a) \leq \varepsilon$ for all $a \in \mathcal{A}$ and thus $\text{gap}_\varepsilon \leq \varepsilon$.

---

\(^7\)The formal definition of turn-based Markov games can be found in [4].
D Proofs for Section 4

D.1 Subroutine WorstCaseBestResponse

We describe the WorstCaseBestResponse subroutine in Algorithm 8.

**Algorithm 8 Subroutine WorstCaseBestResponse(M, V_2)**

Require: MDP $M = (H, S, B, \mathbb{P}_h(\cdot|\cdot), r_{1,h}(\cdot,\cdot), r_{2,h}(\cdot,\cdot))$. Initial state $s_1 \in S$. Target value $V_2$.

1. Solve the following linear program over \{ $d_h(s,b) : h \in [H], s \in S, b \in B$ \}:

\[
\text{minimize } \sum_{h=1}^{H} \sum_{s \in S, b \in B} d_h(s,b) r_{1,h}(s,b) \\
\text{s.t. } \sum_{h=1}^{H} \sum_{s \in S, b \in B} d_h(s,b) r_{2,h}(s,b) \geq V_2, \\
\sum_{s \in S, b \in B} d_h(s,b) \mathbb{P}_h(s'|s,b) = \sum_{b' \in B} d_{h+1}(s',b') \text{ for all } 1 \leq h \leq H - 1, s' \in S, \\
\sum_{s \in S, b \in B} d_h(s,b) \Delta_{s,b} \in \Delta_B, \quad d_1(s_1,\cdot) = 0 \text{ for all } s' \neq s_1.
\]

Above, $\Delta_B$ denotes the probability simplex on $B$ (which is a set of $B + 1$ linear constraints).

Let $d_h$ denote the solution and $V_1$ denote the value of the above program.

2. Set $\pi^b_h(b|s) \leftarrow d_h(s,b)/\sum_{b\in B} d_h(s,b)$ for all $(h, s, b)$ (with the convention $0/0 = 1/B$).

**output** $(\pi^b_h, V_1)$.

D.2 Proof of Theorem 4

**Correctness of subroutine** We first show that the WorstCaseBestResponse subroutine (Algorithm 8) with input $(\hat{M}^a, \hat{V}_2^a(a) - \eta/4)$ indeed solves the nominal problem (7). To see this, observe that in the nominal problem (7), both the objective function and the constraint are linear functions of the visitation distribution $\{ \mathbb{P}_h^a(s,b) \}$ induced by $\pi^b$. Therefore, maximizing over all visitation distributions is equivalent to maximizing over all $\pi^b$. To ensure that a general $\{ d_h(s,b) \}_{h,s,b}$ is a visitation distribution, it suffices for it to satisfy the constraints $d_1(s_1,\cdot) \in \Delta_B, d_1(s_1,\cdot) = 0$ for $s' \neq s_1$, and at each $h \geq 2$ and each state $s'$ the in-flow is equal to the out-flow, meaning that

\[
\sum_{s \in S, b \in B} d_h(s,b) \mathbb{P}_h(s'|s,b) = \sum_{b \in B} d_{h+1}(s',b)
\]

for all $h \geq 1$, $s' \in S$. These are exactly the constraints specified in the linear program (18). Finally, for a visitation distribution $d_h$, notice that $\pi_h^b(b|s) = d_h(s,b)/\sum_{b\in B} d_h(s,b)$ (with the convention $0/0 = 1/B$) defines a policy $\pi^b$ whose visitation distribution is exactly $d_h$. This shows that the linear program (18) is indeed a correct algorithm for solving (7).

**Properties of reward-free exploration** For each $a \in A$, Algorithm 2 played the Reward-Free RL-Explore algorithm of Jin et al. [18] for $N = \hat{O}(H^2 S^2 B/\varepsilon^2 + H^7 S^4 B/\varepsilon)$ episodes and obtained an estimate of the transition dynamics $\hat{\mathbb{P}}^a$. (More specifically, it ran $N_0 = \hat{O}(H^2 S^4 B/\varepsilon)$ episodes in its exploration phase and $N_{\text{data}} = \hat{O}(H^5 S^2 B/\varepsilon^2)$ episodes in its data-gathering phase.) Further, let $\{ \hat{r}_{1,h}(a,s,b), \hat{r}_{2,h}(a,s,b) \}$ denote the empirical mean of the observed rewards in the data-gathering phase.

