MAGISTERARBEIT | MASTER'S THESIS

Titel | Title

Density estimation under Differential Privacy

verfasst von | submitted by

Dominik Schiller BSc

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Magister der Sozial- und Wirtschaftswissenschaften (Mag.rer.soc.oec.)

Wien | Vienna, 2024

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 066 951
Studienrichtung lt. Studienblatt | Degree programme as it appears on the student record sheet:	Magisterstudium Statistik
Betreut von | Supervisor:	Assoz. Prof. Mag. Lukas Steinberger Bakk. BA PhD

Abstract

This paper focuses on the histogram density estimator and examines its properties in the classical setting, as well as with regards to Differential Privacy. Preserving privacy is an important part of contemporary statistics, and it generally entails a trade-off between accuracy and privacy. Numerous techniques for preserving privacy have been proposed, a rather recent development is Differential Privacy, where one releases a randomized database. In this context we determine lower and upper bounds on the minimax mean integrated squared error of the histogram density estimator in both the classical and the differentially private setting.

Zusammenfassung

Diese Arbeit konzentriert sich auf den Histogramm-Dichte-Schätzer und untersucht seine Eigenschaften im klassischen Rahmen sowie im Hinblick auf Differential Privacy. Ein wichtiger Bestandteil der modernen Statistik ist die Wahrung der Privatsphäre, wobei dies im Allgemeinen einen Kompromiss zwischen Genauigkeit und Privatsphäre mit sich bringt. Es wurden zahlreiche Techniken zur Wahrung der Privatsphäre vorgeschlagen, eine relativ neue Entwicklung ist Differential Privacy, bei der an Stelle der original Daten, eine randomisierte Version herausgegeben wird. In diesem Zusammenhang bestimmen wir untere und obere Schranken für den minimax mean integrated squared error des Histogramm-Dichte-Schätzers sowohl für den klassischen, als auch für den Fall unter Differential Privacy.

Contents

1 Introduction

Releasing any information based on the data of individuals carries with it an inherent risk. A malicious actor with auxiliary information has the opportunity to draw conclusions about an individual (Gambs, Killijian, and Prado Cortez 2014, Narayanan and Shmatikov 2008, Malin and Sweeney 2004). Numerous privacy-preserving techniques have been developed (Sweeney 2002, N. Li, T. Li, and Venkatasubramanian 2006, Kooiman 1997), in this paper we focus on the notion of *Differential Privacy*, first formalized in Dwork et al. 2006. In the framework of Differential Privacy not the original data, but a randomized version of it is released. This leads to a trade-off, the stronger the randomization, the stronger is also the protection of the privacy of the individual, but the accuracy of the inference based on the randomized data decreases.

In this context we examine the asymptotic properties of the histogram density estimator, first in the non-privacy-preserving setting (Section 2). After the formal introduction of Differential Privacy, we also consider the estimator in this context (Section 3). We reproduce classical results in the ordinary setting, and show that the differentially private histogram has worst case risk bounded by $C \max\left\{(n\epsilon)^{-\frac{2\beta}{\beta+1}}, n^{-\frac{2\beta}{2\beta+1}}\right\}$ from above and by $c \max\left\{(n\epsilon)^{-\frac{2\beta}{\beta+1}}, n^{-\frac{2\beta}{2\beta+1}}\right\}$ from below.

2 Classical Density Estimation

Let

$$\mathcal{P}(L,\beta) = \left\{ p \,|p : [0,1] \to \mathbb{R}_+, \int_0^1 p(s)ds = 1, |p(s) - p(t)| \leq L|s-t|^\beta \right\},$$

with $L \in (0,\infty)$ and $\beta \in (0,1]$ be the set of continuous probability densities on $\mathcal{X} = [0,1]$, which are also in the set of Hölder continuous functions $H(L,\beta)$. Consider $X_1, ..., X_n$, independent and identically distributed random variables with probability density $p \in \mathcal{P}(L,\beta)$ with respect to the Lebesgue measure. The sample size is $n \in \mathbb{N}$ and we will denote the n-fold product measure with respect to p as P_p.

Definition 1. Let $m \in \mathbb{N}$ be the parameter that controls the number of bins and their width. Define $\Delta_1 := [0, \frac{1}{m}]$ and $\Delta_k := (\frac{k-1}{m}, \frac{k}{m}]$ for $k = 2, ..., m$. Δ_k represents the k-th bin. $C_k(X) := |\left\{ i \,\middle|\, X_i \in \Delta_k \right\}| = \sum_{i=1}^n \mathbb{1}_{\Delta_k}(X_i)$ is the number of observations in the k-th bin. Then $\tilde{p}_n(s) := m \sum_{k=1}^m \frac{C_k}{n} \mathbb{1}_{\Delta_k}(s)$ is called the histogram density estimator at $s \in [0,1]$.

2.1 Upper bound in the classical setting

Theorem 2.1. Consider a $p \in \mathcal{P}(L,\beta)$, then an upper bound for the Mean Integrated Squared Error (MISE) of $\tilde{p}_n$ is given by

$$R_{p,n}(\tilde{p}) := \mathbb{E}_p[\|\tilde{p}_n - p\|_2^2] \leq \frac{m}{n} + L^2 \left(\frac{1}{m}\right)^{2\beta}.$$

Here $\mathbb{E}_p$ denotes the expectation with respect to P_p.

Proof. First consider the following decomposition of the MISE,

$$\begin{aligned}
\mathbb{E}_p[\|\tilde{p}_n - p\|_2^2] &= \mathbb{E}_p\left[\int_{\mathcal{X}} (\tilde{p}_n(x) - p(x))^2 dx\right] = \int_{\mathcal{X}} \mathbb{E}_p[(\tilde{p}_n(x) - p(x))^2] dx \\
&= \int_{\mathcal{X}} \mathbb{E}_p[\tilde{p}_n(x)^2 - 2\tilde{p}_n(x)p(x) + p(x)^2] dx \\
&= \int_{\mathcal{X}} \mathbb{E}_p[\tilde{p}_n(x)^2] - 2\mathbb{E}_p[\tilde{p}_n(x)]p(x) + p(x)^2 dx \\
&= \int_{\mathcal{X}} \mathbb{E}_p[\tilde{p}_n(x)^2] - \mathbb{E}_p[\tilde{p}_n(x)]^2 + \mathbb{E}_p[\tilde{p}_n(x)]^2 - 2\mathbb{E}_p[\tilde{p}_n(x)]p(x) \\
&\qquad + p(x)^2 dx \\
&= \int_{\mathcal{X}} \mathbb{E}_p[\tilde{p}_n(x)^2] - \mathbb{E}_p[\tilde{p}_n(x)]^2 dx + \int_{\mathcal{X}} \mathbb{E}_p[\tilde{p}_n(x)]^2 \\
&\qquad - 2\mathbb{E}_p[\tilde{p}_n(x)]p(x) + p(x)^2) dx \\
&= \int_{\mathcal{X}} \mathbb{E}_p[\tilde{p}_n(x)^2] - \mathbb{E}_p[\tilde{p}_n(x)]^2 dx + \int_{\mathcal{X}} (\mathbb{E}_p[\tilde{p}_n(x)] - p(x))^2 dx \\
&= \int_{\mathcal{X}} Var_p(\tilde{p}_n(x)) dx + \int_{\mathcal{X}} Bias(\tilde{p}_n(x))^2 dx.
\end{aligned}$$

We will consider these terms individually. For the variance term, an upper bound can be found as follows,

$$
\begin{aligned}
&\int_{\mathcal{X}} Var_p(\tilde{p}_n(s))ds \\
&\quad = \int_{\mathcal{X}} Var_p\left(m\sum_{k=1}^{m}\frac{C_k}{n}\mathbb{1}_{\Delta_k}(s)\right)ds = \frac{m^2}{n^2}\int_{\mathcal{X}} Var_p\left(\sum_{k=1}^{m}C_k\mathbb{1}_{\Delta_k}(s)\right)ds \\
&\quad = \frac{m^2}{n^2}\left[\sum_{j=1}^{m}\int_{\Delta_j} Var_p\left(\sum_{k=1}^{m}C_k\mathbb{1}_{\Delta_k}(s)\right)ds\right] = \frac{m^2}{n^2}\left[\sum_{j=1}^{m}\int_{\Delta_j} Var_p\left(C_j\right)ds\right] \\
&\quad = \frac{m^2}{n^2}\left[\sum_{j=1}^{m} Var_p\left(C_j\right)\frac{1}{m}\right] = \frac{m}{n^2}\left[\sum_{j=1}^{m} Var_p\left(\sum_{i=1}^{n}\mathbb{1}_{\Delta_j}(X_i)\right)\right] \\
&\quad = \frac{m}{n^2}\left[\sum_{j=1}^{m}\sum_{i=1}^{n} Var_p\left(\mathbb{1}_{\Delta_j}(X_i)\right)\right] = \frac{m}{n^2}\left[\sum_{j=1}^{m} n\, Var_p\left(\mathbb{1}_{\Delta_j}(X_1)\right)\right] \\
&\quad = \frac{m}{n}\left[\sum_{j=1}^{m} Var_p\left(\mathbb{1}_{\Delta_j}(X_1)\right)\right] = \frac{m}{n}\left[\sum_{j=1}^{m}\mathbb{E}_p[\mathbb{1}_{\Delta_j}(X_1)^2] - \mathbb{E}_p[\mathbb{1}_{\Delta_j}(X_1)]^2\right] \\
&\quad = \frac{m}{n}\left[\sum_{j=1}^{m}\mathbb{E}_p[\mathbb{1}_{\Delta_j}(X_1)] - \mathbb{E}_p[\mathbb{1}_{\Delta_j}(X_1)]^2\right] \\
&\quad = \frac{m}{n}\left[\sum_{j=1}^{m} P(X_1 \in \Delta_j) - P(X_1 \in \Delta_j)^2\right] \leq \frac{m}{n}\left[\sum_{j=1}^{m} P(X_1 \in \Delta_j)\right] = \frac{m}{n}.
\end{aligned}
$$

Now for the Bias term,

$$
\begin{aligned}
&\int_{\mathcal{X}} [Bias(\tilde{p}_n(s))]^2 \, ds \\
&= \int_{\mathcal{X}} [\mathbb{E}_p(\tilde{p}_n) - p(s)]^2 \, ds = \int_{\mathcal{X}} \left[\mathbb{E}_p \left(m \sum_{k=1}^{m} \frac{C_k}{n} \mathbb{1}_{\Delta_k}(s) \right) - p(s) \right]^2 ds \\
&= \int_{\mathcal{X}} \left[\frac{m}{n} \sum_{k=1}^{m} \mathbb{E}_p(C_k) \mathbb{1}_{\Delta_k}(s) - p(s) \right]^2 ds \\
&= \int_{\mathcal{X}} \left[\frac{m}{n} \sum_{k=1}^{m} \mathbb{E}_p \left(\sum_{i=1}^{n} \mathbb{1}_{\Delta_k}(X_i) \right) \mathbb{1}_{\Delta_k}(s) - p(s) \right]^2 ds \\
&= \sum_{j=1}^{m} \int_{\Delta_j} \left[\frac{m}{n} \sum_{k=1}^{m} \sum_{i=1}^{n} \mathbb{E}_p \left(\mathbb{1}_{\Delta_k}(X_i) \right) \mathbb{1}_{\Delta_k}(s) - p(s) \right]^2 ds \\
&= \sum_{j=1}^{m} \int_{\Delta_j} \left[\frac{m}{n} \sum_{k=1}^{m} \sum_{i=1}^{n} P(X_i \in \Delta_k) \mathbb{1}_{\Delta_k}(s) - p(s) \right]^2 ds \\
&= \sum_{j=1}^{m} \int_{\Delta_j} \left[\frac{m}{n} \sum_{i=1}^{n} P(X_i \in \Delta_j) - p(s) \right]^2 ds \\
&= \sum_{j=1}^{m} \int_{\Delta_j} [m \, P(X_1 \in \Delta_j) - p(s)]^2 \, ds = \sum_{j=1}^{m} \int_{\Delta_j} \left[m \int_{\Delta_j} p(t) dt - p(s) \right]^2 ds \\
&= \sum_{j=1}^{m} \int_{\Delta_j} \left[m \left(\int_{\Delta_j} p(t) - p(s) dt \right) \right]^2 ds.
\end{aligned}
$$

