

Zrnic, Tijana et al. (2021). “Who leads and who follows in strategic classification?”  
In: *Advances in Neural Information Processing Systems* 34, pp. 15257–15269.

## B. Online Appendix – to be put on a website but not into paper

[polish this part more]

In this section, we elaborate on the results of Section 3. We consider cases in which the short-run players’ information about the algorithm’s input is such that the algorithm is neither opaque nor transparent. We discuss under which condition the algorithm learns to play the Stackelberg action in each state.

Throughout, we maintain Assumptions 1 and 2. However, we do not impose Assumption 3. Given these assumptions, it is without loss of generality to assume that  $|S_{\text{SR}}| = 1$ ; otherwise, all statements hold conditional on each  $s \in S_{\text{SR}}$ . Moreover, we assume that the signalling structure  $(\Phi, p)$  has full support according to Definition 5.

Assume the short-run players can condition their actions on a subset of the outcomes of past interactions. Formally, for any period  $t$  let  $P^t$  be a partition of the set of histories

$$(S_Q \times A_Q \times U_Q)^t.$$

A strategy for the short-run player in period  $t$ ,  $\text{SR}^t$  is a map

$$\sigma_{\text{SR}^t} : P^{t-1} \times \Phi \rightarrow \Delta(A_{\text{SR}}).$$

This formulation includes the special cases in which the short-run players observe the entire history up to period  $t$  as well as the special case in which the short-run players do not observe any outcome of previous interactions.

### B.1. A necessary condition for learning the Stackelberg action

Consider the following auxiliary extensive-form game between the algorithmic player and one short-run player. The algorithmic player has  $|S_Q|$ -many types. Each cell  $s \in S_Q$  corresponds to a type of the algorithmic player. Each type of the algorithmic player has the same set of actions  $A_Q$ . First, nature draws the algorithmic player’s type  $s$  which is private information of the algorithmic player. After being informed of its type, the algorithmic player selects an action  $a_Q \in A_Q$ . After the algorithmic player takes its action  $a_Q$ , a signal  $\phi \in \Phi$  is drawn according to  $p(\cdot|a_Q)$ . The short-run player observes the signal  $\phi$  and takes an action  $a_{\text{SR}} \in A_{\text{SR}}$ .

For each  $a \in A_Q \times A_{SR}$  the payoffs of the short-run player is given by  $\mathbb{E}[u_{SR}(a, \omega)]$  and the payoff of the algorithmic player is given by  $\mathbb{E}[u_Q(a, \omega)|s]$  if its type is  $s$ . Denote this auxiliary game by  $G(S_Q, (\Phi, p))$ .

Let  $\tau_Q : S_Q \rightarrow A_Q$  and  $\tau_{SR} : \Phi \rightarrow A_{SR}$  be a strict Nash equilibrium of  $G(S_Q, (\Phi, p))$ .<sup>60</sup>

**[find an elegant way to add the qualifier “in any equilibrium”] [relate to Claim 1 in Appendix A.6]]**

**Theorem 5.** *For any  $\xi > 0$  there exists an open set of parameters  $\langle Q^0, (\alpha^t), (\varepsilon^t)_t \rangle$  and for each  $(s, a_Q)$  an open neighborhood  $\mathcal{O}_{(s, a_Q)}$  of*

$$\sum_{\phi \in \Phi} p(\phi | a_Q) \mathbb{E}[u_Q(a_Q, \tau_{SR}(\phi), \omega) | s]$$

*such that if  $Q^0(s, a_Q) \in \mathcal{O}_{(s, a_Q)}$  for each  $(s, a_Q)$ , then*

$$\mathbb{P} \left[ \lim_{T \rightarrow \infty} \frac{\sum_{t=0}^T \mathbb{1}\{(a_Q^t, s^t) = (\tau_Q(s), s)\}}{\sum_{t=0}^T \mathbb{1}\{s^t = s\}} = 1 \right] \geq 1 - \xi.$$