Let $\hat{V}_1(a, \pi^b)$ and $\hat{V}_2(a, \pi^b)$ denote the value functions of the empirical MDPs $(\hat{\mathbb{P}}^a, \hat{r}_1)$ and $(\hat{\mathbb{P}}^a, \hat{r}_2)$ (note that these MDPs combine the true models and the empirical rewards). With our choice $N$, by [18, Theorem 3.1], we have with probability at least $1 - \delta$ that

\[
\sup_{\pi^b} \left| \hat{V}_i(a, \pi^b) - \bar{V}_i(a, \pi^b) \right| \leq \varepsilon/16 \text{ for } i = 1, 2.
\]
We now argue that the Reward-Free RL-Explore algorithm can correctly estimate the rewards, along with estimating transitions. Indeed, we have the following

**Lemma D.1.** Suppose we run the Reward-Free RL-Explore algorithm where the data gathering phase contains \( N_{\text{data}} \geq \tilde{O}(H^3S^2B/\varepsilon^2) \) trajectories, and we in addition receive (stochastic) reward signals \( r_{1,h}, r_{2,h} \) along the trajectories. Then with probability at least \( 1 - \delta \), the empirical reward estimates \( \hat{r}_{1,h}, \hat{r}_{2,h} \) and the associated value functions \( \hat{V}_1 \) and \( \hat{V}_2 \) satisfy that

\[
\sup_{a,b} \left| \hat{V}_i(a, \pi^b) - V_i(a, \pi^b) \right| \leq \varepsilon \quad \text{for } i = 1, 2.
\]

We defer the proof of Lemma D.1 to Appendix D.3. As we have \( N_{\text{data}} = \tilde{O}(H^3S^2B/\varepsilon^2) \), we can apply Lemma 6 and get (by choosing a large absolute constant in the choice of \( N_{\text{data}} \)) that

\[
\sup_{a,b} \left| \hat{V}_i(a, \pi^b) - V_i(a, \pi^b) \right| \leq \varepsilon/16 \quad \text{for } i = 1, 2.
\]

(20)

Combining (19) and (20) (and noticing those are true for all \( a \in \mathcal{A} \)), we get

\[
\sup_{a \in \mathcal{A}, \pi^b} \left| \hat{V}_i(a, \pi^b) - V_i(a, \pi^b) \right| \leq \varepsilon/8 \quad \text{for } i = 1, 2.
\]

(21)

**Guarantees on \( \text{BR}_{3\varepsilon/4}(a) \)** Now, for any \( a \in \mathcal{A} \), recall Algorithm 2 constructed the empirical best-response set (cf. (7))

\[
\text{BR}_{3\varepsilon/4}(a) := \left\{ \pi^b : \hat{V}_2(a, \pi^b) \geq \max_{\pi^b} \hat{V}_2(a, \tilde{\pi}^b) - 3\varepsilon/4 \right\}.
\]

We claim that

\[
\text{BR}_\varepsilon(a) \supseteq \text{BR}_{3\varepsilon/4}(a) \supseteq \text{BR}_{2\varepsilon/2}(a) \quad \text{for all } a \in \mathcal{A}.
\]

Indeed, fixing any \( a \in \mathcal{A} \), let \( \pi^* \) denote the optimal policy for \( V_2(a, \cdot) \) and \( \tilde{\pi}^* \) denote the optimal policy for \( \hat{V}_2(a, \cdot) \) (dropping dependence on \( a \) for notational simplicity). Suppose \( \pi^b \in \text{BR}_{3\varepsilon/4}(a) \), then we have

\[
V_2(a, \pi^* ) - V_2(a, \pi^b) \\
\leq V_2(a, \pi^* ) - \hat{V}_2(a, \pi^*) + \hat{V}_2(a, \pi^*) - \hat{V}_2(a, \tilde{\pi}^*) + \hat{V}_2(a, \tilde{\pi}^*) - \hat{V}_2(a, \pi^b) + \hat{V}_2(a, \pi^b) - V_2(a, \pi^b) \\
\leq \varepsilon/8 \leq 0 \leq 3\varepsilon/4 \leq \varepsilon/8
\]

\[
\leq 3\varepsilon/4 + 2 \cdot \varepsilon/8 \leq \varepsilon.
\]

This shows that \( \text{BR}_{3\varepsilon/4}(a) \subseteq \text{BR}_{\varepsilon}(a) \). Notably, this implies that the output \( \tilde{\pi}^b \in \text{BR}_\varepsilon(\tilde{a}) \), the desired optimality guarantee for \( \tilde{\pi}^b \).

Similar as above, take any \( \pi^b \in \text{BR}_{2\varepsilon/2}(a) \), we have

\[
\hat{V}_2(a, \tilde{\pi}^* ) - \hat{V}_2(a, \pi^b) \\
\leq \hat{V}_2(a, \tilde{\pi}^* ) - V_2(a, \tilde{\pi}^*) + V_2(a, \tilde{\pi}^*) - V_2(a, \pi^* ) + V_2(a, \pi^* ) - V_2(a, \pi^b) + V_2(a, \pi^b) - \hat{V}_2(a, \pi^b) \\
\leq \varepsilon/2 \leq 0 \leq \varepsilon/8 \leq \varepsilon/8
\]

\[
\leq \varepsilon/2 + 2 \cdot \varepsilon/8 \leq 3\varepsilon/4.
\]

This shows that \( \text{BR}_{2\varepsilon/2}(a) \subseteq \text{BR}_{3\varepsilon/4}(a) \), the other part of the claim.