Here $p(s) = m \int_{\Delta_j} p(s) dt$ was used, and

$$
\begin{aligned}
\int_{\mathcal{X}} [Bias(\tilde{p}_n(s))]^2 \, ds &\leq \sum_{j=1}^{m} \int_{\Delta_j} \left[m \left(\int_{\Delta_j} |p(t) - p(s)| dt \right) \right]^2 ds \\
&\leq \sum_{j=1}^{m} \int_{\Delta_j} \left[m \left(\int_{\Delta_j} L \left(\frac{1}{m} \right)^{\beta} dt \right) \right]^2 ds \\
&= \sum_{j=1}^{m} \int_{\Delta_j} \left[L \left(\frac{1}{m} \right)^{\beta} \right]^2 ds = L^2 \left(\frac{1}{m} \right)^{2\beta}.
\end{aligned}
$$

Therefore an upper bound for the MISE of $\tilde{p}_n$ is given by

$$
\mathbb{E}_p[\|\tilde{p}_n - p\|_2^2] \leq \frac{m}{n} + L^2 \left(\frac{1}{m} \right)^{2\beta}.
$$

□

According to Tsybakov 2009, Theorem 1.1 the minimax optimal m is given by $m = n^{\frac{1}{2\beta+1}}$. Which leads to the following upper bound for the MISE: $\mathbb{E}_p[\|\tilde{p}_n - p\|_2^2] \leq n^{-\frac{2\beta}{2\beta+1}}(L^2 + 1)$.

2.2 Lower bound in the classical setting

This section is adapted from Tsybakov 2009, Chapter 2.

2.2.1 Reduction to minimax probability of error

This section follows Section 2.2 from Tsybakov 2009. Earlier we established an upper bound for the MISE of $\tilde{p}_n$ given by

$$\inf_{\tilde{p}} \sup_{p \in \mathcal{P}(L,\beta)} R_{p,n}(\tilde{p}) \leq C\gamma_n,$$

where $\gamma_n := n^{-\frac{2\beta}{2\beta+1}}$ and some constant C. To find a lower bound for this expression, we start by considering

$$\mathbb{E}_p[\gamma_n^{-1}\|\tilde{p}_n - p\|_2^2] \geq aP_p(\gamma_n^{-1}\|\tilde{p}_n - p\|_2^2 \geq a) = aP_p(\|\tilde{p}_n - p\|_2^2 \geq a\gamma_n), \quad (2.1)$$

where $a > 0$ and the Markov inequality was used. This fact gives rise to the observation, that it is now enough to identify a lower boundary for this probability. A lower bound for the minimax MISE of $\tilde{p}_n$ can therefore be constructed by considering a c such that

$$\inf_{\tilde{p}} \sup_{p \in \mathcal{P}(L,\beta)} P_p(\|\tilde{p}_n - p\|_2^2 \geq u_n) \geq c,$$

where

$$u_n := a\gamma_n. \quad (2.2)$$

Further observe that

$$\inf_{\tilde{p}} \sup_{p \in \mathcal{P}(L,\beta)} P_p(\|\tilde{p}_n - p\|_2^2 \geq u_n) \geq \inf_{\tilde{p}} \sup_{p \in \{p_0, p_1, \dots p_h\}} P_p(\|\tilde{p}_n - p\|_2^2 \geq u_n),$$

where $h \in \mathbb{N}$ and $\{p_0, p_1, \dots p_h\} \subseteq \mathcal{P}(L,\beta)$. If

$$\|p_i - p_j\|_2^2 \geq 4u_n \text{ for all } i, j \in \{0, 1, \dots, h\} \text{ with } i \neq j \quad (2.3)$$

then

$$P_{p_j}(\|\tilde{p}_n - p_j\|_2^2 \geq u_n) \geq P_{p_j}(p^* \neq j),\ j \in \{0, 1, \dots, h\}. \quad (2.4)$$

Here $p^* : \mathcal{X}^n \mapsto \{0, 1, \dots, h\}$ is the minimum distance test, given by

$$p^* = \arg \min_{0 \leq k \leq h} \|\tilde{p}_n - p_k\|_2^2.$$

Then inequality (2.4) follows from the fact that for $k \neq j$

$$\begin{aligned}
\{p^* \neq j\} &= \{\arg \min_{0 \leq k \leq h} \|\tilde{p}_n - p_k\|_2^2 \neq j\} \\
&\subseteq \{\|\tilde{p}_n - p_j\|_2^2 \geq \min_{\substack{0 \leq k \leq h \\ k \neq j}} \|\tilde{p}_n - p_k\|_2^2\} \\
&= \{\|\tilde{p}_n - p_j\|_2 \geq \min_{\substack{0 \leq k \leq h \\ k \neq j}} \|\tilde{p}_n - p_k\|_2\}.
\end{aligned}$$

The triangle inequality and (2.3) motivate the following observation:

$$
\begin{aligned}
&\|p_k - p_j\|_2 \le \|p_k - \tilde{p}_n\|_2 + \|p_j - \tilde{p}_n\|_2 \\
\implies &\|\tilde{p}_n - p_k\|_2 \ge \|p_k - p_j\|_2 - \|p_j - \tilde{p}_n\|_2 \\
\implies &\|\tilde{p}_n - p_k\|_2 \ge \sqrt{4u_n} - \|p_j - \tilde{p}_n\|_2.
\end{aligned}
$$

Therefore

$$
\begin{aligned}
\{p^* \neq j\} &\subseteq \{\|\tilde{p}_n - p_j\|_2 \ge \min_{\substack{0\le k\le h \\ k\neq j}} \sqrt{4u_n} - \|\tilde{p}_n - p_j\|_2\} \\
&= \{\|\tilde{p}_n - p_j\|_2 \ge \sqrt{4u_n} - \|\tilde{p}_n - p_j\|_2\} \\
&= \{\|\tilde{p}_n - p_j\|_2^2 \ge u_n\}.
\end{aligned}
$$

For $\{p_0, p_1, \dots, p_h\}$ that satisfy (2.3), it holds that

$$
\inf_{\tilde{p}} \sup_{p\in\{p_0,p_1,\dots p_h\}} P_p(\|\tilde{p}_n - p\|_2^2 \ge u_n) \ge \inf_{\tau} \max_{0\le j\le h} P_{p_j}(\tau \neq j), \tag{2.5}
$$

where $\inf_\tau$ is the infimum of all tests and a test is defined as a $\mathcal{F}^n =: \mathcal{B}((0,1))^n$ measurable function $\tau : \mathcal{X} \mapsto \{0, 1, \dots, h\}$. Therefore in order to find a lower bound for the MISE of $\tilde{p}_n$, it is sufficient to find a lower bound for

$$
r_h := \inf_{\tau} \max_{0\le j\le h} P_{p_j}(\tau \neq j). \tag{2.6}
$$

2.2.2 Lower bound of the minimax probability of error

Theorem 2.2. (Proposition 2.2 in Tsybakov 2009) Consider probability measures $P_0, P_1, P_2, \dots, P_h$ on $(\mathcal{X}^n, \mathcal{F}^n)$. Further define $P_{0,1}^a, P_{0,2}^a, \dots, P_{0,h}^a$ as the absolutely continuous component of P_0 with respect to $P_1, P_2, \dots, P_h$, respectively. Then

$$
r_h \ge sup_{v>0} \frac{vh}{1+vh} \left(\frac{1}{h} \sum_{j=1}^{h} P_j \left(\frac{dP_{0,j}^a}{dP_j} \ge v \right) \right).
$$

Proof. First let $v > 0$ and define $A_j := \left\{ \frac{dP_{0,j}^a}{dP_j} \ge v \right\}$ and observe that for any test τ it holds that $\bigcup_{j=1}^h \{\tau = j\} = \{\tau \neq 0\}$ and that the events $\{\tau = j\}$ and $\{\tau = k\}$ are disjoint for all $j, k \in \{0, 1, \dots, h\}$ with $j \neq k$. Thus we have

$$
\begin{aligned}
P_0(\tau \neq 0) = \sum_{j=1}^{h} P_0(\tau = j) &\ge \sum_{j=1}^{h} P_{0,j}^a(\tau = j) \\
&\ge v \sum_{j=1}^{h} P_j(\{\tau = j\} \cap A_j),
\end{aligned}
$$

where this inequality follows from

$$
\int_{\{\tau=j\}} dP_{0,j}^a = \int_{\{\tau=j\}} \frac{dP_{0,j}^a}{dP_j} dP_j \ge v \int_{\{\tau=j\}\cap A_j} dP_j,
$$

for all $j \in \{1, \ldots, h\}$. Therefore

$$\begin{aligned}
P_0(\tau \neq 0) &\geq v \sum_{j=1}^{h} P_j(\{\tau = j\} \cap A_j) \\
&= v \sum_{j=1}^{h} [P_j(\{\tau = j\}) - P_j(\{\tau = j\} \setminus A_j)] \\
&\geq v \sum_{j=1}^{h} [P_j(\tau = j) - P_j(A_j^c)] \\
&= vh \left(\frac{1}{h} \sum_{j=1}^{h} P_j(\tau = j) \right) - v \sum_{j=1}^{h} P_j(A_j^c) \\
&= vh(\theta_0 - \alpha),
\end{aligned}$$

where $\theta_0 := \frac{1}{h} \sum_{j=1}^{h} P_j(\tau = j)$ and $\alpha := \frac{1}{h} \sum_{j=1}^{h} P_j \left(\frac{dP_{0,j}^a}{dP_j} < v \right)$. Now consider

$$\begin{aligned}
\max_{0 \leq j \leq h} P_j(\tau \neq j) &= \max \left\{ P_0(\tau \neq 0), \max_{1 \leq j \leq h} P_j(\tau \neq j) \right\} \\
&\geq \max \left\{ vh(\theta_0 - \alpha), \frac{1}{h} \sum_{j=1}^{h} P_j(\tau \neq j) \right\} \\
&= \max \left\{ vh(\theta_0 - \alpha), 1 - \theta_0 \right\} \\
&\geq \min_{0 \leq \theta \leq 1} \max \left\{ vh(\theta - \alpha), 1 - \theta \right\}.
\end{aligned}$$

Setting $vh(\theta - \alpha) = 1 - \theta$ yields $\theta = \frac{vh\alpha + 1}{vh + 1}$. With this

$$\begin{aligned}
\min_{0 \leq \theta \leq 1} \max \left\{ vh(\theta - \alpha), 1 - \theta \right\} &= \min_{0 \leq \theta \leq 1} \max \left\{ vh(\frac{vh\alpha + 1}{vh + 1} - \alpha), 1 - \frac{vh\alpha + 1}{vh + 1} \right\} \\
&= \frac{vh(1 - \alpha)}{1 + vh}.
\end{aligned}$$