*Proof in Appendix ??.*

**Corollary 2.** *Suppose each action of the algorithmic player is the Stackelberg action for some state, i.e., for each  $a_Q$  there exists  $s \in S_Q$  such that  $a_Q = a_Q^{\text{Stack}}(s)$ . For any  $\xi > 0$  there exists  $\bar{\gamma} > 0$  and an open set of parameters  $\langle Q^0, (\alpha^t), (\varepsilon^t) \rangle$  such that for all  $\gamma$ -perfect signalling structures,  $0 < \gamma < \bar{\gamma}$ , and all states  $s \in S_Q$ ,*

$$\mathbb{P} \left[ \lim_{T \rightarrow \infty} \frac{\sum_{t=0}^T \mathbb{1}\{(a_Q^t, s^t) = (a_Q^{\text{Stack}}(s), s)\}}{\sum_{t=0}^T \mathbb{1}\{s^t = s\}} = 1 \right] \geq 1 - \xi.$$

Theorem 5 is a generalization of Theorem 2. For the case of a transparent algorithm, Theorem 2 shows that, when the  $Q$ -values are close to the expected payoffs when the short-run player plays according to a Nash equilibrium of the auxiliary games, then with probability close to 1, both the algorithmic player and the short-run players play according to this Nash equilibrium in almost all future periods. Theorem 5 generalizes this result in two directions. First, it allows for the possibility that the short-run players do not observe the current state of the algorithm.<sup>61</sup> In this case, the auxiliary game is an extensive form game with the

<sup>60</sup>The assumption that the signalling structure  $(\Phi, p)$  has full support ensures that each Nash equilibrium of the auxiliary extensive-form game is outcome-equivalent to a sequential equilibrium.

<sup>61</sup>The case in which the short-run players observe the algorithm's state corresponds to the case  $|S_Q| = 1$ .

algorithmic player's type equal to the current state. Second, Theorem 5 allows for the possibility that the short-run players do not observe the outcome of past interactions. In particular, Theorem 5 admits the possibility that the short-run players have no information about the outcome of past interactions. The theorem thus applies to the case of an opaque algorithm as well.<sup>62</sup> Why do Nash equilibria of the auxiliary game have a similar stability property when the algorithm is opaque? When the short-run players play according to a Nash equilibrium  $\tau_{\text{SR}}$  of the auxiliary game in all periods, the environment is stationary. The algorithm then learns to play a best-response to  $\tau_{\text{SR}}$ . This corresponds to playing according to the Nash equilibrium  $\tau_Q$ . When experimentation rates are low and the algorithm's greedy actions correspond to playing according to the Nash equilibrium, the short-run players' best-response is  $\tau_{\text{SR}}$ . When the short-run players know the  $Q$ -values, they keep playing according to  $\tau_{\text{SR}}$  until the greedy action no longer corresponds to  $\tau_Q$ . Theorems 2 and 2 show that the probability that this occurs for some period  $t$  can be made arbitrarily close to 1. When the short-run players do not know the  $Q$ -values – e.g., when they do not observe the outcome of past interactions – they play according to  $\tau_{\text{SR}}$  as long as they believe with probability close to 1 that the greedy action corresponds to  $\tau_Q$ .

Theorem 5 has an important consequence. Any condition on payoff functions that guarantees that the algorithm learns the Stackelberg action in each state must imply the following: the algorithmic player plays the Stackelberg action in any strict Nash equilibrium  $(\tau_Q, \tau_{\text{SR}})$  of the auxiliary extensive-form game, i.e.,  $\tau_Q(s) = a_Q^{\text{Stack}}(s)$ .<sup>63</sup> One might therefore conjecture that a sufficient condition for convergence to the Stackelberg outcome is that the Stackelberg outcome corresponds to a unique strict Nash equilibrium. The next example shows that this conjecture is incorrect.

**Example 5.** Suppose that  $|S_Q| = 1$  and the signals  $\phi$  are pure noise, i.e.,  $|\Phi| = 1$ . Suppose the players' action and payoffs are as in Figure 5. Suppose payoffs are deterministic. This game has a unique Nash equilibrium (in pure and mixed strategies)  $(T, L)$ . This Nash equilibrium is strict. Moreover,  $(T, L)$  is also the Stackelberg outcome.