**Stackelberg guarantee for \( \tilde{a} \)** Finally, we show the Stackelberg guarantee for \( \tilde{a} \). This part is similar as in the proof of Theorem 2. First, because \( \tilde{a} \) maximizes \( \tilde{\phi}_{3\varepsilon/4}(a) = \min_{\pi^b \in \text{BR}_{3\varepsilon/4}(a)} \hat{V}_1(a, \pi^b) \), we have for any \( a \in \mathcal{A} \) that

\[
\min_{\pi^b \in \text{BR}_{3\varepsilon/4}(\tilde{a})} \hat{V}_1(\tilde{a}, \pi^b) = \tilde{\phi}_{3\varepsilon/4}(\tilde{a}) \geq \tilde{\phi}_{3\varepsilon/4}(a) = \min_{\pi^b \in \text{BR}_{3\varepsilon/4}(a)} \hat{V}_1(a, \pi^b) \geq \min_{\pi^b \in \text{BR}_\varepsilon(a)} \hat{V}_1(a, \pi^b)
\]
where (i) is because \( \widehat{BR}_{3\varepsilon/4}(a) \subseteq BR_{\varepsilon}(a) \) for all \( a \). By the uniform convergence (21), we get
\[
\min_{\pi^b \in \widehat{BR}_{3\varepsilon/4}(\tilde{a})} V_1(\tilde{a}, \pi^b) \geq \min_{\pi^b \in BR_{\varepsilon}(a)} V_1(\tilde{a}, \pi^b) - 2 \cdot \varepsilon/8 \geq \phi_{\varepsilon}(a) - \varepsilon.
\]

Since the above holds for all \( a \in \mathcal{A} \), taking the max on the right hand side gives
\[
\max_{a \in \mathcal{A}} \phi_{\varepsilon}(a) - \varepsilon \leq \min_{\pi^b \in \widehat{BR}_{3\varepsilon/4}(\tilde{a})} V_1(\tilde{a}, \pi^b) \overset{(i)}{=} \min_{\pi^b \in BR_{\varepsilon/2}(\tilde{a})} V_1(\tilde{a}, \pi^b) = \phi_{\varepsilon/2}(\tilde{a}),
\]
where (i) is because \( \widehat{BR}_{3\varepsilon/4}(\tilde{a}) \supseteq BR_{\varepsilon/2}(a) \). In other words, we have
\[
\phi_{\varepsilon/2}(\tilde{a}) \geq \max_{a \in \mathcal{A}} \phi_{\varepsilon}(a) - \varepsilon = \max_{a \in \mathcal{A}} \phi_0(a) - \text{gap}_{\varepsilon} - \varepsilon.
\]
This is the first part of the bound for \( \tilde{a} \).

On the other hand, since \( \phi_{\varepsilon}(a) \) is increasing as we decrease \( \varepsilon \), we directly have
\[
\phi_{\varepsilon/2}(\tilde{a}) \leq \phi_0(\tilde{a}) \leq \max_{a \in \mathcal{A}} \phi_0(a).
\]
This is the second part of the bound for \( \tilde{a} \).

\[\square\]

D.3 Proof of Lemma D.1

We consider estimating a single reward \( r_h = r_{1,h} \). The bound for two rewards can be obtained by setting \( \delta \rightarrow \delta/2 \) and applying a union bound. Consider the MDP \( M^a \) which consists of \( S \) states, \( B \) actions, and \( H \) steps. Let \( V(a, \pi^b; r) \) denote the value function using the true MDP, policy \( \pi^b \) and reward function \( r \), and \( V(a, \pi^b; \hat{r}) \) denote the value function using the estimated reward \( \hat{r} \). Further, let
\[
\mathcal{S}_h^\delta := \left\{ s : \max_{\pi^b} \mathbb{P}_h^\delta(s) \geq \delta \right\},
\]
denote the set of \( \delta \)-significant states. By [18], the data gathering phase of Reward-Free RL-Explore obtains data where the \( h \)-th step is sampled i.i.d. from some policy \( \mu_h \), such that for any \( s \in \mathcal{S}_h^\delta \) we have
\[
\max_{\pi^b} \mathbb{P}_h^\delta(s, b) \leq 2SBH.
\]

We have for any \( \pi^b \) that
\[
\left| V_1(a, \pi^b) - V_1(a, \pi^b) \right| = \left| V(a, \pi^b; r) - V(a, \pi^b; \hat{r}) \right|
\]
\[
= \left| \sum_{h=1}^{H} \sum_{s,b} \mathbb{P}_h^\delta(s, b)(\hat{r}_h(s, b) - \mathbb{E}[r_h(s, b)]) \right|
\]
\[
\leq \left| \sum_{h=1}^{H} \sum_{s \notin \mathcal{S}_h^\delta, b} \mathbb{P}_h^\delta(s, b)(\hat{r}_h(s, b) - \mathbb{E}[r_h(s, b)]) + \sum_{h=1}^{H} \sum_{s \in \mathcal{S}_h^\delta, b} \mathbb{P}_h^\delta(s, b)(\hat{r}_h(s, b) - \mathbb{E}[r_h(s, b)]) \right|
\]
\[
\leq \sum_{h=1}^{H} \sum_{s \notin \mathcal{S}_h^\delta} \mathbb{P}_h^\delta(s, b) + \sum_{h=1}^{H} \sum_{s \notin \mathcal{S}_h^\delta, b} \mathbb{P}_h^\delta(s, b)(\hat{r}_h(s, b) - \mathbb{E}[r_h(s, b)])
\]
\[
:= \Delta_h
\]
\[
\leq HS\delta + \sum_{h=1}^{H} \Delta_h.
\]
For any $h$, by the Cauchy-Schwarz inequality, we have