Finally

$$\begin{aligned}
\max_{0 \leq j \leq h} P_j(\tau \neq j) \geq \min_{0 \leq \theta \leq 1} \max \left\{ vh(\theta - \alpha), 1 - \theta \right\} &= \frac{vh(1 - \alpha)}{1 + vh} \\
&= \frac{vh}{1 + vh} \left(\frac{1}{h} \sum_{j=1}^{h} P_j \left(\frac{dP_{0,j}^a}{dP_j} \geq v \right) \right).
\end{aligned}$$

□

Definition 2. The Kullback–Leibler divergence between two probability measures P and Q is defined by

$$D_{KL}(P, Q) := \begin{cases} \int \ln \frac{dP}{dQ} dP, & if P \ll Q, \\ +\infty, & otherwise. \end{cases}$$

Lemma 2.3. (Lemma 2.2 in Tsybakov 2009) If P and Q are product measures of the form $P = \bigotimes_{i=1}^{n} P_i$ and $Q = \bigotimes_{i=1}^{n} Q_i$, then

$$D_{KL}(P, Q) = \sum_{i=1}^{n} D_{KL}(P_i, Q_i).$$

Lemma 2.4. (Lemma 2.5 in Tsybakov 2009) The second Pinsker's inequality states that if $P \ll Q$, then

$$\int \max\left\{0, \ln \frac{dP}{dQ}\right\} dP \leq D_{KL}(P, Q) + \sqrt{\frac{D_{KL}(P, Q)}{2}}.$$

For a proof of this lemma, see Appendix B.2.

Theorem 2.5. (Proposition 2.3 in Tsybakov 2009) Consider probability measures $P_0, P_1, P_2, \ldots, P_h$ on $(\mathcal{X}^n, \mathcal{F}^n)$, which satisfy

$$\frac{1}{h} \sum_{j=1}^{h} D_{KL}(P_j, P_0) \leq \eta,$$

where $\eta \in (0, \infty)$. Then for r_h as defined in (2.6) we get

$$r_h \geq \sup_{0<v<1} \left(\frac{vh}{1+vh} \left(1 + \frac{\eta + \sqrt{\frac{\eta}{2}}}{\ln v} \right) \right).$$

Proof. In light of Theorem 2.2 it is sufficient to verify that

$$\frac{1}{h} \sum_{j=1}^{h} P_j \left(\frac{dP_{0,j}^a}{dP_j} \geq v \right) \geq 1 + \frac{\eta + \sqrt{\frac{\eta}{2}}}{\ln v},$$

for all $v \in (0, 1)$. Because of the condition on the Kullback-Leibler divergence, it immediatly follows that $P_j \ll P_0$ and $\frac{dP_j}{dP_0} = \frac{dP_j}{dP_{0,j}^a}$ P_j-almost surely for all $j \in \{1, \ldots, h\}$. Therefore

$$\begin{aligned}
P_j \left(\frac{dP_{0,j}^a}{dP_j} \geq v \right) &= P_j \left(\frac{dP_j}{dP_0} \leq \frac{1}{v} \right) = 1 - P_j \left(\ln \frac{dP_j}{dP_0} > \ln \frac{1}{v} \right) \\
&= 1 - P_j \left(\max\left\{0, \ln \frac{dP_j}{dP_0}\right\} + \min\left\{0, \ln \frac{dP_j}{dP_0}\right\} > \ln \frac{1}{v} \right) \\
&\geq 1 - P_j \left(\max\left\{0, \ln \frac{dP_j}{dP_0}\right\} > \ln \frac{1}{v} \right) \\
&\geq 1 - \frac{1}{\ln \frac{1}{v}} \int \max\left\{0, \ln \frac{dP_j}{dP_0}\right\} dP_j,
\end{aligned}$$

where the Markov inequality was used. Then

$$\begin{aligned}
P_j \left(\frac{dP_{0,j}^a}{dP_j} \geq v \right) &\geq 1 - \frac{1}{\ln \frac{1}{v}} \int \max\left\{0, \ln \frac{dP_j}{dP_0}\right\} dP_j \\
&\geq 1 - \frac{1}{\ln \frac{1}{v}} \left(D_{KL}(P_j, P_0) + \sqrt{\frac{D_{KL}(P_j, P_0)}{2}} \right),
\end{aligned}$$

by the Pinsker inequality, Lemma 2.4. Now the following result is given by the Jensen inequality,

$$\frac{1}{h}\sum_{j=1}^{h}\sqrt{D_{KL}(P_j,P_0)} \leq \left(\frac{1}{h}\sum_{j=1}^{h}D_{KL}(P_j,P_0)\right)^{\frac{1}{2}} \leq \sqrt{\eta}.$$

And therefore

$$\begin{aligned}\frac{1}{h}\sum_{j=1}^{h}P_j\left(\frac{dP^a_{0,j}}{dP_j}\geq v\right) &\geq 1-\frac{1}{\ln\frac{1}{v}}\left(\frac{1}{h}\sum_{j=1}^{h}\left[D_{KL}(P_j,P_0)+\sqrt{\frac{D_{KL}(P_j,P_0)}{2}}\right]\right)\\ &\geq 1-\frac{\eta+\sqrt{\frac{\eta}{2}}}{\ln\frac{1}{v}} = 1+\frac{\eta+\sqrt{\frac{\eta}{2}}}{\ln v}.\end{aligned}$$

□

Theorem 2.6. (Theorem 2.5 in Tsybakov 2009) Let $h \geq 2$ and consider $p_0, p_1, \ldots, p_h \in \mathcal{P}(L,\beta)$, which satisfy the following conditions:

i. $\|p_j - p_k\|_2^2 \geq 4u_n > 0$ for all $0 \leq j < k \leq h$ and

ii. $\frac{1}{h}\sum_{j=1}^{h} D_{KL}(P_{p_j}, P_{p_0}) \leq \eta' \ln h$,

where $\eta' \in (0, \frac{1}{8})$. Then

$$\inf_{\tilde{p}}\sup_{p\in\mathcal{P}(L,\beta)} P_p(\|\tilde{p}-p\|_2^2 \geq u_n) \geq \frac{\sqrt{h}}{1+\sqrt{h}}\left(1-2\eta'-\sqrt{\frac{2\eta'}{\ln h}}\right) > 0.$$

Proof. We use Theorem 2.5 where we set $\eta = \eta' \ln h$ and $v = \frac{1}{\sqrt{h}}$. With this we get

$$\begin{aligned} r_h &\geq \frac{\frac{1}{\sqrt{h}}h}{1+\frac{1}{\sqrt{h}}h}\left(1+\frac{\eta'\ln h+\sqrt{\frac{\eta'\ln h}{2}}}{\ln\frac{1}{\sqrt{h}}}\right)\\ &= \frac{\sqrt{h}}{1+\sqrt{h}}\left(1-2\eta'-\sqrt{\frac{2\eta'}{\ln h}}\right)\\ &\geq \frac{\sqrt{h}}{1+\sqrt{h}}\left(1-\left(2\eta'+\sqrt{\frac{2\eta'}{\ln 2}}\right)\right)\\ &\geq \frac{\sqrt{h}}{1+\sqrt{h}}\left(1-\left(\frac{2}{8}+\frac{1}{2\sqrt{\ln 2}}\right)\right) > 0,\end{aligned}$$

for $\eta' \in (0, \frac{1}{8})$. The claim follows with (2.5). □

2.2.3 Construction of PDF candidates

This section follows Section 2.6.1 from Tsybakov 2009. Consider a $c_0 \in (0,\infty)$ and define $w_n := \left\lceil c_0 n^{\frac{1}{2\beta+1}}\right\rceil$, $x_{+,k} := \frac{k-\frac{3}{4}}{w_n}$ and $x_{-,k} := \frac{k-\frac{1}{4}}{w_n}$. Further define

$K(y) := \exp\left(-\frac{1}{1-y^2}\right)\mathbb{1}_{(-1,1)}(y)$ and

$$\phi_k(x;\lambda) := \lambda L\left(\frac{1}{w_n}\right)^{\beta}\left(K\left(4w_n(x-x_{+,k})\right) - K\left(4w_n(x-x_{-,k})\right)\right),$$

where $0 < \lambda \leq 1$ sufficiently small and $k \in \{1,\ldots,w_n\}$. Now consider the following partition of $[0,1]$, similar to the one employed in section 2, $\Delta_1 := [0, \frac{1}{w_n}]$ and $\Delta_k := (\frac{k-1}{w_n}, \frac{k}{w_n}]$ for $k \in \{2,\ldots,w_n\}$ and $\Delta_{+,1} = [0, \frac{1}{2w_n}], \Delta_{-,1} = (\frac{1}{2w_n}, \frac{1}{w_n}]$ and $\Delta_{+,k} = (\frac{k-1}{w_n}, \frac{2k-1}{2w_n}], \Delta_{-,k} = (\frac{2k-1}{2w_n}, \frac{k}{w_n}]$.

Figure 1: Example of $\phi_1(x;\lambda)$ with $\lambda = L = \beta = 1$ and $w_n = 3$.

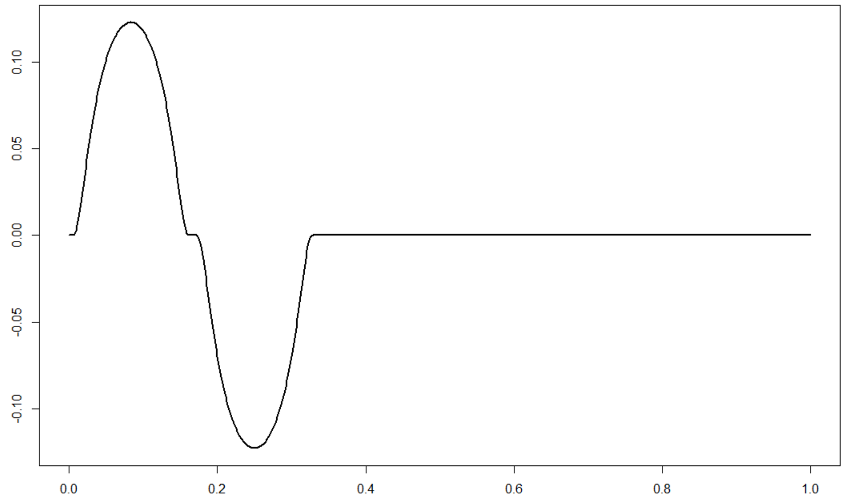
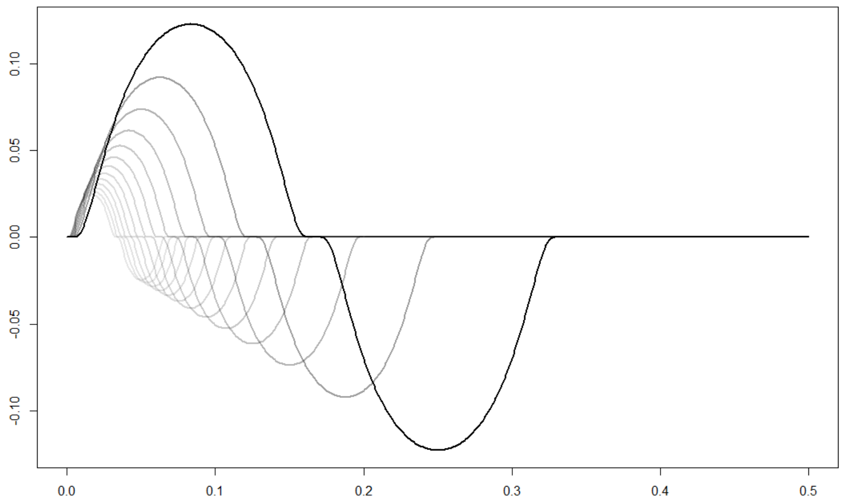


Figure 2: Example of $\phi_1(x;\lambda)$ with $\lambda = L = \beta = 1$ and $w_n \in \{3, 4, 5, \ldots, 15\}$.



