Tutorial Part I: Information theory meets machine learning

Emmanuel Abbe UC Berkeley Martin Wainwright Princeton University

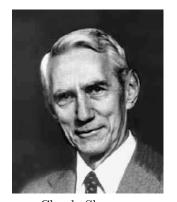
Introduction

Era of massive data sets

Fascinating problems at the interfaces between information theory and statistical machine learning.

- Fundamental issues
 - ► Concentration of measure: high-dimensional problems are remarkably predictable
 - ► Curse of dimensionality: without structure, many problems are hopeless
 - ▶ Low-dimensional structure is essential
- Machine learning brings in algorithmic components
 - ► Computational constraints are central
 - Memory constraints: need for distributed and decentralized procedures
 - ► Increasing importance of privacy

Historical perspective: info. theory and statistics



Claude Shannon



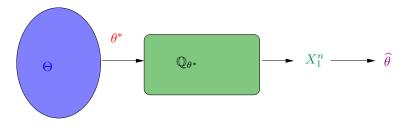
Andrey Kolmogorov

A rich intersection between information theory and statistics

- Hypothesis testing, large deviations
- 2 Fisher information, Kullback-Leibler divergence
- 3 Metric entropy and Fano's inequality

Statistical estimation as channel coding

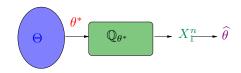
- Codebook: indexed family of probability distributions $\{\mathbb{Q}_{\theta} \mid \theta \in \Theta\}$
- Codeword: nature chooses some $\theta^* \in \Theta$



- Channel: user observes n i.i.d. draws $X_i \sim \mathbb{Q}_{\theta^*}$
- Decoding: estimator $X_1^n \mapsto \widehat{\theta}$ such that $\widehat{\theta} \approx \theta^*$

Statistical estimation as channel coding

- Codebook: indexed family of probability distributions $\{\mathbb{Q}_{\theta} \mid \theta \in \Theta\}$
- Codeword: nature chooses some $\theta^* \in \Theta$



- Channel: user observes n i.i.d. draws $X_i \sim \mathbb{Q}_{\theta^*}$
- Decoding: estimator $X_1^n \mapsto \widehat{\theta}$ such that $\widehat{\theta} \approx \theta^*$

Perspective dating back to Kolmogorov (1950s) with many variations:

- codebooks/codewords: graphs, vectors, matrices, functions, densities....
- channels: random graphs, regression models, elementwise probes of vectors/machines, random projections
- closeness $\widehat{\theta} \approx \theta^*$: exact/partial graph recovery in Hamming, ℓ_p -distances, $L^{(\mathbb{Q})}$ -distances, sup-norm etc.

Machine learning: algorithmic issues to forefront!

- Efficient algorithms are essential
 - ▶ only (low-order) polynomial-time methods can ever be implemented
 - ▶ trade-offs between computational complexity and performance?
 - fundamental barriers due to computational complexity?
- 2 Distributed procedures are often needed
 - ▶ many modern data sets: too large to stored on a single machine
 - ▶ need methods that operate separately on pieces of data
 - ▶ trade-offs between decentralization and performance?
 - ▶ fundamental barriers due to communication complexity?
- 3 Privacy and access issues
 - conflicts between individual privacy and benefits of aggregation?
 - principled information-theoretic formulations of such trade-offs?

Part I of tutorial: Three vignettes

- Graphical model selection
- 2 Sparse principal component analysis
- Structured non-parametric regression and minimax theory

Vignette A: Graphical model selection

Simple motivating example: Epidemic modeling

Disease status of person s:
$$x_s = \begin{cases} +1 & \text{if individual } s \text{ is infected} \\ -1 & \text{if individual } s \text{ is healthy} \end{cases}$$

$$\mathbb{Q}(x_1,\ldots,x_5) \propto \prod_{s=1}^5 \exp(\theta_s x_s)$$

$$\mathbb{Q}(x_1, \dots, x_5) \propto \prod_{s=1}^5 \exp(\theta_s x_s) \prod_{(s,t) \in C} \exp(\theta_{st} x_s x_t)$$

