

Full Appendix

## A Proofs for Section §3

### A.1 Proof of Lemma 3.2

*Goal.* For any fixed  $(q, C_t(q), d^+)$  and any  $d^- \in C_t(q)$ , show

$$\mathbf{1}[s_\theta(q, d^-) \geq s_\theta(q, d^+)] \leq \frac{1}{\log 2} \mathcal{L}_{\text{NCE}}^{(1)}(\theta; q, C_t(q), d^+). \quad (1)$$

where

$$\begin{aligned} & \mathcal{L}_{\text{NCE}}^{(1)}(\theta; q, C_t(q), d^+) \\ &= \log \left( 1 + \sum_{d \in C_t(q)} \exp \left( \frac{s_\theta(q, d) - s_\theta(q, d^+)}{\tau} \right) \right), \quad \tau > 0. \end{aligned} \quad (2)$$

Averaging (1) over  $(q, d^+, C_t(q), d^-)$  then yields the bound on  $X_t$ .

*Step 1: Log-sum-exp dominates any single negative.* Fix  $q, C_t(q)$  and  $d^+ \in D_q^+$ . For any  $d^- \in C_t(q)$ , define  $z := (s_\theta(q, d^-) - s_\theta(q, d^+))/\tau$ . Since all terms in the sum are nonnegative,

$$\sum_{d \in C_t(q)} e^{(s_\theta(q, d) - s_\theta(q, d^+))/\tau} \geq e^z,$$

hence

$$\mathcal{L}_{\text{NCE}}^{(1)}(\theta; q, C_t(q), d^+) \geq \log(1 + e^z). \quad (3)$$

*Step 2: Normalized softplus upper-bounds the indicator.*  $h(z) := \log(1 + e^z)/\log 2$  is increasing,  $h(0) = 1$ , and  $h(z) \geq 0$ ; thus

$$\mathbf{1}[z \geq 0] \leq \frac{\log(1 + e^z)}{\log 2}. \quad (4)$$

*Step 3: Combine Steps 1–2.*

$$\begin{aligned} & \mathbf{1}[s_\theta(q, d^-) \geq s_\theta(q, d^+)] \\ &= \mathbf{1}[z \geq 0] \\ &\leq \frac{\log(1 + e^z)}{\log 2} \\ &\leq \frac{\mathcal{L}_{\text{NCE}}^{(1)}(\theta; q, C_t(q), d^+)}{\log 2}. \end{aligned} \quad (5)$$

Averaging proves the claim.

### A.2 Proof of Proposition 3.4

Let  $Y = \mathbf{1}_{[g=+1]}$  be the clean anchor label on a flipped item ( $\pi = \text{YES}$ ). WF replaces  $Y$  by a constant weight  $w \in [0, 1]$ . Consider

$$\begin{aligned} J(w) &= \mathbb{E}[(w - Y)^2 \mid \pi = \text{YES}] \\ &= (w - 1)^2 \Pr(Y=1 \mid \pi=\text{YES}) + w^2 \Pr(Y=0 \mid \pi=\text{YES}). \end{aligned} \quad (6)$$

Then  $J'(w) = 2w - 2 \Pr(Y=1 \mid \pi=\text{YES})$ , so the unique minimizer in  $[0, 1]$  is

$$w^\star = \Pr(Y=1 \mid \pi=\text{YES}) = \Pr[g=+1 \mid \pi=\text{YES}] = 1 - \sigma_t.$$

### A.3 A bound on the per-anchor InfoNCE loss

Assume bounded logits  $|s_\theta(q, \cdot)| \leq B$  and  $|C_t(q)| \leq K$ . For any anchor  $a$  (true or flipped),

$$\begin{aligned} \mathcal{L}^{(1)}(\theta; q, C_t(q), a) &= \log \left( 1 + \sum_{d \in C_t(q)} \exp \left( \frac{s_\theta(q, d) - s_\theta(q, a)}{\tau} \right) \right) \\ &\leq \log(1 + K e^{2B/\tau}) \doteq \ell_{\max}(B, K, \tau). \end{aligned} \quad (7)$$