Lemma 2.7. The function ϕ_k has the following properties:

i. $\phi_k(x;\lambda) = 0$ for all $x \in \mathbb{R} \setminus \Delta_k$ and all $k \in \{1, \dots, w_n\}$,

ii. $\int_0^1 (\phi_k(x;\lambda))^2 dx = \frac{\lambda^2 L^2}{2} \left(\frac{1}{w_n}\right)^{2\beta+1} \|K\|_2^2$ for all $k \in \{1, \dots, w_n\}$,

iii. $\int_0^1 \phi_k(x;\lambda) dx = 0$ for all $k \in \{1, \dots, w_n\}$ and

iv. $|\phi_k(x;\lambda) - \phi_k(y;\lambda)| \leq L|x-y|^\beta$ with $\lambda \leq \frac{5}{8}\frac{1}{4^\beta}$ and for all $k \in \{1, \dots, w_n\}$.

v. $|\phi_k(x;\lambda)| \leq 1$ with $\lambda \leq \frac{e}{L}$ for all $x \in [0,1]$ and for all $k \in \{1, \dots, w_n\}$.

Proof. We start by proving the first statement. First observe that $\mathbb{R} \setminus \Delta_1 = (-\infty, 0) \cup (\frac{1}{w_n}, \infty)$ and $\mathbb{R} \setminus \Delta_k = (-\infty, \frac{k-1}{w_n}] \cup (\frac{k}{w_n}, \infty)$ for all $k \in \{2, \dots, w_n\}$. Then we will look at the first use of the function K for the case $k = 1$ first. It is obvious that it is sufficient to examine the indicator function. We check for which $x \in \mathbb{R}$ it holds that $\mathbb{1}_{(-1,1)}(4w_n(x - x_{+,1})) = 1$. Therefore

$$\begin{aligned} -1 < 4w_n(x - x_{+,1}) < 1 &\iff -\frac{1}{4w_n} < x - \frac{1-\frac{3}{4}}{w_n} < \frac{1}{4w_n} \\ &\iff 0 < x < \frac{1}{2w_n}. \end{aligned}$$

We have shown that $\mathbb{1}_{(-1,1)}(4w_n(x - x_{+,1})) = 1$ for all $x \in (0, \frac{1}{2w_n}) \subset \Delta_{+,1} \subseteq \Delta_1$ and therefore $K(4w_n(x - x_{+,1})) = 0$ for all $x \in \mathbb{R} \setminus \Delta_{+,1} \supseteq \mathbb{R} \setminus \Delta_1$. It can be shown in a similar fashion that $K(4w_n(x - x_{-,1})) = 0$ for all $x \in \mathbb{R} \setminus \Delta_{-,1} \supseteq \mathbb{R} \setminus \Delta_1$. This implies the desired result for $k = 1$, the proof for $k = 2, \dots, w_n$ follows the same structure.

Now for the proof of the second statement. Let $u_+ = 4w_n(x - x_{+,k})$ and $u_- = 4w_n(x - x_{-,k})$, then

$$\begin{aligned} \int_0^1 (\phi_k(x;\lambda))^2 dx &= \int_0^1 \left(\lambda L \left(\frac{1}{w_n}\right)^\beta (K(u_+) - K(u_-))\right)^2 dx \\ &= \lambda^2 L^2 \left(\frac{1}{w_n}\right)^{2\beta} \int_0^1 (K(u_+) - K(u_-))^2 dx. \end{aligned}$$

The next two equalities follow from Lemma 2.7.i and the observation that $K(4w_n(x - x_{+,k})) = 0$ for all $x \in \mathbb{R} \setminus \Delta_{+,k}$ and $K(4w_n(x - x_{-,k})) = 0$ for all $x \in \mathbb{R} \setminus \Delta_{-,k}$ for all $k \in \{1, \dots, w_n\}$. Therefore

$$\begin{aligned} \int_0^1 (\phi_k(x;\lambda))^2 dx &= \lambda^2 L^2 \left(\frac{1}{w_n}\right)^{2\beta} \int_{\Delta_k} (K(u_+) - K(u_-))^2 dx \\ &= \lambda^2 L^2 \left(\frac{1}{w_n}\right)^{2\beta} \left(\int_{\Delta_{+,k}} (K(u_+))^2 dx + \int_{\Delta_{-,k}} (K(u_-))^2 dx\right) \\ &= \lambda^2 L^2 \left(\frac{1}{w_n}\right)^{2\beta} \frac{1}{4w_n} \left(\int_{-1}^1 (K(y))^2 dy + \int_{-1}^1 (K(y))^2 dy\right) \\ &= \frac{\lambda^2 L^2}{2} \left(\frac{1}{w_n}\right)^{2\beta+1} \|K\|_2^2. \end{aligned}$$

The third statement follows immediately from the construction of ϕ_k.

To arrive at a proof of the fourth statement, we first show that K is Lipschitz continuous. Consider

$$K'(x) = \begin{cases} -\frac{2x\exp\left(-\frac{1}{1-x^2}\right)}{(1-x^2)^2}, & \text{for } -1 < x < 1 \\ 0, & \text{otherwise} \end{cases}$$

and

$$K''(x) = \begin{cases} \frac{2(3x^4-1)\exp\left(-\frac{1}{1-x^2}\right)}{(1-x^2)^4}, & \text{for } -1 < x < 1 \\ 0, & \text{otherwise.} \end{cases}$$

Setting $K''(x)$ equal to zero on $(-1,1)$ provides $x_{1,2} = \pm\sqrt[4]{\frac{1}{3}}$. Then for K' it holds that $\left|K'\left(\pm\sqrt[4]{\frac{1}{3}}\right)\right| \leq \frac{4}{5}$, and K is therefore Lipschitz continuous with constant $\frac{4}{5}$. This in turn implies that $K \in H(\frac{4}{5}, \beta)$. Then

$$\begin{aligned}
|\phi_k(x;\lambda) - \phi_k(y)| &= \lambda L \left(\frac{1}{w_n}\right)^\beta |K(4w_n(x - x_{+,k})) - K(4w_n(x - x_{-,k})) \\
&\quad - K(4w_n(y - x_{+,k})) + K(4w_n(y - x_{-,k}))| \\
&\leq \lambda L \left(\frac{1}{w_n}\right)^\beta (|K(4w_n(x - x_{+,k})) - K(4w_n(y - x_{+,k}))| \\
&\quad + |K(4w_n(x - x_{-,k})) - K(4w_n(y - x_{-,k}))|) \\
&\leq \lambda L \left(\frac{1}{w_n}\right)^\beta \left(\frac{4|4w_n(x - x_{+,k}) - 4w_n(y - x_{+,k})|^\beta}{5}\right. \\
&\quad \left. + \frac{4|4w_n(x - x_{-,k}) - 4w_n(y - x_{-,k})|^\beta}{5}\right) \\
&= 8\frac{4^\beta}{5}\lambda L|x-y|^\beta \leq L|x-y|^\beta,
\end{aligned}$$

for $\lambda \leq \frac{5}{8}\frac{1}{4^\beta}$.

For the fifth statement, let $K_{max} := \max_{x\in(-1,1)} K(x)$ and consider

$$\begin{aligned}
|\phi_k(x;\lambda)| &= \left|\lambda L \left(\frac{1}{w_n}\right)^\beta (K(4w_n(x - x_{+,k}) - K(4w_n(x - x_{-,k}))\right| \\
&\leq \left|\lambda L \left(\frac{1}{w_n}\right)^\beta K_{max}\right| = \left|\lambda L \left(\frac{1}{w_n}\right)^\beta e^{-1}\right| \leq \left|\lambda L e^{-1}\right| \leq 1,
\end{aligned}$$

for $\lambda \leq \frac{e}{L}$. ☐

Now consider $\Omega := \{0,1\}^{w_n}$, the set of all binary sequences of length w_n. Then define $p_0(x) = \mathbb{1}_{[0,1]}(x)$ and

$$\Sigma := \left\{p_\omega(x) = p_0(x) + \sum_{k=1}^{w_n} \omega_k \phi_k(x;\lambda) : \omega \in \Omega\right\}.$$

Now for $\omega, \omega' \in \Omega$,

$$\begin{aligned}
\|p_\omega - p_{\omega'}\|_2^2 &= \int_0^1 \left(p_\omega(x) - p_{\omega'}(x)\right)^2 dx \\
&= \int_0^1 \left(p_0(x) + \sum_{k=1}^{w_n} \omega_k \phi_k(x;\lambda) - p_0(x) - \sum_{k=1}^{w_n} \omega_k' \phi_k(x;\lambda)\right)^2 dx \\
&= \int_0^1 \left(\sum_{k=1}^{w_n} (\omega_k - \omega_k')\phi_k(x;\lambda)\right)^2 dx \\
&= \sum_{j=1}^{w_n} \int_{\Delta_j} \left(\sum_{k=1}^{w_n} (\omega_k - \omega_k')\phi_k(x;\lambda)\right)^2 dx.
\end{aligned}$$

Using Lemma 2.7.i and Lemma 2.7.ii we get

$$\begin{aligned}
\|p_\omega - p_{\omega'}\|_2^2 &= \sum_{j=1}^{w_n} (\omega_j - \omega_j')^2 \int_{\Delta_j} \left(\phi_j(x;\lambda)\right)^2 dx \\
&= \sum_{j=1}^{w_n} (\omega_j - \omega_j')^2 \frac{\lambda^2 L^2}{2} \left(\frac{1}{w_n}\right)^{2\beta+1} \|K\|_2^2 \\
&= \frac{\lambda^2 L^2}{2} \left(\frac{1}{w_n}\right)^{2\beta+1} \|K\|_2^2 d_{ham}(\omega, \omega'). \qquad (2.7)
\end{aligned}$$

Here $d_{ham}(\omega, \omega')$ denotes the Hamming distance between ω and ω', i.e. the number of differing components between the vectors.

Lemma 2.8. If $0 \leq \lambda \leq \frac{e}{L}$, then $p_\omega \in \Sigma$ is a probability density function.