$$
\sup_{\pi^h} \Delta_h \leq \sup_{\pi^h} \left[ \sum_{s \in S_h^1, b} \mathbb{P}^{\pi^h}_{h, b}(s) (\tilde{r}_h(s, b) - \mathbb{E}[r_h(s, b)])^2 \right]^{1/2}
$$

$$
\leq \sup_{\pi^h} \max_{\nu : S \rightarrow B} \left[ \sum_{s \in S_h^1, b} \mathbb{P}^{\pi^h}_{h, b}(s)(\tilde{r}_h(s, b) - \mathbb{E}[r_h(s, b)])^2 \mathbf{1}\{b = \nu(s)\} \right]^{1/2}
$$

(i) \quad \leq \max_{\nu : S \rightarrow B} \left[ 2SBH \cdot \sum_{s \in S_h^1, b} \mu_h(s, b)(\tilde{r}_h(s, b) - \mathbb{E}[r_h(s, b)])^2 \mathbf{1}\{b = \nu(s)\} \right]^{1/2}

(ii) \quad \leq \max_{\nu : S \rightarrow B} \left[ 2SBH \cdot \sum_{s \in S_h^1, b} \mu_h(s, b) \tilde{\delta} \left( \frac{1}{N_h(s, b)} \right) \cdot \mathbf{1}\{b = \nu(s)\} \right]^{1/2}

(iii) \quad \leq \max_{\nu : S \rightarrow B} \left[ 2SBH \cdot \sum_{s \in S_h^1, b} \mu_h(s, b) \tilde{\delta} \left( \frac{1}{N\mu_h(s, b)} \right) \cdot \mathbf{1}\{b = \nu(s)\} \right]^{1/2}

= \tilde{O} \left( \sqrt{\frac{S^2BH}{N}} \right).

Above, (i) used the fact that $\mathbb{P}^{\pi^h}_{h}(s)\mathbf{1}\{b = \nu(s)\} \leq 2SBH \cdot \mu_h(s, b)$ as $\{\pi^h_k\}^{h \leq h-1} \cup \{\nu\}$ is a valid policy. (ii) used the Hoeffding inequality (and a union bound) for the reward estimates, and the fact that the visitation of the reward-free algorithm is independent of the observed reward. (iii) used the multiplicative Chernoff bound for the visitation count $N_h(s, b) \sim \text{Bin}(N, \mu_h(s, b))$ and a union bound over $(s, b)$, which requires $N \geq O(1/\min_{s, b} \mu_h(s, b))$. Recall that Reward-Free RL-Explore used $\delta = \varepsilon/2H^2S$ and $\mu_h(s, b) \geq \frac{\varepsilon}{4H^2S^2B}$ for all $(s, b)$. Thus the requirement for $N$ is $N \geq O(H^3S^2B/\varepsilon^2)$ which is implied by our assumption that $N \geq \tilde{O}(H^3S^2B/\varepsilon^2)$.

Further, plugging in the choice of $N$ (with a sufficiently large constant) into the above bound yields

$$
\sup_{\pi^h} \Delta_h \leq \tilde{O} \left( \frac{S^2BH}{H^3S^2B/\varepsilon^2} \right) \leq \varepsilon/2H.
$$

This further implies that

$$
\left| \hat{V}_1(a, \pi^h) - V_1(a, \pi^h) \right| \leq HS \cdot \varepsilon/(2H^2S) + H \cdot \varepsilon/(2H) \leq \varepsilon,
$$

the desired result. \hfill \square

E \quad Proofs for Section 5

E.1 \quad Proof of Theorem 5

First by the guarantee (10) for the CoreSet subroutine, we have $K = |K| \leq 4d \log \log d + 16$. At each $j \in [K]$ and associated $(a_j, b_j) \in K$, as we queried the rewards for $N$ times, the empirical means satisfy (letting $\phi_j := \phi(a_j, b_j)$ for shorthand)

$$
\hat{\mu}_{i,j} = \phi_j^{\top} \theta_i^* + \tilde{z}_{i,j}, \quad i = 1, 2,
$$

where $\tilde{z}_{i,j}$ is the empirical mean of $N$ i.i.d. 1-sub-Gaussian noises, and thus is $1/N$-sub-Gaussian. Therefore, the weighted least squares estimator (9) can be expressed as (letting $\rho_j := \rho(a_j, b_j)$ for shorthand)

$$
\hat{\theta}_i = \arg \min_{\theta \in \mathbb{R}^d} \sum_{i=1}^{K} \rho_i(a_j, b_j)(\phi(a_j, b_j)^\top \theta - \hat{\mu}_{i,j})^2 = \left( \sum_{j=1}^{K} \rho_j \phi_j \phi_j^\top \right)^{-1} \sum_{j=1}^{K} \rho_j \phi_j \cdot \hat{\mu}_{i,j}
$$