#### 1 A.4 Proof of Proposition 3.3

2 Compare the *unweighted* clean objective (true positives only) to WF, which adds flipped anchors with weight  $w_{\text{flip}}$ . For a fixed  $(q, C_t(q))$ ,  
3 write  $F_t(q) = F_t^+(q) \dot{\cup} F_t^-(q)$  for truly positive vs. false flips. The per-list increment is  
4

$$5 \quad \Delta(q) = (w_{\text{flip}} - 1) \sum_{a \in F_t^+(q)} \mathcal{L}^{(1)}(\theta; \cdot, a) + w_{\text{flip}} \sum_{a \in F_t^-(q)} \mathcal{L}^{(1)}(\theta; \cdot, a). \quad (8)$$

6 Since  $w_{\text{flip}} \leq 1$ , the first term is nonpositive; hence  
7

$$8 \quad \Delta(q)_+ \leq w_{\text{flip}} \sum_{a \in F_t^-(q)} \mathcal{L}^{(1)}(\theta; q, C_t(q), a) \quad (9)$$

$$9 \quad \leq w_{\text{flip}} \ell_{\max}(B, K, \tau) |F_t^-(q)| \quad (\text{using App. A.3}).$$

10 Taking expectations and writing  $m_t = \mathbb{E}_q[|F_t(q)|]$  and  $\sigma_t = \Pr[g = -1 \mid a \in F_t(q)]$ ,  
11

$$12 \quad \zeta_t = \frac{1}{\log 2} \mathbb{E}[\Delta(q)_+] \leq \underbrace{\frac{m_t}{\log 2} \ell_{\max}(B, K, \tau)}_{C_{\text{loss}}(B, K, \tau, m_t)} w_{\text{flip}} \sigma_t. \quad (10)$$

13 With  $w_{\text{flip}}^\star = 1 - \sigma_t$ ,  $\zeta_t \leq C_{\text{loss}} \sigma_t (1 - \sigma_t) \leq C_{\text{loss}}/4$ .  
14

#### 15 A.5 Properties of $f(\rho)$ in Equation (5) to (6)

16 *Setup and notation.* Let  $A := 1 - \alpha > 0$  and  $B := \gamma \in [0, 1)$  with  $A > B$  when  $\alpha + \gamma < 1$ . Fix a pool with *pre-judge* hidden-positive rate  
17  $\rho \in [0, 1]$ .  
18

19 *Derivation of  $f(\rho)$ .* Among the items the judge keeps as No,  
20

$$21 \quad f(\rho) = \Pr(g = +1 \mid \pi = \text{No}) \\ 22 \quad = \frac{\Pr(\pi = \text{No} \mid g = +1) \Pr(g = +1)}{\Pr(\pi = \text{No})} = \frac{B\rho}{A(1 - \rho) + B\rho}. \quad (11)$$

23 *Derivative at 0.*  $f$  is smooth on  $[0, 1)$  and  
24

$$25 \quad f'(\rho) = \frac{BA}{(A - (A - B)\rho)^2}; \quad \text{hence} \quad f'(0) = \frac{B}{A} = \kappa.$$

26 *Global quadratic upper bound.* For all  $\rho \in [0, 1]$ ,

$$27 \quad f(\rho) \leq \rho - \frac{A - B}{A} \rho(1 - \rho), \quad (12)$$

28 because  
29

$$30 \quad \rho - f(\rho) = \frac{A - B}{A - (A - B)\rho} \rho(1 - \rho) \geq \frac{A - B}{A} \rho(1 - \rho).$$

31 *Local linear bound with explicit  $\bar{\rho}(\epsilon)$ .* Using Taylor with remainder,  $f(\rho) = \kappa\rho + \frac{\rho^2}{2} f''(\xi_\rho)$  where  $f''(\rho) = \frac{2AB(A - B)}{(A - (A - B)\rho)^3}$ . For  
32  $\rho \leq A/(2(A - B))$ ,  $f''(\rho) \leq 16AB(A - B)/A^3$ . Set  
33

$$34 \quad \bar{\rho}(\epsilon) := \min \left\{ \frac{A}{2(A - B)}, \frac{\epsilon A^3}{8AB(A - B)} \right\}.$$