Proof. With Lemma 2.7.iii it immediately follows that

$$\int_0^1 p_\omega(x) dx = \int_0^1 p_0(x) + \sum_{k=1}^{w_n} \omega_k \phi_k(x;\lambda) dx = 1.$$

Then according to Lemma 2.7.v, for $x \in \Delta_j$

$$p_\omega(x) = p_0(x) + \sum_{k=1}^{w_n} \omega_k \phi_k(x;\lambda) = p_0(x) + \omega_j \phi_j(x;\lambda) \geq p_0(x) - \omega_k = 0,$$

for all $j \in \{1, \ldots, w_n\}$. ∎

As it was established in Section 2.2.1, we need to construct functions $p_{j,n}$, where $j \in \{0, \ldots, w_n\}$ such that $\|p_{j,n} - p_{k,n}\|_2^2 > 4u_n \propto n^{-\frac{2\beta}{2\beta+1}}$ for $j \neq k$. This can be accomplished with the previous construction, where $\|p_\omega - p_{\omega'}\|_2^2 = \frac{L^2}{2}\left(\frac{1}{w_n}\right)^{2\beta+1} \|K\|_2^2 d_{ham}(\omega, \omega') \propto \left(\frac{1}{w_n}\right)^{2\beta+1} d_{ham}(\omega, \omega')$. With this consideration, it is sufficient that $d_{ham}(\omega, \omega') \propto w_n$.

2.2.4 Lower bound of the MISE

Theorem 2.9. (Lemma 2.9 in Tsybakov 2009) The Varshamov–Gilbert bound states that for $n \geq 8$ there exists $N \geq 2^{\frac{n}{8}}$ and $\{\omega^{(0)}, \dots, \omega^{(N)}\} \subseteq \Omega := \{0,1\}^n$ such that $\omega^{(0)} = (0, \dots, 0)$ and

$$d_{ham}(\omega^{(i)}, \omega^{(j)}) \geq \frac{n}{8},$$

for all $i, j \in \{0, \dots, N\}$ with $i \neq j$.

A proof of this theorem is given in Appendix B.1.

Theorem 2.10. (Theorem 2.8 in Tsybakov 2009) Let $L > 0$ and $\beta > 0$, then there exists $c > 0$, such that

$$\liminf_{n\to\infty} \inf_{\tilde{p}_n} \sup_{p\in\mathcal{P}(L,\beta)} \mathbb{E}_p(n^{\frac{2\beta}{2\beta+1}} \|\tilde{p}_n - p\|_2^2) \geq c.$$

Proof. Let $\{\omega^{(0)}, \omega^{(1)}, \dots, \omega^{(N)}\} \subseteq \Omega = \{0,1\}^{w_n}$ as in Theorem 2.9 and let $\eta' \in (0, \frac{1}{8})$. Further define $p_{j,n} := p_{\omega^{(j)}}$ and $P_{j,n}$ as the probability measure with respect to $p_{j,n}$ for all $j \in \{0, \dots, N\}$. Additionally let $P_{j,n}^n$ denote the n-fold product measure with respect to $p_{j,n}$ for all $j \in \{0, \dots, N\}$ and let $0 < \lambda < \min\left\{\frac{e}{L}, \frac{5}{8}\frac{1}{4^\beta}\right\}$. We check the assumptions of Theorem 2.6, in order to apply it. Therefore we examine if the following holds true:

a. $\|p_{j,n} - p_{k,n}\|_2^2 \geq 4u_n$ for all $j, k \in \{0, \dots, N\}$ with $j \neq k$,

b. $p_{j,n} \in \mathcal{P}(L, \beta)$ for all $j \in \{0, \dots, N\}$ and

c. $\frac{1}{N}\sum_{j=1}^N D_{KL}(P_{j,n}^n, P_{0,n}^n) \leq \eta' \ln N$.

For the first assumption, we recall (2.7),

$$\|p_{j,n} - p_{k,n}\|_2^2 = \|p_{\omega^{(j)}} - p_{\omega^{(k)}}\|_2^2 = \frac{\lambda^2 L^2}{2}\left(\frac{1}{w_n}\right)^{2\beta+1} \|K\|_2^2 d_{ham}(\omega^{(j)}, \omega^{(k)}).$$

With Theorem 2.9

$$\|p_{j,n} - p_{k,n}\|_2^2 \geq \frac{\lambda^2 L^2}{2}\left(\frac{1}{w_n}\right)^{2\beta+1} \|K\|_2^2 \frac{w_n}{8} = \frac{\lambda^2 L^2}{16}\left(\frac{1}{w_n}\right)^{2\beta} \|K\|_2^2,$$

for all $w_n \geq 8$. Now set $n_0 = \left(\frac{8}{c_0}\right)^{2\beta+1}$, then for all $n \geq n_0$ we have

$$w_n = \left\lceil c_0 n^{\frac{1}{2\beta+1}} \right\rceil \geq \left\lceil c_0 \left(\left(\frac{8}{c_0}\right)^{2\beta+1}\right)^{\frac{1}{2\beta+1}} \right\rceil = 8,$$

and

$$w_n^{2\beta} = \left\lceil c_0 n^{\frac{1}{2\beta+1}} \right\rceil^{2\beta} \leq \left(1 + \frac{1}{8}\right)^{2\beta} c_0^{2\beta} n^{\frac{2\beta}{2\beta+1}} \leq (2c_0)^{2\beta} n^{\frac{2\beta}{2\beta+1}}.$$

We can therefore conclude that

$$\begin{aligned}\|p_{j,n}-p_{k,n}\|_2^2 &\geq \frac{\lambda^2L^2}{16}\left(\frac{1}{w_n}\right)^{2\beta}\|K\|_2^2\\ &\geq \frac{\lambda^2L^2}{16}(2c_0)^{-2\beta}n^{-\frac{2\beta}{2\beta+1}}\|K\|_2^2 = 4u_n,\end{aligned}$$

where u_n, defined in (2.2), is given by $u_n = an^{-\frac{2\beta}{2\beta+1}}$ and $a = \frac{\lambda^2L^2}{64}(2c_0)^{-2\beta}\|K\|_2^2$.

For the second assumption, recall the definition of $p_{j,n}$,

$$p_{j,n}(x) := p_{\omega^{(j)}}(x) := p_0(x) + \sum_{k=1}^{w_n}\omega_k^{(j)}\phi_k(x;\lambda),$$

where $\omega^{(j)} \in \Omega$. $p_0(x)$ is a constant function on $[0,1]$ and according to Lemma 2.7.iv we have that $\phi_k \in H(L,\beta)$. Since all ϕ_k have disjoint support, it follows that $p_{j,n} \in \mathcal{P}(L,\beta)$ on $[0,1]$ for all $j \in \{0,\dots,N\}$.

For the third assumption, we use Lemma 2.3 and Lemma B.4

$$\begin{aligned}D_{KL}(P_{j,n}^n,P_{0,n}^n) &= nD_{KL}(P_{j,n},P_{0,n}) \leq n\mathcal{X}^2(P_{j,n},P_{0,n}) \qquad (2.8)\\ &= n\int_0^1\left(\frac{p_{j,n}(x)}{p_{0,n}(x)}-1\right)^2 p_{0,n}(x)dx\\ &= n\int_0^1 (p_{j,n}(x)-1)^2\,dx\\ &= n\int_0^1\left(p_0(x)+\left(\sum_{k=1}^{w_n}\omega_k^{(j)}\phi_k(x;\lambda)\right)-1\right)^2 dx\\ &= n\sum_{i=1}^{w_n}\int_{\Delta_i}\left(\sum_{k=1}^{w_n}\omega_k^{(j)}\phi_k(x;\lambda)\right)^2 dx\\ &= n\sum_{i=1}^{w_n}\int_{\Delta_i}\left(\omega_i^{(j)}\phi_i(x)\right)^2 dx\\ &= n\sum_{i=1}^{w_n}\left(\omega_i^{(j)}\right)^2\int_{\Delta_i}(\phi_i(x))^2\,dx\\ &\leq n\sum_{i=1}^{w_n}\int_{\Delta_i}(\phi_i(x))^2\,dx = n\sum_{i=1}^{w_n}\int_0^1(\phi_i(x))^2\,dx.\end{aligned}$$

Using Lemma 2.7.ii we get

$$\begin{aligned}D_{KL}(P_{j,n}^n,P_{0,n}^n) &\leq nw_n\frac{\lambda^2L^2}{2}\left(\frac{1}{w_n}\right)^{2\beta+1}\|K\|_2^2\\ &\leq n\frac{\lambda^2L^2}{2}\left(\frac{1}{c_0n^{\frac{1}{2\beta+1}}}\right)^{2\beta}\|K\|_2^2 \qquad (2.9)\\ &= \frac{\lambda^2L^2}{2}c_0^{-(2\beta+1)}n^{\frac{1}{2\beta+1}}\|K\|_2^2.\end{aligned}$$

Setting $c_0 = \left(\frac{\lambda^2 L^2 \|K\|_2^2}{2\eta'}\right)^{\frac{1}{2\beta+1}}$ then for all $n \geq \max\left\{n_0, \left\lceil \left(\frac{8}{\ln 2}\right)^{\frac{2\beta+1}{2\beta}} \right\rceil\right\}$ we have

$$D_{KL}(P_{j,n}^n, P_{0,n}^n) \leq \eta' n^{\frac{1}{2\beta+1}} \leq \eta' \ln N.$$

All assumptions of Theorem 2.6 are fulfilled, therefore for all estimators $\tilde{p}_n$ it holds that

$$\sup_{p \in \mathcal{P}(L,\beta)} P_p(\|\tilde{p}_n - p\|_2^2 \geq u_n) \geq \frac{\sqrt{N}}{1+\sqrt{N}} \left(1 - 2\eta' - \sqrt{\frac{2\eta'}{\ln N}}\right) > 0.$$

The claim follows from this observation. □

This result, along with the one obtained in Section 2.1, implies that

$$C \geq \liminf_{n\to\infty} \inf_{\tilde{p}} \sup_{p \in \mathcal{P}(L,\beta)} n^{\frac{2\beta}{2\beta+1}} R_{p,n}(\tilde{p}) \geq c,$$

for some constants $c > 0$ and $C < \infty$. Therefore $n^{-\frac{2\beta}{2\beta+1}}$ is the rate of convergence of the MISE of $\tilde{p}_n$.

3 Density Estimation under Differential Privacy

3.1 Differential Privacy

The goal of Differential Privacy can be understood as a type of reassurance for an individual in a database. No amount of auxiliary information, be it in the form of private knowledge about the individual or publicly available databases, should help with the identification of an individual. Note that preserving privacy specifies not being able to identify an individual in a database, but does not forbid learning anything about said individual. To see this, consider an example, where a dental clinic releases a database. Suppose this database allows one to conclude that excessive sugar consumption causes an increase in the probability of developing caries. Then for every individual in this database, some information was gained. But this conclusion would have been reached regardless of whether a single individual was included in the database or not. Therefore the only reservations an individual should have about being in the database should be if there is a risk of identification. Differential privacy is a technique developed for this purpose.

Definition 3. Let $(\mathcal{X}, \mathcal{F})$ and $(\mathcal{Z}, \mathcal{G})$ be measurable spaces. A function $Q : \mathcal{X} \times \mathcal{G} \to [0, 1]$ is called a Markov kernel if it has the following properties

i. $G \mapsto Q(G|x)$ is a probability measure on $(\mathcal{Z}, \mathcal{G})$ for every $x \in \mathcal{X}$,

ii. $x \mapsto Q(G|x)$ is $\mathcal{F}$ measurable for every $G \in \mathcal{G}$.

A Markov kernel is sometimes called a channel.