27
We present a

\[ \begin{align*}
&= \left(\sum_{j=1}^{K} \rho_j \phi_j \phi_j^\top\right)^{-1} \sum_{j=1}^{K} \rho_j \phi_j (\phi_j^\top \theta_i^* + \tilde{z}_{i,j}) \\
&= \theta_i^* + \left(\sum_{j=1}^{K} \rho_j \phi_j \phi_j^\top\right)^{-1} \sum_{j=1}^{K} \rho_j \phi_j \tilde{z}_{i,j}.
\end{align*} \]

This implies the following guarantee (recall \( \Phi = \{ \phi(a, b) : (a, b) \in A \times B \} \)):

\[
\max_{\phi \in \Phi} |\phi^\top (\hat{\theta}_i - \theta_i^*)| \\
\leq \max_{j} |\tilde{z}_{i,j}| \cdot \max_{\phi \in \Phi} \left| \sum_{j=1}^{K} \rho_j \phi_j^\top \left( \sum_{j=1}^{K} \rho_j \phi_j \phi_j^\top \right)^{-1} \phi_j \right|
\]

\[
\leq \max_{j} |\tilde{z}_{i,j}| \cdot \max_{\phi \in \Phi} \left( \sum_{j=1}^{K} \rho_j \phi_j^\top \left( \sum_{j=1}^{K} \rho_j \phi_j \phi_j^\top \right)^{-1} \phi_j \right)^{1/2}
\]

\[
= \max_{j} |\tilde{z}_{i,j}| \cdot \max_{\phi \in \Phi} \left( \phi^\top \left( \sum_{j=1}^{K} \rho_j \phi_j \phi_j^\top \right)^{-1} \phi \right)^{1/2}
\]

\[
\leq \sqrt{2d} \cdot \max_{j} |\tilde{z}_{i,j}|.
\]

Above, (i) uses Jensen’s inequality (over the distribution induced by \( \rho_j \)), and (ii) used the property (10) of the core set. Now, as \( \tilde{z}_{i,j} \) is \( 1/N \)-sub-Gaussian, with probability at least \( 1 - \delta \), we have

\[
\max_{i=1,2} \max_{j \in [K]} |\tilde{z}_{i,j}| \leq \sqrt{\frac{\log(2K/\delta)}{N}} \leq C \sqrt{\frac{\log(d/\delta)}{N}}.
\]

Substituting this into the preceding bound yields

\[
\max_{\phi \in \Phi} |\phi^\top (\hat{\theta}_i - \theta_i^*)| \leq C \sqrt{\frac{\log(d/\delta)}{N}}.
\]

Choosing \( N = C d \log(d/\delta)/\varepsilon^2 \) guarantees that \( \max_{\phi \in \Phi} |\phi^\top (\hat{\theta}_i - \theta_i^*)| \leq \varepsilon/8 \). When this happens, we have for any \( (a, b) \in A \times B \) and any \( i = 1,2 \) that the estimated mean reward is close to the true reward:

\[
|\phi(a, b)^\top \hat{\theta}_i - \phi(a, b)^\top \theta_i^*| \leq \varepsilon/8.
\]

We can then proceed analogously to the proof of Theorem 2 to conclude that the output \( (\hat{a}, \hat{b}) \) satisfies \( \phi_0(\hat{a}) \geq \phi_{z/2}(\hat{a}) \geq \max_{a \in A} \phi_0(a) - \mathbf{gap}_\varepsilon - \varepsilon \) and \( \hat{b} \in \mathbf{BR}_\varepsilon(\hat{a}) \). Further, notice that the total amount of queries is

\[
NK \leq C d \log(d/\delta)/\varepsilon^2 \cdot d \log \log d = \tilde{O}(d^2/\varepsilon^2).
\]

This proves Theorem 5.

\[\square\]

### E.2 Lower bound

We present a \( \Omega(d/\varepsilon^2) \) lower bound for linear bandit games. This shows that the sample complexity upper bound in our Theorem 5 has at most an \( \tilde{O}(d) \) factor from the lower bound.
**Theorem E.1** (Lower bound for linear bandit games). There exists an absolute constant $c > 0$ such that the following holds. For any $\varepsilon \in (0, c)$, $g \in [0, c)$, and any algorithm that queries $n \leq c[d/\varepsilon^2]$ samples and outputs an estimate $\hat{\alpha} \in A$, there exists a linear bandit game $M$ with feature dimension $d$, on which $\text{gap}_e = g$ and the algorithm suffers from $(g + \varepsilon)$ error:

$$
\phi_{e/2}(\hat{\alpha}) \leq \phi_0(\hat{\alpha}) \leq \max_{a \in A} \phi_0(a) - g - \varepsilon.
$$

**Proof.** This lower bound is a direct corollary of the $\Omega(AB/\varepsilon^2)$ lower bound in Theorem 3. Specifically, we can pick the size of the action spaces $A', B'$ so that $d/2 \leq A'B' \leq d$, and take $\phi(a, b) = 1_{a,b} \in \mathbb{R}^d$ where $1_{a,b}$ is the standard basis vector with one at index $(a, b)$ (this index is understood as an index in $[d]$). This family of linear bandit games is equivalent to the family of bandit games with $A'B' \geq d/2$, for which any algorithm has to suffer from at least $(g + \varepsilon)$ error if the number of queries $n \leq cd/\varepsilon^2 \leq cA'B'/\varepsilon^2$ by (the hard instance construction of) Theorem 3. This proves Theorem E.1. □