Assume the algorithm is transparent. Choose  $Q^0(T) = Q^0(B) = 0$  and  $Q^0(M) = 1$ .<sup>64</sup> Fix an arbitrary  $\xi > 0$ . By an argument analogous to the proof of Theorem

<sup>62</sup>This is the reason why the theorem includes a hypothesis on the algorithm's parameters. Instead of the statement “there exists a period  $K$  such that if  $Q_K(s, a_Q) \in \mathcal{O}_{(s, a_Q)}$ ” Theorem 5 requires that  $Q^0(s, a_Q) \in \mathcal{O}_{(s, a_Q)}$  as well as conditions on the sequences  $(\alpha^t)$  and  $(\varepsilon^t)$ . The hypothesis on the initial  $Q$ -values is required because the event  $Q_K(s, a_Q) \in \mathcal{O}_{(s, a_Q)}$  need not be measurable with respect to the short-run players' information  $P^K$ . The requirements on  $(\alpha^t)$  and  $(\varepsilon^t)$  can be weakened. More precisely, for any  $(\tilde{\alpha}^t)$  and  $(\tilde{\varepsilon}^t)$ , there exists a  $K \in \mathbb{N}$  such that the parameters can be chosen to satisfy  $\alpha^t = \tilde{\alpha}^{t+K}$  and  $\varepsilon^t = \tilde{\varepsilon}^{t+K}$ .

<sup>63</sup>The hypotheses of Theorems 3 and 6 imply that this necessary condition is satisfied.

<sup>64</sup>The results stay unchanged if the initial  $Q$ -values are chosen from a sufficiently small open

|           |   | SR player |          |             |
|-----------|---|-----------|----------|-------------|
|           |   | L         | M        | R           |
| algorithm | T | 2, 2      | 0, 0     | 3, 0.4      |
|           | M | 0.02, 0.5 | 1, 1     | 0.01, -0.02 |
|           | B | 0.03, 0.9 | 4, 0.001 | -0.01, 5    |

Figure 5: A game

??, there exists a sequence of experimentation rates  $(\varepsilon^t)$  and updating parameters such that the probability that the  $Q$ -value for action  $M$  is the largest for all but an asymptotic fraction of periods less than  $\xi$  is at least  $1 - \xi$ . Consequently, there is a positive probability that the algorithm does not learn the Stackelberg action, and play fails to converge to a Nash equilibrium of the auxiliary game.<sup>65</sup> ■

The preceding example shows that play need not converge to a (pure) Nash equilibrium of the realized stage game when the algorithm is transparent. An immediate question is: under what conditions on the payoffs and the signalling structure does play converge to some Nash equilibrium, for all parameters of the algorithm? Theorem ?? below implies that looking for such conditions is futile: a transparent algorithm need not learn to play a strictly dominant action for an open set of parameters.

## B.2. Sufficient conditions for learning the Stackelberg action

In this section, we present conditions that are sufficient for the algorithm to learn the Stackelberg action.

**[find an elegant way to add the qualifier “in any equilibrium”]**

**Theorem 6.** *Suppose for each action  $a_Q \in A_Q$  there exists  $s \in S_Q$  such that*

$$\min_{a_{SR}} \mathbb{E}[u_Q(a_Q, a_{SR}, \omega)|s] > \max_{a_{SR}} \mathbb{E}[u_Q(a'_Q, a_{SR}, \omega)|s] \quad \forall a_Q \neq a'_Q. \quad (4)$$

*When the signals about the algorithm’s action are precise enough, the algorithm learns to play the Stackelberg action and receives approximately the Stackelberg payoff in each state.*

*Formally, there exists  $\bar{\gamma} > 0$  such that for all  $\gamma$ -perfect monitoring structures  $(\Phi, p)$  with  $\gamma \leq \bar{\gamma}$ , for all parameters  $\langle Q^0, (\alpha^t), (\varepsilon^t) \rangle$  of the algorithm and for every state*

---

neighborhood around the specified values.

<sup>65</sup>By virtually the same argument, one can show that play does not converge to the set of correlated equilibria.

$s \in S_Q$ ,

$$\lim_{T \rightarrow \infty} \frac{\sum_{t=0}^T \mathbb{1} \{a_Q^t = a_Q^{\text{Stack}}(s)\} \mathbb{1} \{\omega^t \in s\}}{\sum_{t=0}^T \mathbb{1} \{\omega^t \in s\}} = 1,$$

and

$$\lim_{T \rightarrow \infty} \frac{\sum_{t=0}^T u_Q(a_Q^t, a_{\text{SR}}^t, \omega^t) \mathbb{1} \{\omega^t \in s\}}{\sum_{t=0}^T \mathbb{1} \{\omega^t \in s\}} \in ((1 - \gamma)u_Q^{\text{Stack}}(s) - \gamma M, (1 - \gamma)u_Q^{\text{Stack}}(s) + \gamma M)$$

almost surely. Here,  $M$  is a bound on the norm of the algorithmic player's expected payoff.