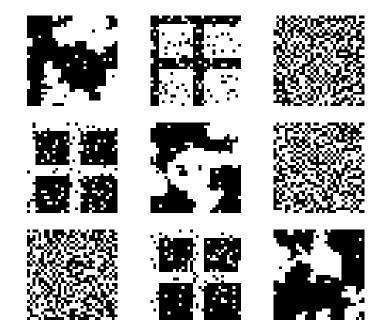
$$\mathbb{Q}(x_1, \dots, x_5) \propto \prod_{s=1}^{5} \exp(\theta_s x_s) \prod_{s \neq t} \exp(\theta_{st} x_s x_t)$$



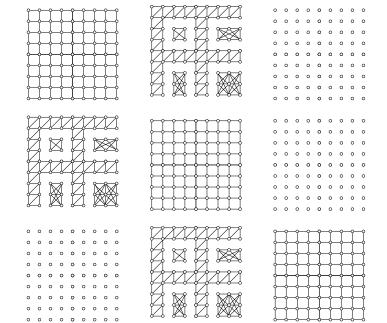
Possible epidemic patterns (on a square)



From epidemic patterns to graphs



Underlying graphs



Model selection for graphs

 \bullet drawn n i.i.d. samples from

$$\mathbb{Q}(x_1, \dots, x_p; \Theta) \propto \exp \left\{ \sum_{s \in V} \theta_s x_s + \sum_{(s,t) \in E} \theta_{st} x_s x_t \right\}$$

- graph G and matrix $[\Theta]_{st} = \theta_{st}$ of edge weights are unknown
- data matrix $\mathbf{X}_1^n \in \{-1, +1\}^{n \times p}$
- \bullet want estimator $\mathbf{X}_1^n \mapsto \widehat{G}$ to minimize error probability

$$\mathbb{Q}^n \left[\widehat{G}(\mathbf{X}_1^n) \neq G \right]$$

Prob. that estimated graph differs from truth

Channel decoding:

Think of graphs as codewords, and the graph family as a codebook.

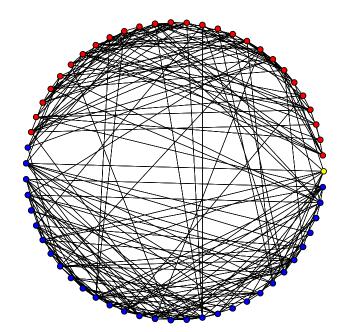
Past/on-going work on graph selection

- exact polynomial-time solution on trees (Chow & Liu, 1967)
- testing for local conditional independence relationships (e.g., Spirtes et al, 2000; Kalisch & Buhlmann, 2008)
- pseudolikelihood and BIC criterion

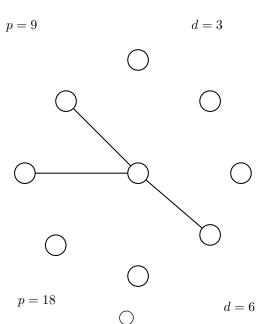
(Csiszar & Talata, 2006)

- pseudolikelihood and ℓ_1 -regularized neighborhood regression
 - ► Gaussian case (Meinshausen & Buhlmann, 2006)
 - ▶ Binary case (Ravikumar, W. & Lafferty et al., 2006)
- various greedy and related methods: (Bresler et al., 2008; Bresler, 2015; Netrapalli et al., 2010; Anandkumar et al., 2013)
- lower bounds and inachievability results
 - ▶ information-theoretic bounds (Santhanam & W., 2012)
 - ▶ computational lower bounds (Dagum & Luby, 1993; Bresler et al., 2014)
 - phase transitions and performance of neighborhood regression (Bento & Montanari, 2009)

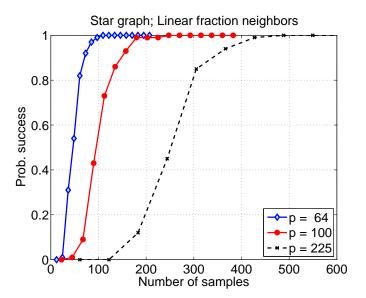
US Senate network (2004–2006 voting)



Experiments for sequences of star graphs

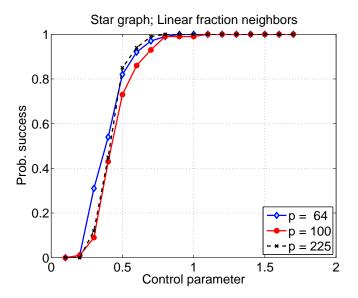


Empirical behavior: Unrescaled plots



Plots of success probability versus raw sample size n.

