

Near-Optimal Model Discrimination

arxiv.org/abs/2012.02901

Dmitrii M. Ostrovskii Mohamed Ndaoud
Adel Javanmard Meisam Razaviyayn

University of Southern California

USC Probability and Statistics Seminar
February 5, 2021

- General problem formulation
- Linear models
- Extensions

General problem

Model discrimination task

- Let $z \in \mathcal{Z}$ be a random observation distributed according to \mathbb{P}_0 or \mathbb{P}_1 .
- Let $\theta_0, \theta_1 \in \mathbb{R}^d$ be the **best-fit models** of z according to $\mathbb{P}_0, \mathbb{P}_1$, i.e.

$$\theta_k = \operatorname{argmin}_{\theta \in \mathbb{R}^d} \{ L_k(\theta) := \mathbb{E}_{z \sim \mathbb{P}_k} \ell_z(\theta) \},$$

with strictly convex loss $\ell_z : \mathbb{R}^d \rightarrow \mathbb{R}$ and population risks $L_0(\cdot), L_1(\cdot)$.

- **Statistician** has access to $\theta^* \in \{\theta_0, \theta_1\}$ (but **not** to $\bar{\theta} \in \{\theta_0, \theta_1\} \setminus \theta^*$) knows ℓ_z , and observes **two** i.i.d. samples:

$$Z^0 = (z_1^0, \dots, z_n^0) \sim \mathbb{P}_0^{\otimes n}, \quad Z^1 = (z_1^1, \dots, z_n^1) \sim \mathbb{P}_1^{\otimes n}.$$

- **Task:** distinguish between the two hypotheses

$$\mathcal{H}_0 : \{\theta^* = \theta_0\}, \quad \mathcal{H}_1 : \{\theta^* = \theta_1\}.$$

Model discrimination task

- **Classical setup:** both θ_0, θ_1 known; one sample $Z \sim \mathbb{P}_\theta^{\otimes n}$ observed.

Which $\theta \in \{\theta_0, \theta_1\}$ corresponds to the sample?

*Two **simple** hypotheses about θ .*

- **Our setup:** we observe both samples but only one model $\theta^* \in \{\theta_0, \theta_1\}$.

Which $Z \in \{Z^0, Z^1\}$ corresponds to θ^ ?*

*Two **composite** hypotheses about (θ_0, θ_1) .*

- **Statistician** has access to $\theta^* \in \{\theta_0, \theta_1\}$ (but **not** to $\bar{\theta} \in \{\theta_0, \theta_1\} \setminus \theta^*$) knows ℓ_Z , and observes **two** i.i.d. samples:

$$Z^0 = (z_1^0, \dots, z_n^0) \sim \mathbb{P}_0^{\otimes n}, \quad Z^1 = (z_1^1, \dots, z_n^1) \sim \mathbb{P}_1^{\otimes n}.$$

- **Task:** distinguish between the two hypotheses about $(\theta_0, \theta_1) \in \mathbb{R}^{2d}$:

$$\mathcal{H}_0 : (\theta_0, \theta_1) \in \{\theta^*\} \times \bar{\Theta}_0 \text{ vs. } \mathcal{H}_1 : (\theta_0, \theta_1) \in \bar{\Theta}_1 \times \{\theta^*\} \text{ for some } \bar{\Theta}_0, \bar{\Theta}_1.$$

$\mathcal{H}_0 : (\theta_0, \theta_1) \in (\theta^*, \bar{\Theta}_0)$ vs. $\mathcal{H}_1 : (\theta_0, \theta_1) \in (\bar{\Theta}_1, \theta^*)$ for some $\bar{\Theta}_0, \bar{\Theta}_1$.

What are $\bar{\Theta}_0, \bar{\Theta}_1$?

- \mathbb{R}^d not an option: then \mathcal{H}_0 and \mathcal{H}_1 have the common point (θ^*, θ^*) .
- Thus we have to **separate** $\bar{\Theta}_0, \bar{\Theta}_1$ from θ^* .
- “Prediction-wise” separation:

$$\Delta_0 := L_0(\theta_1) - L_0(\theta_0) > 0, \quad \Delta_1 := L_1(\theta_0) - L_1(\theta_1) > 0.$$

Possible to recast this information in terms of $\bar{\Theta}_0, \bar{\Theta}_1$, but hardly useful.