35 Then  $f(\rho) \leq (\kappa + \epsilon)\rho$  for  $\rho \in [0, \bar{\rho}(\epsilon)]$ .  
36

#### 37 A.6 Proof of Lemma 3.6: Drifted recursion

38 Let  $(q, d)$  be drawn from the mixture  $P_t^-(\cdot \mid q)$  after marginalizing  $q$ , and define the *global* hidden-positive rate  $\rho_t := \Pr[g = +1]$  under this  
39 mixture. Re-judge with the same  $(\alpha, \gamma)$  to obtain  $U_t$ . By Bayes,  
40

$$41 \quad \mathbb{E}_{U_t} \mathbf{1}[g = +1] = \Pr(g = +1 \mid \pi = \text{No}) \\ 42 \quad = \frac{\gamma \rho_t}{(1 - \alpha)(1 - \rho_t) + \gamma \rho_t} = f(\rho_t). \quad (13)$$

43 By the variational characterization of TV on  $[0, 1]$ ,

$$44 \quad \rho_{t+1} = \mathbb{E}_{P_{t+1}^-} \mathbf{1}[g = +1] \\ 45 \quad \leq \mathbb{E}_{U_t} \mathbf{1}[g = +1] + \text{TV}(P_{t+1}^-, U_t) = f(\rho_t) + \delta_t. \quad (14)$$

117 Using the global quadratic bound on  $f$  yields

$$118 \quad \rho_{t+1} \leq \rho_t - c \rho_t (1 - \rho_t) + \delta_t \quad \text{with} \quad c = \frac{1-\alpha-\gamma}{1-\alpha}. \quad 175$$

## 120 A.7 Proof of Lemma 3.7: Entry into the local region

122 Let  $c = 1 - \kappa > 0$  and  $g(\rho) = \rho - c\rho(1 - \rho) + \bar{\delta}$ . The fixed-point equation  $g(\rho) = \rho$  is  $c\rho(1 - \rho) = \bar{\delta}$  with roots

$$123 \quad \rho_{\pm} = \frac{1}{2} \left( 1 \pm \sqrt{1 - 4\bar{\delta}/c} \right). \quad 181$$

125 If  $\rho_t \geq \frac{1}{2}$  then  $\rho_{t+1} \leq \rho_t - \frac{c}{4} + \bar{\delta} < \rho_t$  since  $\bar{\delta} < c/4$ , so in finitely many steps  $\rho_t \leq \frac{1}{2}$ . If  $\rho_t \in (\rho_-, \frac{1}{2}]$ , then  $c\rho_t(1 - \rho_t) > \bar{\delta}$  and hence  
126  $\rho_{t+1} \leq g(\rho_t) < \rho_t$ . Continuity implies finite-time entry into  $[0, \rho_- + \eta] \subseteq [0, \bar{\delta}(\epsilon)]$  for some  $\eta > 0$ .

## 128 A.8 Proof of Theorem 3.8: Local geometric convergence

129 Inside the local region,  $f(\rho) \leq r\rho$ , so for all  $t \geq T$  we have  $\rho_{t+1} \leq r\rho_t + \delta_t$ . Unrolling this recursion yields

$$131 \quad \begin{aligned} \rho_t &\leq r^{t-T} \rho_T + \sum_{i=0}^{t-T-1} r^i \delta_{t-1-i} \\ 132 &\leq r^{t-T} \rho_T + \frac{\bar{\delta}}{1-r} (1 - r^{t-T}). \end{aligned} \quad 189$$

136 For the pairwise risk, define  $X_t := \mathbb{E}[I_t]$ . By the law of total expectation and  $\Pr(g = +1) = \rho_t$  (hence  $\Pr(g = -1) = 1 - \rho_t$ ),

$$137 \quad \begin{aligned} X_t &= \rho_t \mathbb{E}[I_t | g = +1] + (1 - \rho_t) \mathbb{E}[I_t | g = -1] \\ 138 &\leq \rho_t \mathbb{E}[I_t | g = +1] + (1 - \rho_t) \mathbb{E}[I_t | g = -1] + \zeta_t \\ 139 &\leq \rho_t + (1 - \rho_t) \eta + \zeta_t, \end{aligned} \quad 195$$

141 where the second line uses that, under WF optimization, the realized pairwise risk is within  $\zeta_t$  of the conditional-mixture expression (i.e.,  $\zeta_t$   
142 upper-bounds the WF slack; Prop. 3.3 / App. A.4), and the last line uses Lemma 3.2 and Assumption A2.