Definition 4. (Dwork 2006) Consider $\mathcal{X}^n = [0, 1]^n$ and the measurable spaces $(\mathcal{X}^n, \mathcal{F}^n)$ and $(Y, \mathcal{G})$. For $x, x' \in \mathcal{X}^n$ define the Hamming distance between x and x' as $d_{ham}(x, x') = |\{i : x_i \neq x'_i\}|$, i.e. the number of differing observations. Let $\epsilon \in (0, \infty)$, a Markov kernel $Q : \mathcal{X}^n \times \mathcal{G} \to [0, 1]$ is ϵ-differentially private if for all measurable $G \in \mathcal{G}$ and $x, x' \in \mathcal{X}^n$ with $d_{ham}(x, x') \leq 1$ it holds that

$$Q(G|x) \leq e^{\epsilon} Q(G|x').$$

The ϵ in the definition of Differential Privacy is called the privacy level, or the privacy budget. Higher values of ϵ represent "weaker" privacy protection, lower values "stronger".

Definition 5. The Laplace distribution is a family of continuous probability distributions defined on $\mathbb{R}$. The probability density function of an univariate Laplace distribution is given by $f(x; \mu, \alpha) = \frac{\alpha}{2} \exp(-|x - \mu|\alpha)$, where $\mu \in \mathbb{R}$ is the location and $\alpha \in (0, \infty)$ the rate parameter.

Throughout the upcoming sections, the notation $\mathrm{Lap}(\mu, \alpha)$ will be employed for a Laplace distribution with parameters μ and α. When $\mu = 0$, $\mathrm{Lap}(\alpha)$ will be used.

Let $\mathcal{Z} := \mathbb{R}^m$ and $\mathcal{G}_0 := \mathcal{B}(\mathbb{R}^m)$ and consider $W_1, W_2, \ldots W_m$, a sample of size m of independent and identically distributed random variables from a

$\mathrm{Lap}(\frac{\epsilon}{2})$ distribution. Further define for $x \in \mathbb{R}^n$

$$C(x) := \begin{pmatrix} C_1(x) \\ C_2(x) \\ \vdots \\ C_m(x) \end{pmatrix} \in \mathbb{N}_0^m \text{ and } W := \begin{pmatrix} W_1 \\ W_2 \\ \vdots \\ W_m \end{pmatrix} \in \mathbb{R}^m,$$

where $C_k(x)$ with $k = 1, \ldots, m$ is specified as in Section 2, that is $C_k(x) := |\{ i \,|\, X_i \in \Delta_k \}| = \sum_{i=1}^n \mathbb{1}_{\Delta_k}(X_i)$ with $\Delta_1 := [0, \frac{1}{m}]$ and $\Delta_k := (\frac{k-1}{m}, \frac{k}{m}]$ for $k = 2, ..., m$. Further recall that $X_1, ..., X_n$ are independent and identically distributed random variables with probability density $p \in \mathcal{P}(L, \beta)$. Consider now the estimator $\hat{p}_n(s) := m \sum_{k=1}^m \frac{Z_k}{n} \mathbb{1}_{\Delta_k}(s) = \tilde{p}_n(s) + m \sum_{k=1}^m \frac{W_k}{n} \mathbb{1}_{\Delta_k}(s) =: \tilde{p}_n(s) + \hat{q}_n(s)$, where $Z_k := [C(X) + W]_k$ and $Z := (Z_1, Z_2, \ldots, Z_m)^\top$. Let Q_0 denote the conditional distribution $Z|X = x$.

Lemma 3.1. The channel Q_0 is ϵ-differentially private.

Proof. First consider

$$\begin{aligned}
&\sup_{\substack{x,x' \in \mathcal{X}^n \\ d_{ham}(x,x') \leq 1}} \|C(x) - C(x')\|_1 \\
&\qquad = \sup_{\substack{x,x' \in \mathcal{X}^n \\ d_{ham}(x,x') \leq 1}} \sum_{k=1}^m |C_k(x) - C_k(x')| \\
&\qquad = \sup_{\substack{x,x' \in \mathcal{X}^n \\ d_{ham}(x,x') \leq 1}} \sum_{k=1}^m \left| \sum_{i=1}^n \mathbb{1}_{\Delta_k}(x_i) - \sum_{i=1}^n \mathbb{1}_{\Delta_k}(x_i') \right| \\
&\qquad = \sup_{x,x' \in \mathcal{X}^n} \sum_{k=1}^m |\mathbb{1}_{\Delta_k}(x) - \mathbb{1}_{\Delta_k}(x')| = 2.
\end{aligned}$$

Now consider the distributions of $Z_k|X = x \sim [W + C(x)]_k$ and $Z_k|X = x' \sim [W + C(x')]_k$ which are given by a $\mathrm{Lap}(C_k(x), \frac{\epsilon}{2})$ and a $\mathrm{Lap}(C_k(x'), \frac{\epsilon}{2})$ distribution respectively. Now define $f_{Z|X=x} := \prod_{k=1}^m f\left(z_k; C_k(x), \frac{\epsilon}{2}\right)$ and $Q_0(G|x) := \int_G f_{Z|X=x}(z) d\lambda(z)$, for all $G \in \mathcal{G}_0$. Therefore

$$\frac{Q_0(G|x)}{Q_0(G|x')} = \frac{\int_G \prod_{k=1}^m f\left(z; C_k(x), \frac{\epsilon}{2}\right) d\lambda(z)}{\int_G \prod_{k=1}^m f\left(z; C_k(x'), \frac{\epsilon}{2}\right) d\lambda(z)}.$$

To ensure ϵ-Differential Privacy of the channel Q_0 it is therefore sufficient to consider the quotient of the two Laplace densities at a single point $z \in \mathbb{R}^m$,

$$
\begin{aligned}
\frac{f_{Z|X=x}(z)}{f_{Z|X=x'}(z)} &= \prod_{k=1}^{m} \frac{\frac{\epsilon}{4}\exp\left(-\frac{|z_k - C_k(x)|\epsilon}{2}\right)}{\frac{\epsilon}{4}\exp\left(-\frac{|z_k - C_k(x')|\epsilon}{2}\right)} = \prod_{k=1}^{m} \frac{\exp\left(-\frac{|z_k - C_k(x)|\epsilon}{2}\right)}{\exp\left(-\frac{|z_k - C_k(x')|\epsilon}{2}\right)} \\
&= \prod_{k=1}^{m} \exp\left(-\frac{|z_k - C_k(x)|\epsilon}{2} + \frac{|z_k - C_k(x')|\epsilon}{2}\right) \\
&= \prod_{k=1}^{m} \exp\left(\frac{(|z_k - C_k(x')| - |z_k - C_k(x)|)\epsilon}{2}\right) \\
&\leq \prod_{k=1}^{m} \exp\left(\frac{|C_k(x') - C_k(x)|\epsilon}{2}\right) \\
&= \exp\left(\frac{\sum_{k=1}^{m} |C_k(x') - C_k(x)|\epsilon}{2}\right) \\
&= \exp\left(\frac{\|C(x') - C(x)\|_1\epsilon}{2}\right) \leq \exp\left(\frac{2\epsilon}{2}\right) = \exp(\epsilon).
\end{aligned}
$$

□

3.2 Upper bound in the DP setting

Theorem 3.2. Consider a $p \in \mathcal{P}(L, \beta)$, then an upper bound for the MISE of $\hat{p}_n$ is given by

$$
R_{p,n,\epsilon}(\hat{p}) = \mathbb{E}_{pq}[\|\hat{p}_n - p\|_2^2] \leq 8\left(\frac{m}{n\epsilon}\right)^2 + \frac{m}{n} + L^2\left(\frac{1}{m}\right)^{2\beta}.
$$

Here $\mathbb{E}_{pq}$ is understood to be the expectation with respect to Z, where $X \sim p$ and $Z|X = x \sim Q_0(\cdot|x)$.

Proof. First consider the following decomposition of the MISE,

$$
\begin{aligned}
\mathbb{E}_{pq}[\|\hat{p}_n - p\|_2^2] &= \mathbb{E}_{pq}\left[\|\tilde{p}_n + \hat{q}_n - p\|_2^2\right] \\
&= \mathbb{E}_{pq}\left[\|\hat{q}_n\|_2^2 + \|\tilde{p}_n - p\|_2^2 + 2\langle \hat{q}_n, \tilde{p}_n - p\rangle\right] \\
&= \mathbb{E}_{pq}\left[\|\hat{q}_n\|_2^2\right] + \mathbb{E}_{pq}\left[\|\tilde{p}_n - p\|_2^2\right] + 2\mathbb{E}_{pq}\left[\langle \hat{q}_n, \tilde{p}_n - p\rangle\right].
\end{aligned}
$$

Then for the last term in the most recent equation we get,

$$
\begin{aligned}
\mathbb{E}_{pq}\left[\langle \hat{q}_n, \tilde{p}_n - p\rangle\right] &= \mathbb{E}_{pq}\left[\int_{\mathcal{X}} \hat{q}_n(s)(\tilde{p}_n(s) - p(s))ds\right] \\
&= \mathbb{E}_{pq}\left[\int_{\mathcal{X}} m\sum_{k=1}^{m} \frac{W_k}{n}\mathbb{1}_{\Delta_k}(s)(\tilde{p}_n(s) - p(s))ds\right] \\
&= \int_{\mathcal{X}} m\sum_{k=1}^{m} \frac{\mathbb{E}_{pq}[W_k]}{n}\mathbb{1}_{\Delta_k}(s)\mathbb{E}_{pq}\left[(\tilde{p}_n(s) - p(s))\right]ds \\
&= \int_{\mathcal{X}} m\sum_{k=1}^{m} \frac{0}{n}\mathbb{1}_{\Delta_k}(s)\mathbb{E}_{pq}\left[(\tilde{p}_n(s) - p(s))\right]ds = 0. \qquad (3.1)
\end{aligned}
$$

A justification for the exchange of integrals in (3.1) is given in Appendix A.1. Therefore the MISE of $\hat{p}_n$ is given by

$$\mathbb{E}_{pq}[\|\hat{p}_n - p\|_2^2] = \mathbb{E}_{pq}\left[\|\hat{q}_n\|_2^2\right] + \mathbb{E}_{pq}\left[\|\tilde{p}_n - p\|_2^2\right].$$

An upper bound for the second expression was established in Theorem 2.1. The first expression can be written as

$$\begin{aligned}
\mathbb{E}_{pq}\left[\|\hat{q}_n\|_2^2\right] &= \mathbb{E}_{pq}\left[\int_{\mathcal{X}} \left(m\sum_{k=1}^{m} \frac{W_k}{n} \mathbb{1}_{\Delta_k}(s)\right)^2 ds\right] \\
&= \mathbb{E}_{pq}\left[\sum_{j=1}^{m} \int_{\Delta_j} \left(m\sum_{k=1}^{m} \frac{W_k}{n} \mathbb{1}_{\Delta_k}(s)\right)^2 ds\right] \\
&= \mathbb{E}_{pq}\left[\sum_{j=1}^{m} \int_{\Delta_j} \left(m\frac{W_j}{n}\right)^2 ds\right] \\
&= \mathbb{E}_{pq}\left[\sum_{j=1}^{m} \frac{m^2}{n^2} W_j^2 \int_{\Delta_j} ds\right] = \sum_{j=1}^{m} \frac{m}{n^2}\mathbb{E}_{pq}\left[W_j^2\right] \\
&= \sum_{j=1}^{m} \frac{m}{n^2}\frac{8}{\epsilon^2} = 8\left(\frac{m}{n\epsilon}\right)^2.
\end{aligned}$$