Main question

Characterize the **sample complexity** of distinguishing between \mathcal{H}_0 and \mathcal{H}_1 with fixed error probabilities of both types (say $2/3$) in terms of $\Delta_0, \Delta_1, \dots$

Well-specified linear models

Well-specified linear regression: $z = (x, y)$, and \mathbb{P}_k , $k \in \{0, 1\}$, is given by

$$\mathbb{P}_k : x \sim \mathcal{N}(0, \Sigma_k), \quad y = x^\top \theta_k + \xi \quad \text{with } \xi \sim \mathcal{N}(0, 1)$$

- Write $Z^k = (X^k; Y^k)$, where $X^k \in \mathbb{R}^{n \times d}$ and $Y^k \in \mathbb{R}^n$ for $k \in \{0, 1\}$.
- Covariances Σ_k and their estimates: $\hat{\Sigma}_k := \frac{1}{n} X^{k\top} X^k$.
- Population and empirical ranks: $r_k = \text{rank}(\Sigma_k)$, and $\hat{r}_k = \text{rank}(\hat{\Sigma}_k)$.
- Separations and their empirical counterparts:

$$\Delta_k = \|\theta_1 - \theta_0\|_{\Sigma_k}^2 = \|\Sigma_k^{1/2}(\theta_1 - \theta_0)\|^2$$

$$\hat{\Delta}_k = \|\theta_1 - \theta_0\|_{\hat{\Sigma}_k}^2 = \frac{1}{n} \|X^k(\theta_1 - \theta_0)\|^2.$$

Basic test based on the prediction error of θ^* under \mathcal{H}_0 and \mathcal{H}_1 :

$$\mathbb{1} \{ \|Y^0 - X^0 \theta^*\|^2 - n \geq \|Y^1 - X^1 \theta^*\|^2 - n \}.$$

Let $\xi^k = Y^k - X^k \theta_k \sim \mathcal{N}(0, I_n)$ be the noises. Under $\mathcal{H}_0 : \theta^* = \theta_0$ one has

$$\text{LHS} = \|\xi^0\|^2 - n,$$

$$\text{RHS} = \|\xi^1\|^2 - n - 2 \langle \xi^1, X_1(\theta_0 - \theta_1) \rangle + \|X_1(\theta_1 - \theta_0)\|^2.$$

- Thus, $\mathbb{E}[\text{LHS}] = 0$ and $\mathbb{E}[\text{RHS}|X_1] = \|X_1(\theta_1 - \theta_0)\|^2 = n\hat{\Delta}_1$, where

$$\hat{\Delta}_1 = \frac{1}{n} \|X_1(\theta_0 - \theta_1)\|^2 = \|\theta_0 - \theta_1\|_{\hat{\Sigma}_1}^2$$

is the empirical counterpart of $\Delta_1 = \|\theta_1 - \theta_0\|_{\Sigma_1}^2$.

- This motivates the basic test: type-I error \iff “fluctuations $\geq n\Delta_1$.”

$$\mathbb{1} \{ \|Y^0 - X^0 \theta^*\|^2 - n \geq \|Y^1 - X^1 \theta^*\|^2 - n \}.$$

More precisely, LHS $\sim \chi_n^2 - n$ and $\text{RHS} | X_1 \sim \chi_n^2 - n + 2\mathcal{N}(0, n\hat{\Delta}_1) + n\hat{\Delta}_1$.

- Recall tail inequalities: $\mathbb{P}[\mathcal{N}(0, 1) \geq t] \leq \exp(-t^2)$ and χ^2 -bound:

$$\mathbb{P}[|\chi_s^2 - s| \geq t] \lesssim \exp(-c \min\{t, t^2/s\}),$$

Bound for the (conditional over X_0, X_1) type-I error:

$$\mathbb{P}_I = \mathbb{P}[\text{fluctuations} \geq n\hat{\Delta}_1]$$

$$\leq \mathbb{P}\left[\chi_n^2 - n \geq \frac{n\hat{\Delta}_1}{3}\right] + \mathbb{P}\left[n - \chi_n^2 \geq \frac{n\hat{\Delta}_1}{3}\right] + \mathbb{P}\left[\mathcal{N}(0, n\hat{\Delta}_1) \geq \frac{n\hat{\Delta}_1}{6}\right]$$

$$\lesssim \exp\left(-\frac{cn^2\hat{\Delta}_1^2}{n}\right) + \exp(-cn\hat{\Delta}_1).$$