*Proof in Appendix ??.*

**[add proof to appendix; make sure to include all Lemmas]**

Theorem 6 provides weaker sufficient conditions than 3 that ensures the algorithm learns the Stackelberg action in every state. The sufficient conditions are weaker in two respects.

First, the hypothesis that for each  $a_Q$  equation (4) holds for some state  $s \in S_Q$  is weaker than the hypotheses in Theorem 3.<sup>66</sup> Assumption 3 and the hypothesis that the algorithm's state space is a rich partition according to Definition 6 together imply that for each  $a_Q$  equation (4) holds for some  $s \in S_Q$ .

Second, Theorem 6 makes weaker assumptions on the short-run players' information about the outcome of past interactions. Theorem 3 assumed that the short-run players have no information about past outcomes. Theorem 3 allows for short-run players to observe all past outcomes or even a subset thereof. For example, Theorem 6 includes the case where short-run players observe the algorithm's past action or past states, but not its realized payoff. Moreover, the short-run player in period  $t$  can have more information about outcomes before period  $t - 1$  than  $\text{SR}_{t-1}$ . Nonetheless, both theorems require that  $\text{SR}^t$  does not observe the algorithm's information about the realization of  $\omega^t$ . This cannot be weakened without imposing stronger conditions on the (expected) payoff functions than equation (4).

We remark the following. How precise the signals must be, i.e.,  $\bar{\gamma}$  in the statement of Theorem 6, does not depend on the short-run players information about past outcomes, i.e., the partitions  $\{P_t\}$ . However, the conditions of Theorem 6 are not necessary for the algorithm to learn the Stackelberg outcome.<sup>67</sup>

<sup>66</sup>One could weaken this hypothesis as well: let  $A'_Q = \{a_Q \mid \exists s \in S_Q : a_Q^{\text{Stack}}(s) = a_Q\}$ . Then for each  $a_Q \in A'_Q$  there exists  $s \in S_Q$  such that equation (4) holds.

<sup>67</sup>To see this, consider the game with payoffs given in Figure 6. The Stackelberg payoff is 2 and is attained by the algorithmic player playing  $T$ . Suppose the algorithm is transparent so that the short-run player can condition her action on the  $Q$ -values. Suppose the signal  $\phi$  is pure noise. Eventually,  $Q^t(T) \geq 2$ . Consider a period  $t$  such that  $Q^{t-1}(B) < 2 < Q^t(B)$ . Let  $\tau$  be the next period  $T$  is played. Then  $Q_{\tau+1}(B) < Q_{\tau+1}(T)$  almost surely. Moreover, if the algorithm plays  $B$

|           |   |                 |      |
|-----------|---|-----------------|------|
|           |   | SR <sup>t</sup> |      |
|           |   | L               | R    |
| algorithm | T | 2, 1            | 4, 0 |
|           | B | 3, 0            | 0, 1 |

Figure 6: Payoff functions such that the algorithm achieves the Stackelberg payoff but the sufficient conditions of Theorem 6 fail.

|           |   |                 |      |                 |      |                 |   |      |      |
|-----------|---|-----------------|------|-----------------|------|-----------------|---|------|------|
|           |   | SR <sup>t</sup> |      | SR <sup>t</sup> |      | SR <sup>t</sup> |   |      |      |
|           |   | L               | R    | L               | R    | L               | R |      |      |
| algorithm | T | 3, 1            | 1, 0 | T               | 0, 1 | 0, 0            | T | 0, 1 | 0, 0 |
|           | M | 2, 1            | 0, 0 | M               | 1, 1 | 1, 0            | M | 0, 1 | 0, 0 |
|           | B | 0, 0            | 0, 1 | B               | 0, 0 | 0, 1            | B | 1, 0 | 1, 1 |
|           |   | s <sub>1</sub>  |      | s <sub>2</sub>  |      | s <sub>3</sub>  |   |      |      |

Figure 7: The payoff functions for the counterexample 6. In state  $s_1$ ,  $T$  is a strictly dominant action for the algorithm. Moreover, the Stackelberg payoff in  $s_1$  is attained when playing the strictly dominant action. In states  $s_2$  and  $s_3$ , the actions  $M$  and  $B$ , respectively, satisfy equation (4).