## F Proofs for Section A

### F.1 Proof of Theorem A.1

Recall that Algorithm 4 pulled each arm $(a, b)$ for $N = O(\log(AB/\delta)/\varepsilon^2)$ times, and $\hat{\mu}_1(a, b)$, $\hat{\mu}_2(a, b)$ are the empirical means of the observed rewards. By the Hoeffding inequality and union bound over $(a, b)$, with probability at least $1 - \delta$, we have

$$
\max_{(a, b) \in A \times B} |\hat{\mu}_i(a, b) - \mu_i(a, b)| \leq \varepsilon/8 \quad \text{for } i = 1, 2. \quad (22)
$$

**Properties of $\widehat{\text{BR}}_{3\varepsilon/4}(a)$** On the uniform convergence event (22), we have the following: for any $b \in \text{BR}_{e/2}(a)$, we have

$$
\hat{\mu}_2(a, b) \geq \mu_2(a, b) - \varepsilon/8 \geq \max_{b' \in B} \mu_2(a, b') - 5\varepsilon/8 \geq \max_{b' \in B} \hat{\mu}_2(a, b') - 3\varepsilon/4,
$$

and thus $b \in \widehat{\text{BR}}_{3\varepsilon/4}(a)$. This shows that $\text{BR}_{e/2}(a) \subseteq \widehat{\text{BR}}_{3\varepsilon/4}(a)$. Similarly we can show that $\widehat{\text{BR}}_{3\varepsilon/4}(a) \subseteq \text{BR}_e(a)$. In other words,

$$
\text{BR}_e(a) \supseteq \widehat{\text{BR}}_{3\varepsilon/4}(a) \supseteq \text{BR}_{e/2}(a) \quad \text{for all } a \in A.
$$

Notably, this implies that $\hat{b} \in \widehat{\text{BR}}_{3\varepsilon/4}(\hat{a}) \in \text{BR}_e(\hat{a})$, the desired near-optimality guarantee for $\hat{b}$.

**Near-optimality of $\hat{\alpha}$** On the one hand, because $\hat{\alpha}$ maximizes $\hat{\mu}_1(a, \hat{b}(a))$, we have for any $a \in A$ that

$$
\max_{b' \in \text{BR}_{3\varepsilon/4}(\hat{a})} \hat{\mu}_1(\hat{a}, b') \overset{(i)}{=} \hat{\psi}_{3\varepsilon/4}(\hat{a}) \geq \hat{\psi}_{3\varepsilon/4}(a) \overset{(ii)}{=} \max_{b \in \text{BR}_{e/2}(a)} \hat{\mu}_1(a, b),
$$

where (i) is by definition of $\hat{\psi}_{3\varepsilon/4}$, and (ii) is because $\widehat{\text{BR}}_{3\varepsilon/4}(a) \supseteq \text{BR}_e(a)$. By the uniform convergence (22), we get that

$$
\max_{b' \in \text{BR}_{3\varepsilon/4}(\hat{a})} \mu_1(a, b') \geq \max_{b \in \text{BR}_{e/2}(a)} \mu_1(a, b) - 2\cdot \varepsilon/8 \geq \psi_{e/2}(a) - \varepsilon.
$$

Since the above holds for all $a \in A$, taking the max on the right hand side gives

$$
\max_{a \in A} \psi_{e/2}(a) - \varepsilon \leq \max_{b' \in \text{BR}_{3\varepsilon/4}(\hat{a})} \mu_1(\hat{a}, b') \overset{(i)}{=} \max_{b' \in \text{BR}_e(\hat{a})} \mu_1(\hat{a}, b') = \psi_e(\hat{a}),
$$

where (i) is because $\widehat{\text{BR}}_{3\varepsilon/4}(\hat{a}) \subseteq \text{BR}_e(a)$. This yields that

$$
\psi_e(\hat{a}) \geq \max_{a \in A} \psi_{e/2}(a) - \varepsilon \geq \max_{a \in A} \psi_0(a) - \varepsilon,
$$

and thus $\hat{\alpha} \in A$, and we can further rewrite the above as

$$
\psi_0(\hat{a}) \geq \max_{a \in A} \psi_0(a) - \varepsilon - [\psi_0(\hat{a}) - \psi_e(\hat{a})] \geq \max_{a \in A} \psi_0(a) - \text{gap}_e - \varepsilon.
$$

which is the desired bound for $\hat{\alpha}$. □
Algorithm 9 Subroutine BestCaseBestResponse($M, V_2$)

**Require:** MDP $M = (H, S, B, \mathbb{P}_h(\cdot|\cdot), r_{1,h}(\cdot, \cdot), r_{2,h}(\cdot, \cdot))$. Initial state $s_1 \in S$. Target value $V_2$.