- Thus, error prob. of both types at most $\exp(-cn \min\{\Delta, \Delta^2\})$, where

$$\Delta := \min\{\Delta_0, \Delta_1\}.$$

If $\Delta \lesssim 1$: term $\exp(-cn\Delta^2)$ dominates $\Rightarrow O(1/\Delta^2)$ sample complexity.

Idea: decrease χ^2 -term fluctuations by projecting residuals on signal spaces.

Test for linear model

$$\hat{T} = \mathbb{1} \left\{ \|\boldsymbol{\Pi}_{X^0}[Y^0 - X^0\theta^*]\|^2 - \hat{r}_0 \geq \|\boldsymbol{\Pi}_{X^1}[Y^1 - X^1\theta^*]\|^2 - \hat{r}_1 \right\},$$

where $\boldsymbol{\Pi}_X := X(X^\top X)^\dagger X^\top$ is the projector on signal space $\text{col}(X) \subseteq \mathbb{R}^n$.

- Recall that $\hat{r}_k := \text{rank}(\hat{\boldsymbol{\Sigma}}_k)$ and $\hat{\boldsymbol{\Sigma}} = \frac{1}{n}X^\top X$, hence indeed

$$\dim(\text{col}(X)) = \text{Tr}(\boldsymbol{\Pi}_X) = \text{Tr}[(X^\top X)^\dagger X^\top X] = \text{rank}(X^\top X) = \text{rank}(\hat{\boldsymbol{\Sigma}}).$$

Test for linear model

$$\hat{T} = \mathbb{1} \left\{ \|\Pi_{X^0}[Y^0 - X^0\theta^*]\|^2 - \hat{r}_0 \geq \|\Pi_{X^1}[Y^1 - X^1\theta^*]\|^2 - \hat{r}_1 \right\},$$

where $\Pi_X := X(X^\top X)^\dagger X^\top$ is the projector on signal space $\text{col}(X) \subseteq \mathbb{R}^n$.

- For this test, under \mathcal{H}_0 , we have

$$\text{LHS}|X_0 \sim \chi_{\hat{r}_0}^2 - \hat{r}_0, \quad \text{RHS}|X_1 \sim \chi_{\hat{r}_1}^2 - \hat{r}_1 + 2\mathcal{N}(0, n\hat{\Delta}_1) + n\hat{\Delta}_1.$$

- Smaller χ^2 fluctuations since $\hat{r}_k \stackrel{\text{a.s.}}{\leq} \min\{r_k, n\} \leq n$. Type-I error prob.:

$$\begin{aligned} & \mathbb{P} \left[\chi_{\hat{r}_0}^2 - \hat{r}_0 \geq \frac{n\hat{\Delta}_1}{3} \right] + \mathbb{P} \left[\hat{r}_1 - \chi_{\hat{r}_1}^2 \geq \frac{n\hat{\Delta}_1}{3} \right] + \mathbb{P} \left[\mathcal{N}(0, n\hat{\Delta}_1) \geq \frac{n\hat{\Delta}_1}{6} \right] \\ & \lesssim \exp \left(-\frac{cn^2\hat{\Delta}_1^2}{\hat{r}_0} \right) + \exp \left(-\frac{cn^2\hat{\Delta}_1^2}{\hat{r}_1} \right) + \exp(-cn\hat{\Delta}_1). \end{aligned}$$

Theorem. Denoting $r_{\max} := \max\{r_0, r_1\}$, we have

$$\max\{P_I, P_{II}\} \lesssim \exp \left(-c \min \left\{ n\Delta, \frac{n^2\Delta^2}{\min\{n, r_{\max}\}} \right\} \right).$$

Error probability bound

Theorem. Denoting $r_{\max} := \max\{r_0, r_1\}$, we have

$$\max\{P_I, P_{II}\} = \exp\left(-c \min\left\{n\Delta, \frac{n^2\Delta^2}{\min\{n, r_{\max}\}}\right\}\right).$$