Therefore an upper bound for the MISE of $\hat{p}_n$ is given by

$$\mathbb{E}_{pq}[\|\hat{p}_n - p\|_2^2] \leq 8\left(\frac{m}{n\epsilon}\right)^2 + \frac{m}{n} + L^2\left(\frac{1}{m}\right)^{2\beta}.$$

□

To explore the asymptotic behaviour of this expression, the relationship between $\left(\frac{m}{n\epsilon}\right)^2$ and $\frac{m}{n}$ is crucial. Recall from Section 2, the minimax optimal m was given by $m = n^{\frac{1}{2\beta+1}}$, where the expression to bound was $\frac{m}{n} + L^2\left(\frac{1}{m}\right)^{2\beta}$. This m was established by setting $\frac{m}{n} = \left(\frac{1}{m}\right)^{2\beta}$, a natural course of action is therefore setting

$$\begin{aligned}
\left(\frac{m}{n\epsilon}\right)^2 &= \left(\frac{1}{m}\right)^{2\beta} \\
m^2 &= \frac{(n\epsilon)^2}{m^{2\beta}} \\
m &= (n\epsilon)^{\frac{1}{1+\beta}}.
\end{aligned}$$

Now consider these two candidates for m. First let $m = n^{\frac{1}{2\beta+1}}$, which leads to

$$\begin{aligned}
8\left(\frac{m}{n\epsilon}\right)^2 + \frac{m}{n} + L^2\left(\frac{1}{m}\right)^{2\beta} &= 8\left(\frac{n^{\frac{1}{2\beta+1}}}{n\epsilon}\right)^2 + \frac{n^{\frac{1}{2\beta+1}}}{n} + L^2\left(\frac{1}{n^{\frac{1}{2\beta+1}}}\right)^{2\beta} \\
&= \frac{8}{\epsilon^2}n^{-\frac{4\beta}{2\beta+1}} + n^{-\frac{2\beta}{2\beta+1}} + L^2 n^{-\frac{2\beta}{2\beta+1}} \\
&= \frac{8}{\epsilon^2}n^{-\frac{4\beta}{2\beta+1}} + (1+L^2)n^{-\frac{2\beta}{2\beta+1}}.
\end{aligned}$$

To find the dominant term, we compare $n^{-\frac{2\beta}{2\beta+1}}$ and $\frac{1}{\epsilon^2}n^{-\frac{4\beta}{2\beta+1}}$,

$$\begin{aligned}
\frac{1}{\epsilon^2}n^{-\frac{4\beta}{2\beta+1}} &\leq n^{-\frac{2\beta}{2\beta+1}} \\
\frac{1}{\epsilon^2} &\leq n^{-\frac{2\beta}{2\beta+1}}n^{\frac{4\beta}{2\beta+1}} \\
\epsilon^2 &\geq n^{-\frac{2\beta}{2\beta+1}}.
\end{aligned}$$

If we set $m = (n\epsilon)^{\frac{1}{\beta+1}}$ on the other hand, we observe

$$\begin{aligned}
8\left(\frac{m}{n\epsilon}\right)^2 + \frac{m}{n} + L^2\left(\frac{1}{m}\right)^{2\beta} &= 8\left(\frac{(n\epsilon)^{\frac{1}{\beta+1}}}{n\epsilon}\right)^2 + \frac{(n\epsilon)^{\frac{1}{\beta+1}}}{n} + L^2\left(\frac{1}{(n\epsilon)^{\frac{1}{\beta+1}}}\right)^{2\beta} \\
&= 8(n\epsilon)^{-\frac{2\beta}{\beta+1}} + \epsilon^{\frac{1}{\beta+1}}n^{-\frac{\beta}{\beta+1}} + L^2(n\epsilon)^{-\frac{2\beta}{\beta+1}} \\
&= (8+L^2)(n\epsilon)^{-\frac{2\beta}{\beta+1}} + \epsilon^{\frac{1}{\beta+1}}n^{-\frac{\beta}{\beta+1}}.
\end{aligned}$$

Again, the dominant term is found by a comparison between $(n\epsilon)^{-\frac{2\beta}{\beta+1}}$ and $\epsilon^{\frac{1}{\beta+1}}n^{-\frac{\beta}{\beta+1}}$,

$$\begin{aligned}
(n\epsilon)^{-\frac{2\beta}{\beta+1}} &\geq \epsilon^{\frac{1}{\beta+1}}n^{-\frac{\beta}{\beta+1}} \\
\epsilon^{-\frac{2\beta+1}{\beta+1}} &\geq n^{\frac{\beta}{\beta+1}} \\
\epsilon &\leq n^{-\frac{\beta}{2\beta+1}} \\
\epsilon^2 &\leq n^{-\frac{2\beta}{2\beta+1}}.
\end{aligned}$$

This leads to the following observations about the asymptotic behaviour of the MISE of $\hat{p}_n$: If $\epsilon^2 \geq n^{-\frac{2\beta}{2\beta+1}}$, set $m = n^{\frac{1}{2\beta+1}}$ and obtain $R_{p,n,\epsilon}(\hat{p}) = O\left(n^{-\frac{2\beta}{2\beta+1}}\right)$. Otherwise set $m = (n\epsilon)^{\frac{1}{\beta+1}}$ to obtain $R_{p,n,\epsilon}(\hat{p}) = O\left((n\epsilon)^{-\frac{2\beta}{\beta+1}}\right)$. With this, one obtains an upper bound for the asymptotic behaviour of the MISE of $\hat{p}_n$, given by $R_{p,n,\epsilon}(\hat{p}) \leq C \max\left\{(n\epsilon)^{-\frac{2\beta}{\beta+1}}, n^{-\frac{2\beta}{2\beta+1}}\right\}$ for some $C \in (0, \infty)$.

3.3 Lower bound in the DP setting

3.3.1 Reduction in the DP setting

We employ a similar reduction as in Section 2.2.1. Let $\mathcal{E}$ be the set of ϵ-DP estimators. Then the earlier established upper bound for the MISE of $\hat{p}_n$ given by

$$\inf_{\hat{p}\in\mathcal{E}} \sup_{p\in\mathcal{P}(L,\beta)} R_{p,n,\epsilon}(\hat{p}) \leq C\zeta_{n,\epsilon},$$

where $\zeta_{n,\epsilon} := \max\left\{(n\epsilon)^{-\frac{2\beta}{\beta+1}}, n^{-\frac{2\beta}{2\beta+1}}\right\}$ and some constant C. With the same approach as in (2.1) and $\gamma_{n,\epsilon} := \max\left\{(n\epsilon)^{-2}, n^{-\frac{2\beta}{2\beta+1}}\right\}$, we construct a lower bound for the MISE of $\hat{p}_n$ with a c such that

$$\inf_{\hat{p}\in\mathcal{E}} \sup_{p\in\mathcal{P}(L,\beta)} P_{pq}(\|\hat{p}_n - p\|_2^2 \geq u_{n,\epsilon}) \geq c,$$

where $u_{n,\epsilon} := a\gamma_{n,\epsilon}$ for $a > 0$. If

$$\|p_i - p_j\|_2^2 \geq 4u_{n,\epsilon} \text{ for all } i, j \in \{0, 1, \ldots, h\} \text{ and } i \neq j \tag{3.2}$$

then

$$P_{p_j q}(\|\hat{p}_n - p_j\|_2^2 \geq u_{n,\epsilon}) \geq P_{p_j q}(p^* \neq j),\ j \in \{0, 1, \ldots, h\}. \tag{3.3}$$

Here $p^* : \mathcal{Z} \mapsto \{0, 1, \ldots, h\}$ is the minimum distance test, given by

$$p^* = \arg \min_{0 \leq k \leq h} \|\hat{p}_n - p_k\|_2^2.$$

Then proof of inequality (3.3) follows the same structure as the proof of (2.4). For $\{p_0, p_1, \ldots, p_h\}$ that satisfy (3.2), it holds that

$$\inf_{\hat{p} \in \mathcal{E}} \sup_{p \in \{p_0, p_1, \ldots p_h\}} P_{pq}(\|\hat{p}_n - p\|_2^2 \geq u_{n,\epsilon}) \geq \inf_{\tau} \max_{0 \geq j \geq h} P_{p_j q}(\tau \neq j), \tag{3.4}$$

where $\inf_\tau$ is the infimum of all tests and a test is defined as a $\mathcal{F}^n$ measurable function $\tau : \mathcal{Z} \mapsto \{0, 1, \ldots, h\}$. Therefore in order to find a lower bound for the MISE of $\hat{p}_n$, it is sufficient to find a lower bound for $r_h := \inf_\tau \max_{0 \geq j \geq h} P_{p_j q}(\tau \neq j)$.

3.3.2 Lower bound of the MISE

Consider now datasets $X^{(0)}, \ldots, X^{(h)}$, where $X^{(i)} \in \mathcal{X}^n$ for all $i \in \{0, \ldots, h\}$.

Theorem 3.3. (Theorem 6 in Lalanne, Garivier, and Gribonval 2023) If Q is an ϵ-DP privacy channel and $\tau : \mathcal{Z} \mapsto \{0, 1, \ldots, h\}$, then

$$\begin{aligned}\frac{1}{h+1} \sum_{j=0}^{h} Q(\tau \neq j | X^{(j)}) &\geq 1 - \frac{1 + \frac{\epsilon}{(h+1)^2} \sum_{j=0}^{h} \sum_{i=0}^{h} d_{ham}(X^{(i)}, X^{(j)})}{\ln(h+1)} \\ &=: s_\epsilon(X^{(0)}, \ldots, X^{(h)}).\end{aligned}$$

A proof for this theorem is given in Appendix C.1.

Theorem 3.4. (Theorem 5 in Lalanne, Garivier, and Gribonval 2023) Let $Q \in \mathcal{E}$ be a privacy channel. Then for any probability distributions $p_0, p_1, \ldots, p_h$ on $\mathcal{X}^n$ it holds that

$$\inf_\tau \max_{0 \geq j \geq h} P_{p_j q}(\tau \neq j) \geq \sup_{R \in \Pi(P_{p_0}, \ldots, P_{p_h})} \int_{(\mathcal{X}^n)^{(h+1)}} s_\epsilon dR,$$

where $\Pi(P_{p_0}, \ldots, P_{p_h})$ is the set of distributions with $P_{p_0}, \ldots, P_{p_h}$ as their marginal distributions.

Proof. First observe that

$$\begin{aligned}\max_{0 \geq j \geq h} P_{p_j q}(\tau \neq j) &\geq \frac{1}{h+1} \sum_{j=0}^{h} P_{p_j q}(\tau \neq j) \\ &= \int_{(\mathcal{X}^n)^{(h+1)}} \frac{1}{h+1} \sum_{j=0}^{h} Q(\tau \neq j | X^{(j)}) dR,\end{aligned}$$

then with Theorem 3.3

$$\max_{0\geq j\geq h} P_{p_j q}(\tau \neq j) \geq \int_{(\mathcal{X}^n)^{(h+1)}} s_\epsilon dR.$$

$\square$

Theorem 3.5. (Theorem 3 in Lalanne, Garivier, and Gribonval 2023) Let $Q \in \mathcal{E}$ be a privacy channel. Then for any probability distributions $p_0, p_1, \ldots, p_h$ on $\mathcal{X}^n$ and probability measure R with $P_{p_i} \ll R$ for all $i \in \{0, \ldots, h\}$ it holds that

$$\inf_\tau \max_{0\geq j\geq h} P_{p_j q}(\tau \neq j) \geq 1 - \frac{1 + \frac{1}{h+1}\sum_{j=0}^h D_{KL}(P_{p_j}, R)}{\ln(h+1)}.$$

If the probability measures are of the form $P_{p_i}^n = P_{p_i}^{\bigotimes n}$, that is they are n-fold product measures with respect to p_i for all $i \in \{0, \ldots, h\}$, then it holds that

$$\inf_\tau \max_{0\geq j\geq h} P_{p_j q}(\tau \neq j) \geq 1 - \frac{1 + \frac{n\epsilon}{(h+1)^2}\sum_{j=0}^h \sum_{i=0}^h \frac{2\delta(P_{p_i}, P_{p_j})}{1+\delta(P_{p_i}, P_{p_j})}}{\ln(h+1)},$$

where δ is the total variation distance, Definition 6.