1. Solve the following linear program over $\{d_h(s,b) : h \in [H], s \in S, b \in B\}$:

   $$\text{maximize} \sum_{h=1}^{H} \sum_{s \in S, b \in B} d_h(s,b) r_{1,h}(s,b)$$
   
   $$\text{s.t.} \sum_{h=1}^{H} \sum_{s \in S, b \in B} d_h(s,b) r_{2,h}(s,b) \geq V_2,$$
   
   $$\sum_{s \in S, b \in B} d_h(s,b) \mathbb{P}_h(s'|s,b) = \sum_{b' \in B} d_h(s,b') \quad \text{for all } 1 \leq h \leq H - 1, s' \in S,$$
   
   $$d_1(s_1, \cdot) \in \Delta_B, \quad d_1(s_1', \cdot) = 0 \quad \text{for all } s' \neq s_1.$$

Above, $\Delta_B$ denotes the probability simplex on $B$ (which is a set of $B + 1$ linear constraints).

Let $d_h$ denote the solution and $V_1'$ denote the value of the above program.

2. Set $\pi_1^h(b|s) \leftarrow d_h(s,b)/\sum_{b \in B} d_h(s,b)$ for all $(h, s, b)$ (with the convention $0/0 = 1/B$).

**output** $(\pi_1^h, V_1')$.

---

F.2 Proof of Theorem A.2

The proof is completely analogous to that of Theorem 4 and Theorem A.1: we first establish the uniform convergence of the form (21), and then analyze the value functions similarly as in the proof of Theorem 4, except that we replace $\min$ over best response sets to $\max$ over best response sets, similar as in Theorem A.1. The guarantee we get has the same form as in Theorem 4 except that we replace $\phi$-functions by $\psi$-functions, and replace $\mathsf{gap}_e$ with $\mathsf{gap}_e$. □

---

G Proofs for Section B

G.1 Proof of Theorem B.1

Recall that Algorithm 6 pulled each arm $(a, b) \in \mathcal{A} \times \mathcal{B}$ for $N = O((\log(AB/\delta)/\varepsilon^2)$ times, and $\hat{\mu}_1(a, b), \hat{\mu}_2(a, b)$ denote the empirical means of the observed rewards. By the Hoeffding inequality and union bound over $(a, b)$, with probability at least $1 - \delta$, we have

$$\max_{\pi^a \in \Delta, b \in B} |\hat{\mu}_i(\pi^a,b) - \mu_i(\pi^a,b)| = \max_{(a,b) \in \mathcal{A} \times \mathcal{B}} |\hat{\mu}_i(a,b) - \mu_i(a,b)| \leq \varepsilon/8 \quad \text{for } i = 1, 2. \quad (24)$$

**Properties of $\widehat{\mathsf{BR}}_{3\varepsilon/4}(\pi^a)$** On the uniform convergence event (24), we have the following: for any $b \in \widehat{\mathsf{BR}}_{\varepsilon/2}(\pi^a)$, we have

$$\hat{\mu}_2(\pi^a,b) \geq \mu_2(\pi^a,b) - \varepsilon/8 \geq \max_{b' \in B} \mu_2(\pi^a,b') - 5\varepsilon/8 \geq \max_{b' \in B} \hat{\mu}_2(\pi^a,b') - 3\varepsilon/4,$$

and thus $b \in \widehat{\mathsf{BR}}_{3\varepsilon/4}(\pi^a)$. This shows that $\mathsf{BR}_{\varepsilon/2}(\pi^a) \subseteq \widehat{\mathsf{BR}}_{3\varepsilon/4}(\pi^a)$. Similarly we can show that $\widehat{\mathsf{BR}}_{3\varepsilon/4}(\pi^a) \subseteq \mathsf{BR}_{\varepsilon}(\pi^a)$. In other words,

$$\mathsf{BR}_{\varepsilon}(\pi^a) \supseteq \widehat{\mathsf{BR}}_{3\varepsilon/4}(\pi^a) \supseteq \mathsf{BR}_{\varepsilon/2}(\pi^a) \quad \text{for all } \pi^a \in \Delta_{\mathcal{A}}.$$

Notably, this implies that $\hat{b} \in \widehat{\mathsf{BR}}_{3\varepsilon/4}(\pi^a) \in \mathsf{BR}_{\varepsilon}(\pi^a)$, the desired near-optimality guarantee for $\hat{b}$.

**Near-optimality of $\widehat{\pi}^a$** On the one hand, because $\widehat{\pi}^a$ approximately maximizes $\hat{\mu}_1(\pi^a, \hat{b}(\pi^a))$ (in the sense of (13)), we have for any $\pi^a \in \Delta_{\mathcal{A}}$ that

$$\min_{b' \in \mathsf{BR}_{3\varepsilon/4}(\pi^a)} \hat{\mu}_1(\pi^a,b') = \hat{\phi}_{3\varepsilon/4}(\pi^a) \geq \hat{\phi}_{3\varepsilon/4}(\pi^a) - \varepsilon/8 \geq \min_{b \in \mathsf{BR}_{\varepsilon}(\pi^a)} \hat{\mu}_1(\pi^a,b) - \varepsilon/8.$$
We first check that the BestMixedLeaderStrategy where \( \hat{e} \) is because (i) is because Algorithm 10 Subroutine where (i) is because \( \hat{e} \) this yields the first part of the bound for \( \hat{\phi}(\pi^a) \).