Empirical behavior: Appropriately rescaled



Plots of success probability versus rescaled sample size $\frac{n}{d^2 \log p}$

Some theory: Scaling law for graph selection

- graphs $G_{p,d}$ with p nodes and maximum degree d
- minimum absolute weight θ_{\min} on edges
- \bullet how many samples n needed to recover the unknown graph?

Theorem (Ravikumar, W. & Lafferty, 2010; Santhanam & W., 2012)

Achievable result: Under regularity conditions, for a graph estimate \widehat{G} produced by ℓ_1 -regularized logistic regression:

$$\underbrace{n > c_u \left(d^2 + 1/\theta_{\min}^2\right) \log p}_{Lower\ bound\ on\ sample\ size} \implies \underbrace{\mathbb{Q}[\widehat{G} \neq G] \to 0}_{Vanishing\ probability\ of\ error}$$

Necessary condition: For graph estimate \widetilde{G} produced by any algorithm.

$$\underbrace{n < c_{\ell} \left(d^2 + 1/\theta_{\min}^2 \right) \log p}_{Upper \ bound \ on \ sample \ size} \implies \underbrace{\mathbb{Q}[\widetilde{G} \neq G] \geq 1/2}_{Constant \ probability \ of \ error}$$

Information-theoretic analysis of graph selection

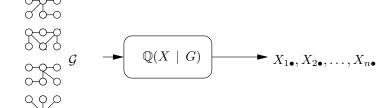
Question:

How to prove lower bounds on graph selection methods?

Answer:

Graph selection is an *unorthodox* channel coding problem.

- \bullet codewords/codebook: graph G in some graph class \mathcal{G}
- channel use: draw sample $X_{i\bullet} = (X_{i1}, \dots, X_{ip}) \in \{-1, +1\}^p$ from the graph-structured distribution \mathbb{Q}_G
- decoding problem: use n samples $\{X_{1\bullet}, \ldots, X_{n\bullet}\}$ to correctly distinguish the "codeword"



Proof sketch: Main ideas for necessary conditions

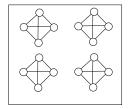
- based on assessing difficulty of graph selection over various sub-ensembles $\mathcal{G}\subseteq\mathcal{G}_{p,d}$
- choose $G \in \mathcal{G}$ u.a.r., and consider multi-way hypothesis testing problem based on the data $\mathbf{X}_1^n = \{X_{1\bullet}, \dots, X_{n\bullet}\}$
- for any graph estimator $\psi: \mathcal{X}^n \to \mathcal{G}$, Fano's inequality implies that

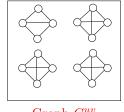
$$\mathbb{Q}[\psi(\mathbf{X}_1^n) \neq G] \ge 1 - \frac{I(\mathbf{X}_1^n; G)}{\log |\mathcal{G}|} - o(1)$$

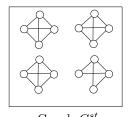
where $I(\mathbf{X}_1^n;G)$ is mutual information between observations \mathbf{X}_1^n and randomly chosen graph G

- remaining steps:
 - **①** Construct "difficult" sub-ensembles $\mathcal{G} \subseteq \mathcal{G}_{p,d}$
 - 2 Compute or lower bound the log cardinality $\log |\mathcal{G}|$.
 - **3** Upper bound the mutual information $I(\mathbf{X}_1^n; G)$.

A "hard" *d*-clique ensemble







Base graph \bar{G}

Graph G^{uv}

Graph G^{st}

- ① Divide the vertex set V into $\lfloor \frac{p}{d+1} \rfloor$ groups of size d+1, and form the base graph \overline{G} by making a (d+1)-clique \mathcal{C} within each group.
- **2** Form graph G^{uv} by deleting edge (u, v) from \overline{G} .
- **3** Consider testing problem over family of graph-structured distributions $\{\mathbb{Q}(\cdot; G^{st}), (s,t) \in \mathcal{C}\}.$

Why is this ensemble "hard"?

Kullback-Leibler divergence between pairs decays exponentially in d, unless minimum edge weight decays as 1/d.