143 Substituting the bound on  $\rho_t$  from Eq. (15) into Eq. (16) yields Eq. (8) in the main text.

## 145 A.9 Proof of Proposition 3.9

146 From  $X_t \leq \eta_t + (1 - \eta_t)\rho_t + \zeta_t$  and  $\eta_{t+1} \leq \eta_t$ ,  $\zeta_{t+1} \leq \zeta_t$ , we have

$$147 \quad \begin{aligned} X_{t+1} - X_t &\leq (1 - \eta_t)(\rho_{t+1} - \rho_t) + (\zeta_{t+1} - \zeta_t) \\ 148 &\leq (1 - \eta_t)(f(\rho_t) - \rho_t + \delta_t) + (\zeta_{t+1} - \zeta_t), \end{aligned} \quad 205$$

150 using Lemma 3.6. Apply the quadratic bound on  $f$  for the sufficient condition.

## 152 A.10 Proof of Corollary 3.10

153 From  $X_0 \leq \eta + (1 - \eta)\rho_0 + \zeta_0$  and

$$155 \quad X_{\star} = \eta + (1 - \eta) \frac{\bar{\delta}}{1-r} + \bar{\zeta}, \quad 212$$

156 the condition

$$157 \quad \rho_0 > \frac{\bar{\delta}}{1-r} + \frac{\bar{\zeta} - \zeta_0}{1-\eta} \quad 215$$

159 implies  $X_0 > X_{\star}$ . Under forward correction  $\zeta_0 = \bar{\zeta} = 0$ .

## 161 A.11 Proof of Corollary 3.11

163 From (15), if  $\delta_t \rightarrow 0$  then for any  $\varepsilon > 0$  there exists  $M$  with  $\sup_{j \geq M} \delta_j < \varepsilon$ , so for all large  $t$ ,

$$164 \quad \sum_{i=0}^{t-T-1} r^i \delta_{t-1-i} \leq \varepsilon \sum_{i=0}^{\infty} r^i = \frac{\varepsilon}{1-r}. \quad 222$$

167 Letting  $t \rightarrow \infty$  gives  $\limsup_t \rho_t \leq \varepsilon/(1-r)$ ; since  $\varepsilon$  is arbitrary,  $\rho_t \rightarrow 0$ . Then

$$168 \quad X_t \leq \eta + (1 - \eta)\rho_t + \zeta_t \rightarrow \eta; \quad \text{if } \eta \rightarrow 0, \text{ then } X_t \rightarrow 0. \quad 226$$

170 *Sufficient conditions.* By the drift decomposition in App. A.13, if the miner/judge operator is locally Lipschitz in  $\theta$  with fixed abstention  
171 thresholds and  $\theta_t$  stabilizes, then support overlap tends to one and in-support reweight drift vanishes, implying  $\delta_t \rightarrow 0$ . Under precision  
172 gating with  $w_{\text{flip}} \leq 1 - \sigma_t$  and a judge whose  $\alpha_t \downarrow 0$  at nontrivial prevalence  $\pi_t^+ \in (0, 1)$ , Eq.(2) gives  $\sigma_t \rightarrow 0$  and hence  $\zeta_t \leq C_{\text{loss}}\sigma_t(1 - \sigma_t) \rightarrow 0$   
173 by Prop.3.3 and Prop. 3.4.