Sample complexity bound

Lemma Assume $\Delta \lesssim 1$. Then $-\log(\max\{P_I, P_{II}\}) \gtrsim 1$ is equivalent to

$$n \gtrsim \min\left\{\frac{1}{\Delta^2}, \frac{\sqrt{r_{\max}}}{\Delta}\right\}.$$

Basic test: $\mathbb{1} \{ \|Y^0 - X^0 \theta^*\|^2 - n \geq \|Y^1 - X^1 \theta^*\|^2 - n \}.$

$$n = O\left(\frac{1}{\Delta^2}\right).$$

Improved test: $\mathbb{1} \{ \|\Pi_{X^0}[Y^0 - X^0 \theta^*]\|^2 - \hat{r}_0 \geq \|\Pi_{X^1}[Y^1 - X^1 \theta^*]\|^2 - \hat{r}_1 \}.$

$$n = O\left(\min\left\{\frac{1}{\Delta^2}, \frac{\sqrt{r_{\max}}}{\Delta}\right\}\right).$$

Note: $\hat{r}_k \stackrel{\text{a.s.}}{=} \min\{r_k, n\}$ and Π_{X^k} projects on $\text{col}(X^k) \subset \mathbb{R}^n$ of dimension \hat{r}_k .
Thus, the two tests coincide when $n \leq \min\{r_0, r_1\}$,

- **Well-sep. regime:** $\Delta \gtrsim \frac{1}{\sqrt{r_{\max}}}$. Sample complexity $\lesssim r_{\max}$ and rank-independent. No need for projections if $r_0 \asymp r_1$.
- **Ill-sep. regime:** $\Delta \ll \frac{1}{\sqrt{r_{\max}}}$, sample complexity $\gg r_{\max}$, projections.

Improved test: $\mathbb{1}\{n\|\theta^* - \hat{\theta}_0\|_{\hat{\Sigma}_0}^2 - \hat{r}_0 \geq n\|\theta^* - \hat{\theta}_1\|_{\hat{\Sigma}_1}^2 - \hat{r}_1\}.$

Sample complexity: $O\left(\min\left\{\frac{1}{\Delta^2}, \frac{\sqrt{r_{\max}}}{\Delta}\right\}\right)$

Improved test: $\mathbb{1}\{n\|\theta^* - \hat{\theta}_0\|_{\hat{\Sigma}_0}^2 - \hat{r}_0 \geq n\|\theta^* - \hat{\theta}_1\|_{\hat{\Sigma}_1}^2 - \hat{r}_1\}.$

Sample complexity: $O\left(\min\left\{\frac{1}{\Delta^2}, \frac{\sqrt{r_{\max}}}{\Delta}\right\}\right) \ll \frac{r_{\max}}{\Delta}.$

- Sample complexity of **estimating** $\bar{\theta} = \theta_0 + \theta_1 - \theta^*$ up to Δ prediction error (i.e., better than by θ^*) is at least $\frac{r_{\min}}{\Delta} \left[\approx \frac{r_{\max}}{\Delta} \text{ when } r_0 \asymp r_1 \right].$

Non-disclosure

*We can **discriminate** between \mathcal{H}_0 and \mathcal{H}_1 with sample size that does not allow to **estimate** the complementary model $\bar{\theta}$ (with better quality than θ^*).*

- Rich potential for applications in “privacy-aware ML” (see our paper).

Interpretation via least-squares

Recall the normal equations for the least-squares estimates $\hat{\theta}_0, \hat{\theta}_1$ of θ_0, θ_1 :

$$\hat{\Sigma}_0 \hat{\theta}_0 = \frac{1}{n} X^{0\top} Y^0, \quad \hat{\Sigma}_1 \hat{\theta}_1 = \frac{1}{n} X^{1\top} Y^1.$$