Can the condition in (4) be weakened to

$$\mathbb{E}[u_Q(a_Q, a_{SR}, \omega)|s] > \mathbb{E}[u_Q(a'_Q, a_{SR}, \omega)|s] \quad \forall a'_Q \neq a_Q, a_{SR} \in A_{SR}?$$

That is, is it sufficient for Theorem 6 that for each action  $a_Q$  there exists  $s \in S_Q$  such that this action  $a_Q$  is strictly dominant action for payoffs  $\mathbb{E}[u_Q(\cdot, a_{SR}, \omega)|s]$ ? The following Example 6 shows that this is not the case.

**Example 6.** Suppose  $A_Q = \{T, M, B\}$  and  $A_{SR} = \{L, R\}$ . Suppose the state space of the algorithm contains three elements,  $S_Q = \{s_1, s_2, s_3\}$ . Suppose that expected payoffs are given by the payoff matrices in Figure 7. The Stackelberg actions are  $T$ ,  $M$  and  $B$  in states  $s_1$ ,  $s_2$  and  $s_3$  respectively. Moreover, the Stackelberg action in each state is strictly dominant. Note, however, that equation (4) is not satisfied for the action  $T$  in any state.

Assume all states occur with probability  $1/3$ . Let the signalling structure be

---

in  $t + 1$ , then  $Q_{t+2}(B) < 2 \leq Q^{t+1}(T)$ . Consequently, the algorithmic player receives a payoff of 0 in a period  $t$  only if it experimented in period  $t - 1$ . Because  $\varepsilon^t \rightarrow 0$ , the algorithm's long-run average payoff is above 2 almost surely.

given by  $\Phi = \{\phi_T, \phi_M, \phi_B\}$  and, for an  $x \in (0, 1)$ ,

$$\begin{aligned} p(\phi_T|T) &= p(\phi_M|M) = p(\phi_B|B) = 1 - \gamma; \\ p(\phi_M|B) &= p(\phi_M|T) = p(\phi_T|B) = p(\phi_B|T) = \gamma/2; \\ p(\phi_T|M) &= x\gamma, p(\phi_B|M) = 1 - \gamma - x\gamma. \end{aligned}$$

Let<sup>68</sup>

$$\begin{aligned} Q^0(s_1, T) &= 1, Q^0(s_1, M) = 2, Q^0(s_1, B) = 0; \\ Q^0(s_2, M) &= 1, Q^0(s_2, T) = Q^0(s_2, B) = 0; \\ Q^0(s_3, B) &= 1, Q^0(s_3, T) = Q^0(s_3, M) = 0. \end{aligned}$$

Then the algorithm plays according to

$$\tau_Q : s_1 \rightarrow M, s_2 \rightarrow M, s_3 \rightarrow B,$$

up to experimentation. For  $x > 0$  and  $\gamma > 0$  small enough, the unique best-response of the short-run player is

$$\tau_{\text{SR}} : \phi_T \mapsto R, \phi_M \mapsto L, \phi_B \mapsto R.$$

Given this strategy, the expected payoff to the algorithm in state  $s_1$  when playing  $T$  is  $1 + \gamma$  and when playing  $M$  is  $2(1 - \gamma)$ . The latter is strictly larger than the former for  $\gamma < 1/2$ . Consequently,  $(\tau_Q, \tau_{\text{SR}})$  is a strict equilibrium of the auxiliary extensive-form game. By Theorem 5, there exists parameters  $\langle Q^0, (\alpha^t), (\varepsilon^t) \rangle$  such that  $\mathbb{E}[u_Q(a_Q^t, a_{\text{SR}}^t, \omega^t) | s_1] < 5/2$  for all  $t$ . Moreover, this holds irrespective of the short-run players' information about past play. The example shows: for any  $\bar{\gamma}$  there exists a  $\gamma$ -perfect signalling structure,  $0 < \gamma < \bar{\gamma}$  and parameters of the algorithm such that the limit of the algorithm's expected average payoff is bounded away from the state-by-state Stackelberg payoff. ■

---

<sup>68</sup>It suffices to assume that the  $Q$ -values are in a neighborhood of the ones specified here.