## 233 A.12 Forward correction is unbiased

234 PROPOSITION A.1 (FORWARD CORRECTION IS UNBIASED). *Under class-conditional noise with confusion matrix  $T$ , the forward-corrected listwise  
235 loss  $\ell_{\text{fc}}$  satisfies  $\mathbb{E}_{\pi|g}[\ell_{\text{fc}}] = \ell_{\text{clean}}$  for each  $(q, C_t(q), d^+)$ ; hence  $\mathbb{E}[\ell_{\text{fc}}] = \mathbb{E}[\ell_{\text{clean}}]$ .*

236 *Sketch.* Let  $\ell_{\text{clean}}$  be the clean per-list loss and  $\ell_{\text{fc}}$  the forward-corrected one. With class-conditional noise  $\Pr(\pi = k | g = j) = T_{jk}$ , the  
237 forward correction replaces the observed one-hot over  $\pi$  by  $T^{-1}$  times the observed label vector. Linearity gives  $\mathbb{E}_{\pi|g}[\ell_{\text{fc}}] = \ell_{\text{clean}}$ , hence  
238  $\mathbb{E}[\ell_{\text{fc}}] = \mathbb{E}[\ell_{\text{clean}}]$ .  
239

## 240 A.13 Drift bound via pool churn

241 *Definition A.2 (Total variation (TV) drift budget).* Let  $U_t(\cdot | q)$  be the distribution obtained by re-judging draws from  $P_t^- (\cdot | q)$  with the  
242 same  $(\alpha, \gamma)$ . Define  
243

$$\delta_t := \mathbb{E}_q[\text{TV}(P_{t+1}^-(\cdot | q), U_t(\cdot | q))]. \quad (18)$$

244 *Two precise bounds.* We provide (i) a general bound that separates support churn and in-intersection reweight drift, and (ii) a cardinality  
245 corollary under a uniform-within-support mining model.  
246

247 **General bound (support churn + reweight drift).** For each  $q$ , let  $M_t(\cdot | q)$  be the mining distribution on  $\mathcal{D}$  and  $\mathcal{J}$  the judge-and-gating  
248 operator mapping  $\mu$  to the post-judge “No” distribution  
249

$$\mathcal{J}(\mu)(A) := \frac{\int_A \mathbf{1}\{\pi(q, d) = \text{No}\} d\mu(d)}{\int_{\mathcal{D}} \mathbf{1}\{\pi(q, d) = \text{No}\} d\mu(d)}. \quad (19)$$

250 Then  $P_t^- (\cdot | q) = \mathcal{J}(M_t(\cdot | q))$  and  $U_t(\cdot | q) = \mathcal{J}(P_t^- (\cdot | q))$ . By triangle inequality,  
251

$$\begin{aligned} \text{TV}(P_{t+1}^-(\cdot | q), U_t(\cdot | q)) &\leq \text{TV}(\mathcal{J}(M_{t+1}), \mathcal{J}(M_t)) \\ &\quad + \underbrace{\text{TV}(\mathcal{J}(M_t), \mathcal{J}(P_t^-))}_{=0}, \end{aligned} \quad (20)$$

252 since  $\mathcal{J}$  is idempotent on its image. Decompose  $M_t$  and  $M_{t+1}$  by the intersection  $I_t(q) = \text{supp } M_t \cap \text{supp } M_{t+1}$  and its complement to  
253 obtain  
254

$$\text{TV}(\mathcal{J}(M_{t+1}), \mathcal{J}(M_t)) \leq |\lambda_{t+1} - \lambda_t| + \lambda_\star \text{TV}(\mathcal{J}(\tilde{M}_{t+1}^I), \mathcal{J}(\tilde{M}_t^I)), \quad (21)$$

255 where  $\lambda_t = M_t(I_t(q))$ ,  $\lambda_{t+1} = M_{t+1}(I_t(q))$ ,  $\lambda_\star = \max\{\lambda_t, \lambda_{t+1}\}$ . As  $\mathcal{J}$  is 1-Lipschitz in TV when restricted to a fixed support (policy fixed on  
256  $I_t(q)$ ), let  
257

$$\omega_t(q) := \text{TV}(\tilde{M}_{t+1}^I(\cdot | q), \tilde{M}_t^I(\cdot | q)), \quad \chi_t^{(\text{mass})} := \mathbb{E}_q[|\lambda_{t+1}(q) - \lambda_t(q)|],$$

258 we get  
259

$$\delta_t \leq \chi_t^{(\text{mass})} + \Omega_t, \quad \Omega_t := \mathbb{E}_q[\omega_t(q)].$$