On the other hand, since maximising the value over \( b \) above problem is exactly the same as the linear program (25). Then, the above problem requires denoting the matrix of estimated rewards. Observe that (14) is equivalent to the following problem 

\[
\text{maximize } (\pi^a)^\top \hat{v}_b \\
\text{s.t. } (\pi^a)^\top (\hat{w}_b - \hat{w}_{b'}) \geq 0 \text{ for all } b' \in B \setminus \{b\}. \\
\pi^a \in \Delta_A.
\]

Let \( \hat{\pi}^a(b), \hat{u}(b) \) denote the solution and the value at the solution respectively.

4: Output \( \hat{b} = \arg \max_{b \in B} \hat{u}(b) \) and \( \hat{\pi}^a = \hat{\pi}^a(\hat{b}) \).

where (i) is because \( \hat{BR}_{\varepsilon/4}(\pi^a) \subseteq BR_{\varepsilon}(\pi^a) \). By the uniform convergence (24), we get that 

\[
\min_{b' \in BR_{\varepsilon/4}(\hat{\pi}^a)} \mu_1(\hat{\pi}^a, b') \geq \min_{b \in BR_{\varepsilon}(\pi^a)} \mu_1(\pi^a, b) - \varepsilon/4 - 2 \cdot \varepsilon/8 \geq \phi_{\varepsilon}(\pi^a) - \varepsilon.
\]

Since the above holds for all \( \pi^a \in \Delta_A \), taking the max on the right hand side gives 

\[
\sup_{\pi^a \in \Delta_A} \phi_{\varepsilon}(\pi^a) - \varepsilon \leq \min_{b' \in BR_{\varepsilon/4}(\hat{\pi}^a)} \mu_1(\hat{\pi}^a, b') \leq \min_{b \in BR_{\varepsilon/2}(\pi^a)} \mu_1(\hat{\pi}^a, b') = \phi_{\varepsilon/2}(\hat{\pi}^a),
\]

where (i) is because \( \hat{BR}_{\varepsilon/4}(\hat{\pi}^a) \supseteq BR_{\varepsilon/2}(\pi^a) \). In other words, 

\[
\phi_{\varepsilon/2}(\hat{\pi}^a) \geq \sup_{\pi^a \in \Delta_A} \phi_{\varepsilon}(\pi^a) - \varepsilon = \sup_{\pi^0 \in \Delta_A} \phi_{0}(\pi^0) - \text{gap}_{\varepsilon} - \varepsilon.
\]

This yields the first part of the bound for \( \hat{\pi}^a \).

On the other hand, since \( \phi_{\varepsilon}(\pi^a) \) is increasing as we decrease \( \varepsilon \), we directly have 

\[
\phi_{\varepsilon/2}(\hat{\pi}^a) \leq \phi_{0}(\hat{\pi}^a) \leq \sup_{\pi^a \in \Delta_A} \phi_{0}(\pi^a).
\]

This is the second part of the bound for \( \hat{\pi}^a \).

G.2 Proof of Theorem B.2

We first check that the BestMixedLeaderStrategy subroutine is a correct algorithm for solving (14).

Let 

\[
\hat{V} = (\hat{\mu}_1(a,b))_{a,b=1}^{A,B} \quad \text{and} \quad \hat{W} = (\hat{\mu}_2(a,b))_{a,b=1}^{A,B}
\]

denote the matrix of estimated rewards. Observe that (14) is equivalent to the following problem 

\[
\max_{\pi^a \in \Delta_A} \max_{b \in BR_{\varepsilon/4}(\pi^a)} \hat{\mu}_1(\pi^a, b) \\
= \max_{b \in B} \max_{\pi^a \in BR_{\varepsilon/4}(\pi^a) \ni b} (\pi^a)^\top \hat{V} e_b \\
= \max_{b \in B} \max_{\pi^a \in \Delta_A} (\pi^a)^\top \hat{W} e_b \\
\text{s.t. } (\pi^a)^\top \hat{W} e_b \geq (\pi^a)^\top \hat{W} e_{b'} \text{ for all } b' \in B,
\]

where \( e_b \in \Delta_B \) denotes the standard basis vector in \( B \) (1 at \( b \) and 0 at \( b' \neq b \)). For each \( b \), the above problem is exactly the same as the linear program (25). Then, the above problem requires maximizing the value over \( b \in B \), which is done in the output step of Algorithm 10. This shows that the BestMixedLeaderStrategy subroutine (Algorithm 10) is correct for solving (14). Note this
also proves that the arg max in (14) is attainable (instead of the sup in Theorem B.1 which may not be attainable in general).

The rest of the proof is analogous to Theorem B.1 where we can again establish the uniform convergence (24) and obtain the suboptimality guarantee in terms of $\psi$ and $\tilde{\text{gap}}_\epsilon$ instead of $\phi$ and $\text{gap}_\epsilon$, similar as in Theorem A.1.