This allows to rewrite the squared norms of the projected residuals:

$$\begin{aligned} \|\Pi_X[Y - X\theta^*]\|^2 &= (Y - X\theta^*)^\top \Pi_X (Y - X\theta^*) \\ &= (X^\top Y - X^\top X\theta^*)^\top (X^\top X)^\dagger (X^\top Y - X^\top X\theta^*) \\ &= n^2 (\hat{\Sigma}(\hat{\theta} - \theta^*))^\top (X^\top X)^\dagger \hat{\Sigma}(\hat{\theta} - \theta^*) \\ &= n(\hat{\theta} - \theta^*)^\top \hat{\Sigma} \hat{\Sigma}^\dagger \hat{\Sigma}(\hat{\theta} - \theta^*) = n(\hat{\theta} - \theta^*)^\top \hat{\Sigma}(\hat{\theta} - \theta^*) \\ &= n \|\hat{\theta} - \theta^*\|_{\hat{\Sigma}}^2. \end{aligned}$$

Thus, our test amounts to $\mathbb{1}\left\{\|\theta^* - \hat{\theta}_0\|_{\hat{\Sigma}_0}^2 - \frac{\hat{r}_0}{n} \geq \|\theta^* - \hat{\theta}_1\|_{\hat{\Sigma}_1}^2 - \frac{\hat{r}_1}{n}\right\}$.

- We compare the empirical prediction distances from $\hat{\theta}^*$ to $\hat{\theta}_0$ and $\hat{\theta}_1$ *after debiasing them under the matching hypothesis*.
- **NB:** we don't require $\hat{\theta}_0, \hat{\theta}_1$ to be unique (i.e. $n \geq r_{\max}$).

Lower bound: key ideas

We need to prove two bounds:

$$\inf_{\hat{T}} \sup_{\|\theta_1 - \theta_0\|_{\Sigma}^2 \geq \Delta} P_I(\hat{T}) + P_{II}(\hat{T}) \gtrsim \max \left\{ \exp(-cn\Delta), \exp\left(-c \frac{n^2 \Delta^2}{\min\{n, r\}}\right) \right\}.$$

- **First bound**: easier problem with **known** $\bar{\theta}$ and **simple hypotheses**:

$$\mathcal{H}_0^o : (\theta_0, \theta_1) = (\theta^*, \bar{\theta}), \quad \text{vs.} \quad \mathcal{H}_1^o : (\theta_0, \theta_1) = (\bar{\theta}, \theta^*).$$

- Likelihood-ratio (LR) test

$$T_{\text{LR}} = \mathbb{1}\{\|Y^0 - X^0 \theta^*\|^2 + \|Y^1 - X^1 \bar{\theta}\|^2 \geq \|Y^0 - X^0 \bar{\theta}\|^2 + \|Y^1 - X^1 \theta^*\|^2\}$$

is optimal (w.r.t. sum of errors) by the Neyman-Pearson lemma.

- **Second bound** captures dependence on the rank. Bayesian approach:
 - Put Gaussian prior on $\bar{\theta}$, lower-bound $\max\{\mathbb{P}_I, \mathbb{P}_{II}\}$ for the Bayes test.
 - Lower-bounding is technical and requires that $\hat{\Sigma}_0, \hat{\Sigma}_1$ commute.
 - We achieve this by sampling x and \tilde{x} from $\sqrt{r}\{\pm e_1, \dots, \pm e_r\}$.

In our paper:

- General result for parametric models in asymptotic regime $n \rightarrow \infty$ with fixed r_0, r_1 and $n\Delta \rightarrow \lambda$.
- Technical result for generalized linear models (GLMs) allowing for heavy tails and misspecification.
- **Same general picture:**

$$\max\{P_I, P_{II}\} = \exp\left(-c \min\left\{n\Delta, \frac{n^2\Delta^2}{\max\{\rho_0, \rho_1\}}\right\}\right)$$

where ρ_0, ρ_1 are “effective model ranks”.

Open questions:

- General nonasymptotic result;
- Full optimality;
- Adaptation.

Thank you!