260 **Cardinality corollary (uniform within support).** If the miner samples uniformly on finite supports  $S_t(q)$  and  $S_{t+1}(q)$  (e.g., top- $K$  lists),  
261 and the judge policy is fixed on the intersection, then  
262

$$\chi_t^{(\text{mass})} \leq \mathbb{E}_q\left[1 - \frac{|S_{t+1}(q) \cap S_t(q)|}{|S_t(q)|}\right] = \chi_t, \quad \Omega_t = 0,$$

263 hence  $\delta_t \leq \chi_t$ . Approximate ANN/top- $K$  effects contribute additively by a small  $\zeta_t^{\text{ANN}}$ , giving  $\delta_t \leq \chi_t + \zeta_t^{\text{ANN}}$ .  
264

## 265 A.14 Derivations for Equation (2) and (4)

266 By Bayes,  
267

$$\begin{aligned} \sigma_t &= \Pr[g = -1 | \pi = \text{YES}] \\ &= \frac{\Pr(\pi = \text{YES} | g = -1) \Pr(g = -1)}{\Pr(\pi = \text{YES})} \\ &= \frac{\alpha(1 - \pi_t^+)}{(1 - \gamma)\pi_t^+ + \alpha(1 - \pi_t^+)}, \end{aligned} \quad (22)$$

268 giving Eq.(2). To enforce  $\sigma_t \leq \sigma^\star \in (0, 1)$ , solve for  $\alpha$ :  
269

$$\alpha(1 - \pi_t^+) \leq \sigma^\star((1 - \gamma)\pi_t^+ + \alpha(1 - \pi_t^+)) \iff \alpha \leq \frac{\sigma^\star(1 - \gamma)\pi_t^+}{(1 - \pi_t^+)(1 - \sigma^\star)}, \quad (23)$$

270 which is Eq.(4).  
271

349    **LEMMA A.3 (MINIMAX-SAFE FLIP WEIGHTING).** *Let  $\sigma_t = \Pr[g = -1 \mid \pi = \text{Yes}]$  and suppose the per-anchor InfoNCE loss is bounded by  $\ell_{\max}$*   
 350 *(App. A.3). Then for*

$$351 \quad G_+(w) := (\mathbb{E}[\tilde{\mathcal{L}}_{\text{WF}}^{(1)}] - \mathbb{E}[\mathcal{L}_{\text{clean}}^{(1)}])_+, \quad G_-(w) := (\mathbb{E}[\mathcal{L}_{\text{clean}}^{(1)}] - \mathbb{E}[\tilde{\mathcal{L}}_{\text{WF}}^{(1)}])_+, \quad (24)$$

352 *we have  $G_+(w) \leq \ell_{\max} m_t w \sigma_t$  and  $G_-(w) \leq \ell_{\max} m_t (1-w)(1-\sigma_t)$ ; the minimax  $w^* = \arg \min_w \max\{G_+(w), G_-(w)\}$  equals  $1 - \sigma_t$ . Moreover,*  
 353 *for any  $w \leq 1 - \sigma_t$ ,*

$$354 \quad \max\{G_+(w), G_-(w)\} \leq \ell_{\max} m_t (1-w)(1-\sigma_t) \leq \ell_{\max} m_t \sigma_t (1-\sigma_t),$$

355 *with equality at  $w = 1 - \sigma_t$ .*

## B Proofs for Section 4

### B.1 Proof of Proposition 4.1 (bias under fixed adversary)

360 Let  $F(\theta, \tau) = \nabla_\theta L_{\text{distill}}(\theta; \phi^*) + \tau \nabla_\theta L_{\text{adv}}(\theta; \phi^*)$  with  $\tau = \lambda_{\text{adv}}/\lambda_{\text{distill}}$ . Since  $L_{\text{distill}}(\cdot; \phi^*)$  is  $C^2$  and locally strongly convex at  $\theta^*$ , we have  
 361  $F(\theta^*, 0) = 0$  and  $\partial_\theta F(\theta^*, 0) = H_{\text{distill}} \succ 0$ . By the Implicit Function Theorem there exists a  $C^1$  curve  $\theta(\tau)$  with  $F(\theta(\tau), \tau) = 0$ ,  $\theta(0) = \theta^*$ , and  
 362  $\theta'(0) = -H_{\text{distill}}^{-1} g_{\text{adv}}$  where  $g_{\text{adv}} = \nabla_\theta L_{\text{adv}}(\theta^*; \phi^*)$ . Hence  $\hat{\theta} = \theta(\tau) = \theta^* - \tau H_{\text{distill}}^{-1} g_{\text{adv}} + O(\tau^2)$ .