Vignette B: Sparse principal components analysis

Principal component analysis:

- \bullet widely-used method for {dimensionality reduction, data compression etc.}
- \bullet extracts top eigenvectors of sample covariance matrix $\widehat{\Sigma}$
- classical PCA in p dimensions: inconsistent unless $p/n \to 0$
- low-dimensional structure: many applications lead to sparse eigenvectors

Population model: Rank-one spiked covariance matrix

$$\Sigma = \underbrace{\nu}_{\text{SNR parameter rank-one spike}} + I_p$$

Sampling model: Draw n i.i.d. zero-mean vectors with $cov(X_i) = \Sigma$, and form sample covariance matrix

$$\widehat{\Sigma} := \underbrace{\frac{1}{n} \sum_{i=1}^n X_i X_i^T}_{p\text{-dim. matrix, rank min}\{n,p\}}$$

Example: PCA for face compression/recognition



First 25 standard principal components (estimated from data)

Example: PCA for face compression/recognition

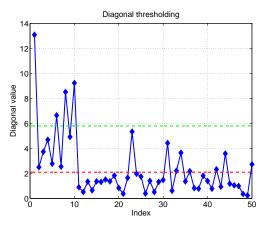


First 25 sparse principal components (estimated from data)

Perhaps the simplest estimator....

Diagonal thresholding:

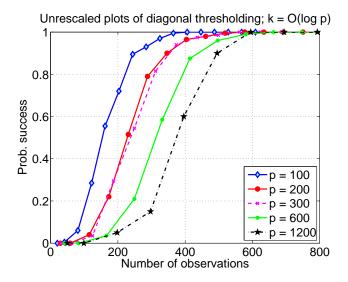
(Johnstone & Lu, 2008)



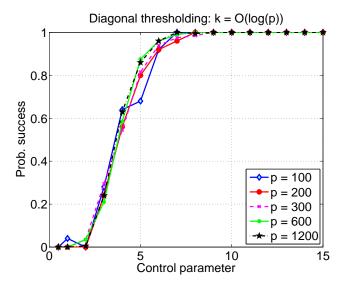
Given n i.i.d. samples X_i with zero mean, and with spiked covariance $\Sigma = \nu \theta^* (\theta^*)^T + I$:

- **①** Compute diagonal entries of sample covariance: $\widehat{\Sigma}_{jj} = \frac{1}{n} \sum_{i=1}^{n} X_{ij}^2$.
- **2** Apply threshold to vector $\{\widehat{\Sigma}_{jj}, j = 1, \dots, p\}$

Diagonal thresholding: unrescaled plots



Diagonal thresholding: rescaled plots



Scaling is quadratic in sparsity: $\frac{n}{k^2 \log p}$

Diagonal thresholding and fundamental limit

Consider spiked covariance matrix

$$\Sigma = \underbrace{\nu}_{\text{Signal-to-noise}} \underbrace{\theta^*(\theta^*)^T}_{\text{rank one spike}} + I_{p \times p} \quad \text{where} \quad \underbrace{\theta \in \mathbb{B}_0(k) \cap \mathbb{B}_2(1)}_{k\text{-sparse and unit norm}}$$

Theorem (Amini & W., 2009)

(a) There are thresholds $\tau_{\ell}^{DT} \leq \tau_{u}^{DT}$ such that

$$\frac{n}{k^2 \log p} \le \tau_\ell^{DT} \qquad \qquad \underbrace{\frac{n}{k^2 \log p}} \ge \tau_u^{DT}$$

$$DT \text{ fails w.h.p.} \qquad \qquad DT \text{ succeeds w.h.p.}$$

(b) For optimal method (exhaustive search):

$$\underbrace{\frac{n}{k \log p} < au^{ES}}_{ extbf{Fail w.h.p.}} \qquad \underbrace{\frac{n}{k \log p} > au^{ES}}_{ ext{Succeed w.h.p.}}.$$

One polynomial-time SDP relaxation

Recall Courant-Fisher variational formulation:

$$\theta^* = \arg \max_{\|z\|_2 = 1} \Big\{ z^T \underbrace{\left(\nu \theta^*(\theta^*)^T + I_{p \times p}\right)}_{\text{Population covariance } \Sigma} z \Big\}.$$