And check our paper:

arxiv.org/abs/2012.02901

General asymptotics

General setup: Newton decrement test

Linear model: $\mathbb{1} \{ \|\boldsymbol{\Pi}_{X^0}[Y^0 - X^0\theta^*]\|^2 - \hat{r}_0 \geq \|\boldsymbol{\Pi}_{X^1}[Y^1 - X^1\theta^*]\|^2 - \hat{r}_1 \}.$

General setup:

- Empirical risk $\hat{L}_k(\theta) = \frac{1}{n} \sum_{i=1}^n \ell_{z_i^k}(\theta)$ has gradient $\nabla \hat{L}_k(\theta)$ and Hessian $\hat{\mathbf{H}}_k(\theta)$:

$$\hat{\mathbf{H}}_k(\theta) := \nabla^2 \hat{L}_k(\theta), \quad \mathbf{H}_k(\theta) := \nabla^2 L_k(\theta).$$

- Let $\mathbf{G}_k(\theta) := \text{Cov}_{\mathbb{P}_k}[\nabla \ell_z(\theta)]$. **For well-specified models:**

$$\mathbf{G}_k(\theta_k) = \mathbf{H}_k(\theta_k).$$

- Standardized Fisher matrix: $\mathbf{J}_k(\theta) := \mathbf{H}_k(\theta)^{-\dagger/2} \mathbf{G}_k(\theta) \mathbf{H}_k(\theta)^{-\dagger/2}.$
- Effective rank $\rho_k := \text{Tr}[\mathbf{J}_k(\theta_k)]$. **For well-specified models:** $\rho_k = r_k.$

In linear regression $\nabla \hat{L}(\theta) = \frac{1}{n} X^\top (Y - X\theta)$ and $\nabla^2 \hat{L}(\theta) \equiv \frac{1}{n} X^\top X$, hence

$$\|\boldsymbol{\Pi}_X[Y - X\theta^*]\|^2 = \|(X^\top X)^{\dagger/2} X^\top (Y - X\theta^*)\|^2 = n \|\hat{\mathbf{H}}(\theta^*)^{\dagger/2} \nabla \hat{L}(\theta^*)\|^2.$$

General setup: Newton decrement test (cont'd)

$$\mathbb{1} \{ \|\mathbf{\Pi}_{X^0}[Y^0 - X^0\theta^*]\|^2 - \hat{r}_0 \geq \|\mathbf{\Pi}_{X^1}[Y^1 - X^1\theta^*]\|^2 - \hat{r}_1 \}.$$

- Replace $\|\mathbf{\Pi}_{X^k}[Y^k - X^k\theta^*]\|^2$ with $n\|\hat{\mathbf{H}}_k(\theta_k)^{\dagger/2}\nabla\hat{L}_k(\theta^*)\|^2$.
- When $n \rightarrow \infty$,

$$\mathbb{E}_k[n\|\hat{\mathbf{H}}_k(\theta_k)^{\dagger/2}\nabla\hat{L}_k(\theta_k)\|^2] \rightarrow \rho_k = \text{Tr}[\mathbf{J}_k(\theta_k)].$$

- Cannot use ρ_k 's as one of them uses $\bar{\theta}$ which is unknown. Instead use

$$\text{Tr}[\mathbf{J}_k(\theta^*)] = n_k \mathbb{E}_k [\|\mathbf{H}_k(\theta^*)^{\dagger/2}[\nabla\hat{L}_k(\theta^*) - \nabla L_k(\theta^*)]\|^2],$$

or, more precisely, its asymptotically (as $n \rightarrow \infty$) unbiased estimate:

$$\hat{\mathbf{T}}_k = \frac{1}{2}n_k\|\mathbf{H}_k(\theta^*)^{\dagger/2}[\nabla\hat{L}_k(\theta^*) - \hat{\nabla}L'_k(\theta^*)]\|^2.$$

$$\hat{\mathbf{T}} = \mathbb{1} \{ n_0\|\hat{\mathbf{H}}_0(\theta^*)^{\dagger/2}\nabla\hat{L}_0(\theta^*)\|^2 - \hat{\mathbf{T}}_0 \geq n_1\|\hat{\mathbf{H}}_1(\theta^*)^{\dagger/2}\nabla\hat{L}_1(\theta^*)\|^2 - \hat{\mathbf{T}}_1 \}.$$

Theorem. Denoting $\rho_{\max} := \max\{\rho_0, \rho_1\}$, we have that

$$\lim_{n \rightarrow \infty} [\max\{P_I, P_{II}\}] \lesssim \exp \left(-c \min \left\{ n\Delta, \frac{n^2\Delta^2}{\rho_{\max}} \right\} \right).$$