### B.2 Proof of Proposition 4.2 (variance inflation)

364 Let unbiased mini-batch gradients be  $\hat{g}_{\text{distill}}$  and  $\hat{g}_{\text{adv}}$  with covariances  $\Sigma_{\text{distill}}$  and  $\Sigma_{\text{adv}}$ . For  $\hat{g} = \lambda_{\text{distill}} \hat{g}_{\text{distill}} + \lambda_{\text{adv}} \hat{g}_{\text{adv}}$ ,

$$365 \quad \text{Var}[\hat{g}] = \lambda_{\text{distill}}^2 \Sigma_{\text{distill}} + \lambda_{\text{adv}}^2 \Sigma_{\text{adv}} + \lambda_{\text{distill}} \lambda_{\text{adv}} (\Sigma_{\times} + \Sigma_{\times}^\top).$$

368 Near  $\theta^*$ , continuity implies  $\text{tr Var}[\hat{g}] > \lambda_{\text{distill}}^2 \text{tr } \Sigma_{\text{distill}}$  for any fixed  $\lambda_{\text{adv}} > 0$  as long as  $\Sigma_{\text{adv}}$  is nonzero, proving strict inflation.

### B.3 Proof of Theorem 4.3 (convergence with ALD)

371 Consider SGD

$$372 \quad \theta_{t+1} = \theta_t - \eta_t \left( \nabla L_{\text{distill}}(\theta_t; \phi_t) + \lambda_{\text{adv}}(t) \nabla L_{\text{adv}}(\theta_t; \phi_t) + \xi_t \right),$$

374 with  $\mathbb{E}[\xi_t \mid \mathcal{F}_t] = 0$ ,  $\mathbb{E}[\|\xi_t\|^2 \mid \mathcal{F}_t] \leq C$ ,  $\sum_t \eta_t = \infty$ ,  $\sum_t \eta_t^2 < \infty$ , and bounded iterates. Add and subtract  $\nabla L_{\text{distill}}(\theta_t; \phi^*)$ :

$$376 \quad \begin{aligned} \theta_{t+1} = & \theta_t - \eta_t \left( \nabla L_{\text{distill}}(\theta_t; \phi^*) \right. \\ 377 & + \underbrace{\Delta_t^{(\phi)}}_{\nabla L_{\text{distill}}(\theta_t; \phi_t) - \nabla L_{\text{distill}}(\theta_t; \phi^*)} \\ 378 & + \underbrace{\lambda_{\text{adv}}(t) \nabla L_{\text{adv}}(\theta_t; \phi_t)}_{\Delta_t^{(\text{adv})}} \\ 379 & \left. + \xi_t \right). \end{aligned}$$

386 If  $\phi_t \rightarrow \phi^*$  and gradients are locally Lipschitz, then  $\|\Delta_t^{(\phi)}\| \rightarrow 0$ ; ALD imposes  $\lambda_{\text{adv}}(t) \rightarrow 0$  and  $\sum_t \eta_t \lambda_{\text{adv}}(t) < \infty$ , so  $\sum_t \eta_t \|\Delta_t^{(\text{adv})}\| < \infty$   
 387 (bounded gradients locally). Thus the recursion is a Robbins–Monro scheme for the limiting ODE  $\dot{\theta} = -\nabla L_{\text{distill}}(\theta; \phi^*)$  with a summable  
 388 perturbation and square-summable noise. Standard stochastic approximation results imply almost-sure convergence to the stationary set of  
 389  $L_{\text{distill}}(\cdot; \phi^*)$ ; the bias therefore vanishes and the adversarial variance contribution decays as  $O(\lambda_{\text{adv}}(t)^2)$ .