Equivalently, lifting to matrix variables $Z = zz^T$:

$$\theta\theta^T = \arg\max_{\substack{Z \in \mathbb{R}^{P^{\times_P}} \\ Z = Z^T, \quad Z \succeq 0}} \left\{ \operatorname{trace}(Z^T \Sigma) \right\} \quad \text{s.t. } \operatorname{trace}(Z) = 1, \text{ and } \operatorname{rank}(Z) = 1$$

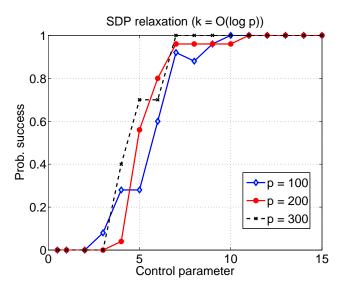
Dropping rank constraint yields a standard SDP relaxation:

$$\widehat{Z}^T = \arg \max_{\substack{Z \in \mathbb{R}^{p \times p} \\ Z = Z^T, \quad Z \succeq 0}} \left\{ \operatorname{trace}(Z^T \Sigma) \right\} \quad \text{s.t. } \operatorname{trace}(Z) = 1.$$

In practice: (d'Aspremont et al., 2008)

- apply this relaxation using the sample covariance matrix $\hat{\Sigma}$
- add the ℓ_1 -constraint $\sum_{i,j=1}^p |Z_{ij}| \leq k^2$.

Phase transition for SDP: logarithmic sparsity



Scaling is linear in sparsity: $\frac{n}{k \log p}$

A natural question

Questions:

Can logarithmic sparsity or rank one condition be removed?

Computational lower bound for sparse PCA

Consider spiked covariance matrix

$$\Sigma = \underbrace{\nu}_{\text{signal-to-noise}} \qquad \underbrace{(\theta^*)(\theta^*)^T}_{\text{rank one spike}} + I_{p \times p} \qquad \text{where} \qquad \underbrace{\theta^* \in \mathbb{B}_0(k) \cap \mathbb{B}_2(1)}_{k\text{-sparse and unit norm}}$$

Sparse PCA detection problem:
$$\begin{array}{ll} \mathbf{H}_0 & \text{(no signal):} & X_i \sim \mathcal{D}(0, I_{p \times p}) \\ \mathbf{H}_1 & \text{(spiked signal):} & X_i \sim \mathcal{D}(0, \Sigma). \end{array}$$

Distribution \mathcal{D} with sub-exponential tail behavior.

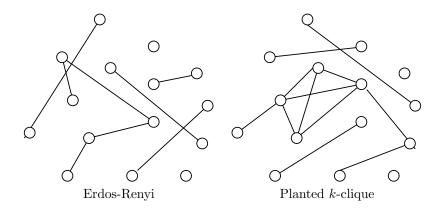
Theorem (Berthet & Rigollet, 2013)

Under average-case hardness of planted clique, polynomial-minimax level of detection ν_{POLY} is given by

$$u_{\scriptscriptstyle POLY} \asymp \frac{k^2 \log p}{n} \qquad \text{for all sparsity } \log p \ll k \ll \sqrt{p}$$

Classical minimax level $\nu_{\scriptscriptstyle OPT} \asymp rac{k \log p}{n}$.

Planted *k*-clique problem

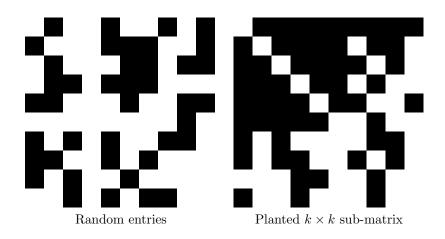


Binary hypothesis test based on observing random graph G on p-vertices:

 H_0 Erdos-Renyi, each edge randomly with prob. 1/2

 H_1 Planted k-clique, remaining edges random

Planted *k*-clique problem



Binary hypothesis test based on observing random binary matrix:

 H_0 Random $\{0,1\}$ matrix with Ber(1/2) on off-diagonal

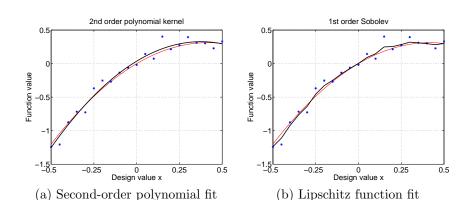
 H_1 Planted $k \times k$ sub-matrix

Vignette C: (Structured) non-parametric regression

Goal: How to predict output from covariates?

- given covariates $(x_1, x_2, x_3, \dots, x_p)$
- output variable y
- want to predict y based on (x_1, \ldots, x_p)

Examples: Medical Imaging; Geostatistics; Astronomy; Computational Biology



High dimensions and sample complexity

Possible models:

• ordinary linear regression:
$$y = \sum_{j=1}^{r} \theta_{j}^{*} x_{j} + w$$

• general non-parametric model: $y = f^*(x_1, x_2, \dots, x_p) + w$.

Estimation accuracy: How well can f^* be estimated using n samples?

- linear models
 - without any structure: error $\delta^2 \simeq p/n$

• with sparsity $k \ll p$: error $\delta^2 \asymp \underbrace{\left(k \log \frac{ep}{k}\right)/n}$

logarithmic in p

• non-parametric models: p-dimensional, smoothness α

Curse of dimensionality: Error $\delta^2 \simeq (1/n)^{\frac{2\alpha}{2\alpha+p}}$

Exponential slow-down

Minimax risk and sample size

Consider a function class \mathcal{F} , and n i.i.d. samples from the model

$$y_i = f^*(x_i) + w_i$$
, where f^* is some member of \mathcal{F} .

For a given estimator $\{(x_i, y_i)\}_{i=1}^n \mapsto \widehat{f} \in \mathcal{F}$, worst-case risk in a metric ρ :

$$R_{\text{worst}}^n(\widehat{f}; \mathcal{F}) = \sup_{f^* \in \mathcal{F}} \mathbb{E}^n[\rho^2(\widehat{f}, f^*)].$$

Minimax risk

For a given sample size n, the minimax risk

$$\inf_{\widehat{f}} R^n_{\text{worst}}(\widehat{f}; \mathcal{F}) \ = \ \inf_{\widehat{f}} \ \sup_{f^* \in \mathcal{F}} \mathbb{E}^n \big[\rho^2(\widehat{f}, f^*) \big]$$

where the infimum is taken over all estimators.

How to measure "size" of function classes?



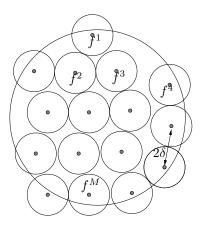
• A 2δ -packing of \mathcal{F} in metric ρ is a collection $\{f^1, \ldots, f^M\} \subset \mathcal{F}$ such that

$$\rho(f^j, f^k) > 2\delta$$
 for all $j \neq k$.

• The packing number $M(2\delta)$ is the cardinality of the largest such set.

- Packing/covering entropy: emerged from Russian school in 1940s/1950s (Kolmogorov and collaborators)
- Central object in proving minimax lower bounds for nonparametric problems (e.g., Hasminskii & Ibragimov, 1978; Birge, 1983; Yu, 1997; Yang & Barron, 1999)

Packing and covering numbers

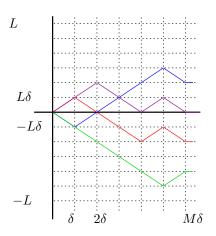


• A 2δ -packing of $\mathcal F$ in metric ρ is a collection $\{f^1,\ldots,f^M\}\subset\mathcal F$ such that

$$\rho(f^j, f^k) > 2\delta$$
 for all $j \neq k$.

• The packing number $M(2\delta)$ is the cardinality of the largest such set.

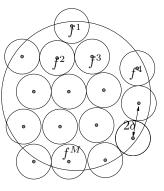
Example: Sup-norm packing for Lipschitz functions



- δ -packing set: functions $\{f^1, f^2, \dots, f^M\}$ such that $\|f^j f^k\|_2 > \delta$ for all $j \neq k$
- for L-Lipschitz functions in 1-dimension:

$$M(\delta) \approx 2^{(L/\delta)}$$
.

Standard reduction: from estimation to testing



- goal: to characterize the minimax risk for ρ -estimation over \mathcal{F}
- construct a 2δ -packing of \mathcal{F} :

collection $\{f^1,\dots,f^M\}$ such that $\rho(f^j,f^k)>2\delta$

- now form a *M*-component mixture distribution as follows:
 - draw packing index $V \in \{1, ... M\}$ uniformly at random
 - ▶ conditioned on V = j, draw n i.i.d. samples $(X_i, Y_i) \sim \mathbb{Q}_{f^j}$
- Claim: Any estimator \hat{f} such that $\rho(\hat{f}, f^J) \leq \delta$ w.h.p. can be used to solve the M-ary testing problem.
- ② Use standard techniques ({Assouad, Le Cam, Fano }) to lower bound the probability of error in the testing problem.

Minimax rate via metric entropy matching

- observe (x_i, y_i) pairs from model $y_i = f^*(x_i) + w_i$
- two possible norms

$$\|\widehat{f} - f^*\|_n^2 := \frac{1}{n} \sum_{i=1}^n (\widehat{f}(x_i) - f^*(x_i))^2$$
, or $\|\widehat{f} - f^*\|_2^2 = \mathbb{E}[(\widehat{f}(\widetilde{X}) - f^*(\widetilde{X}))^2]$.

Metric entropy master equation

For many regression problems, minimax rate $\delta_n > 0$ determined by solving the master equation

$$\log M(2\delta; \mathcal{F}, ||\cdot||) \approx n\delta^2.$$

- basic idea (with Hellinger metric) dates back to Le Cam (1973)
- elegant general version due to Yang and Barron (1999)

Example 1: Sparse linear regression

Observations $y_i = \langle x_i, \theta^* \rangle + w_i$, where

$$\theta^* \in \Theta(k,p) := \Big\{ \theta \in \mathbb{R}^p \mid \|\theta\|_0 \le k, \quad \text{and} \quad \|\theta\|_2 \le 1 \Big\}.$$

Gilbert-Varshamov: can construct a 2δ -separated set with

$$\log M(2\delta) \approx k \log \left(\frac{ep}{k}\right)$$
 elements

Master equation and minimax rate

$$\log M(2\delta) \approx n\delta^2 \iff \delta^2 \approx \frac{k \log \left(\frac{ep}{k}\right)}{n}.$$

Polynomial-time achievability:

(Zhang, W. & Jordan, 2014)

- by ℓ_1 -relaxations under restricted eigenvalue (RE) conditions (Candes & Tao, 2007; Bickel et al., 2009; Buhlmann & van de Geer, 2011)
- achieve minimax-optimal rates for ℓ_2 -error (Raskutti, W., & Yu, 2011)
- ℓ_1 -methods can be sub-optimal for prediction error $\|X(\widehat{\theta} \theta^*)\|_2 / \sqrt{n}$

Example 2: α -smooth non-parametric regression

Observations $y_i = f^*(x_i) + w_i$, where

$$f^* \in \mathcal{F}(\alpha) = \Big\{ f: [0,1] \to \mathbb{R} \mid \text{ f is α-times diff'ble, with $\sum_{j=0}^{\alpha} \|f^{(j)}\|_{\infty} \leq C \Big\}.$$

Classical results in approximation theory (e.g., Kolmogorov & Tikhomorov, 1959)

$$\log M(2\delta; \mathcal{F}) \simeq (1/\delta)^{1/\alpha}$$

Master equation and minimax rate

$$\log M(2\delta) \approx n\delta^2 \iff \delta^2 \approx (1/n)^{\frac{2\alpha}{2\alpha+1}}.$$

Example 3: Sparse additive and α -smooth

Observations $y_i = f^*(x_i) + w_i$, where f^* satisfies constraints

Additively decomposable:
$$f^*(x_1, \dots x_p) = \sum_{i=1}^p g_j^*(x_j)$$

Sparse: At most k of (g_1^*, \ldots, g^*p) are non-zero

Smooth: Each
$$g_j^*$$
 belongs to α -smooth family $\mathcal{F}(\alpha)$

Combining previous results yields 2δ -packing with

$$\log M(2\delta; \mathcal{F}) \simeq k (1/\delta)^{1/\alpha} + k \log \left(\frac{ep}{k}\right)$$

Master equation and minimax rate

Solving $\log M(2\delta) \approx n\delta^2$ yields

$$\delta^2 \asymp \underbrace{k(1/n)^{\frac{2\alpha}{2\alpha+1}}}_{k\text{-component estimation}} + \underbrace{\frac{k\log\left(\frac{ep}{k}\right)}{n}}_{\text{search complexity}}$$

Summary

To be provided during tutorial....