A proof is given in Appendix C.2.

Theorem 3.6. Let $L, \beta, \epsilon > 0$, then there exists $c > 0$, such that

$$\liminf_{n\to\infty} \inf_{\hat{p}_n \in \mathcal{E}} \sup_{p\in\mathcal{P}(L,\beta)} \mathbb{E}_{pq}\left(\max\left\{(n\epsilon)^{-\frac{2\beta}{\beta+1}}, n^{-\frac{2\beta}{2\beta+1}}\right\}\|\hat{p}_n - p\|_2^2\right) \geq c.$$

Proof. Consider the construction of PDF alternatives, Section 2.2.3, with $w_n = \left\lceil c_1 \max\left\{(n\epsilon)^{\frac{1}{\beta+1}}, n^{\frac{1}{2\beta+1}}\right\}\right\rceil$, where $c_1 > 0$ and $0 < \lambda < \max\left\{\frac{\epsilon}{L}, \frac{5}{8}\frac{1}{4^\beta}\right\}$. Then we will use Theorem 3.5 with the alternatives $p_{j,n} := p_{\omega^{(j)}}$ for $j \in \{0, 1, \ldots, N\}$, with N as in Theorem 2.9 and proceed by cases.

Case 1: $n^{\frac{1}{2\beta+1}} > (n\epsilon)^{\frac{1}{\beta+1}}$. Similar as in the Proof of assumption a in Theorem 2.10 we conclude that

$$\begin{aligned}\|p_{j,n} - p_{k,n}\|_2^2 &\geq \frac{\lambda^2 L^2}{16}\left(\frac{1}{w_n}\right)^{2\beta}\|K\|_2^2 \\ &\geq \frac{\lambda^2 L^2}{16}(2c_1)^{-2\beta} n^{-\frac{2\beta}{2\beta+1}}\|K\|_2^2 = 4u_{n,\epsilon},\end{aligned}$$

for all $n > n_1$ where $n_1 = \left(\frac{8}{c_1}\right)^{2\beta}$ and $u_{n,\epsilon}$ defined in the paragraph preceding display (3.2), is given by $u_{n,\epsilon} = an^{-\frac{2\beta}{2\beta+1}}$ and $a = \frac{\lambda^2 L^2}{64}(2c_1)^{-2\beta}\|K\|_2^2$. Let $P_{j,n}$ be the probability measure with respect to $p_{j,n}$ for all $j \in \{0, \ldots, N\}$ and let $P_{j,n}^n$ denote the n-fold product measure with respect to $p_{j,n}$ for all $j \in \{0, \ldots, N\}$, then according to Theorem 3.5 and the fact that $P_{j,n}^n \ll P_{0,n}^n$ for all $j \in \{0, \ldots, N\}$,

$$\max_{0\geq j\geq N} P_{j,nq}(\tau \neq j) \geq 1 - \frac{1 + \frac{1}{N+1}\sum_{j=0}^N D_{KL}(P_{j,n}^n, P_{0,n}^n)}{\ln(N+1)},$$

then with (2.8)

$$\geq 1 - \frac{1 + \frac{1}{N+1}\sum_{j=0}^{N}\frac{\lambda^2 L^2}{2} c_1^{-(2\beta+1)} n^{\frac{1}{2\beta+1}} \|K\|_2^2}{\ln(N+1)}.$$

Now setting $c_1 = \left(\frac{\lambda^2 L^2 \|K\|_2^2}{2}\right)^{\frac{1}{2\beta+1}}$ and defining n_2 as the smallest n satisfying $1 + n^{\frac{1}{2\beta+1}} < \ln(N+1)$ provides

$$\max_{0\geq j\geq N} P_{j,nq}(\tau \neq j) \geq 1 - \frac{1 + n^{\frac{1}{2\beta+1}}}{\ln(N+1)} > 0,$$

for all $n > \max\{n_1, n_2\}$.

Case 2: $(n\epsilon)^{\frac{1}{\beta+1}} \geq n^{\frac{1}{2\beta+1}}$. With a similar argumentation as in Case 1 we arrive at

$$\begin{aligned}
\|p_{j,n} - p_{k,n}\|_2^2 &\geq \frac{\lambda^2 L^2}{16}\left(\frac{1}{w_n}\right)^{2\beta} \|K\|_2^2 \\
&\geq \frac{\lambda^2 L^2}{16}(2c_1)^{-2\beta}(n\epsilon)^{-\frac{2\beta}{\beta+1}}\|K\|_2^2 = 4u_{n,\epsilon},
\end{aligned}$$

for all $n \geq n_3 = \left(\frac{8}{\epsilon^{\frac{1}{\beta}} c_1}\right)^{\beta+1}$, where $u_{n,\epsilon}$, defined in the paragraph preceding display (3.2), is given by $u_{n,\epsilon} = a(n\epsilon)^{-\frac{2\beta}{\beta+1}}$ and $a = \frac{\lambda^2 L^2}{64}(2c_1)^{-2\beta}\|K\|_2^2$. Then again with Theorem 3.5 we get

$$\max_{0\geq j\geq N} P_{j,nq}(\tau \neq j) \geq 1 - \frac{1 + \frac{n\epsilon}{N+1^2}\sum_{j=1}^{N+1}\sum_{i=1}^{N+1}\frac{2\delta(P_{i,n},P_{j,n})}{1+\delta(P_{i,n},P_{j,n})}}{\ln N + 1}.$$

Now consider the Total variation distance between $P_{i,n}$ and $P_{j,n}$,

$$\begin{aligned}
\delta\left(P_{i,n}, P_{j,n}\right) &= \frac{1}{2}\int |p_{i,n}(x) - p_{j,n}(x)|\, dx \\
&= \frac{1}{2}\int \left|\sum_{k=1}^{w_n}\omega_k^{(i)}\phi_k(x,\lambda) - \sum_{k=1}^{w_n}\omega_k^{(j)}\phi_k(x,\lambda)\right| dx \\
&= \frac{1}{2}\int \left|\sum_{k=1}^{w_n}\left(\omega_k^{(i)} - \omega_k^{(j)}\right)\phi_k(x,\lambda)\right| dx \leq \frac{1}{2}\int \left|\sum_{k=1}^{w_n}\phi_k(x,\lambda)\right| dx \\
&= w_n \int_{\Delta_{+,1}} \phi_1(x,\lambda)dx = w_n \int_0^1 \frac{1}{4w_n}\lambda L \left(\frac{1}{w_n}\right)^{\beta} K(u)du \\
&\leq \frac{\lambda L}{8}\left(\frac{1}{w_n}\right)^{\beta}.
\end{aligned}$$

Therefore

$$\max_{0\geq j\geq N} P_{j,nq}(\tau\neq j) \geq 1-\frac{1+\frac{n\epsilon}{N+1^2}\sum_{j=1}^{N+1}\sum_{i=1}^{N+1}\frac{2\delta(P_{i,n},P_{j,n})}{1+\delta(P_{i,n},P_{j,n})}}{\ln(N+1)}$$
$$\geq 1-\frac{1+\frac{n\epsilon}{N+1^2}\sum_{j=1}^{N+1}\sum_{i=1}^{N+1}\frac{\frac{\lambda L}{4}\left(\frac{1}{w_n}\right)^\beta}{1+\frac{\lambda L}{8}\left(\frac{1}{w_n}\right)^\beta}}{\ln(N+1)}$$
$$\geq 1-\frac{1+n\epsilon\frac{\frac{\lambda L}{4}c_1^{-\beta}(n\epsilon)^{-\frac{\beta}{\beta+1}}}{1+\frac{\lambda L}{8}c_1^{-\beta}(n\epsilon)^{-\frac{\beta}{\beta+1}}}}{\ln(N+1)} = 1-\frac{1+\frac{\frac{\lambda L}{4}c_1^{-\beta}(n\epsilon)^{\frac{1}{\beta+1}}}{1+\frac{\lambda L}{8}c_1^{-\beta}(n\epsilon)^{-\frac{\beta}{\beta+1}}}}{\ln(N+1)}.$$

Setting $c_1 = \left(\frac{\lambda L}{4}\right)^\beta$ leads to

$$\max_{0\geq j\geq N} P_{j,nq}(\tau\neq j) \geq 1-\frac{1+\frac{(n\epsilon)^{\frac{1}{\beta+1}}}{1+\frac{1}{2}(n\epsilon)^{-\frac{\beta}{\beta+1}}}}{\ln(N+1)} \geq 1-\frac{1+(n\epsilon)^{\frac{1}{\beta+1}}}{\ln(N+1)} > 0,$$

for all $n > n_4$, where n_4 is defined as the smallest n satisfying $1+(n\epsilon)^{\frac{1}{\beta+1}} < \ln(N+1)$ provides. Then the claim follows from (3.4). □

Taking this lower bound, and the upper bound from Section 3.2, we get

$$C \geq \inf_{\tilde{p}} \sup_{p\in\mathcal{P}(L,\beta)} \max\left\{(n\epsilon)^{\frac{2\beta}{\beta+1}}, n^{\frac{2\beta}{2\beta+1}}\right\} R_{p,n,\epsilon}(\hat{p}) \geq c,$$

for all $n \geq n_0$, where $n_0 = \max\{n_1, n_2, n_3, n_4\}$ and for some constants $c > 0$ and $C < \infty$. Therefore $\max\left\{(n\epsilon)^{-\frac{2\beta}{\beta+1}}, n^{-\frac{2\beta}{2\beta+1}}\right\}$ is the rate of convergence of the MISE of $\hat{p}_n$.

References

Dwork, Cynthia (2006). "Differential privacy". In: *International colloquium on automata, languages, and programming.* Springer, pp. 1–12.

Dwork, Cynthia, Frank McSherry, Kobbi Nissim, and Adam Smith (2006). "Calibrating noise to sensitivity in private data analysis". In: *Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3.* Springer, pp. 265–284.

Gambs, Sébastien, Marc-Olivier Killijian, and Miguel Núñez del Prado Cortez (2014). "De-anonymization attack on geolocated data". In: *Journal of Computer and System Sciences* 80.8, pp. 1597–1614.

Giraud, Christophe (2021). *Introduction to high-dimensional statistics.* CRC Press.

Kooiman, Peter (1997). "PRAM: A method for disclosure limitation of microdata". In: *Report, Department of Statistical Methods.*

Lalanne, Clément, Aurélien Garivier, and Rémi Gribonval (2023). *On the Statistical Complexity of Estimation and Testing under Privacy Constraints.* arXiv: 2210.02215 [cs.LG].

Li, Ninghui, Tiancheng Li, and Suresh Venkatasubramanian (2006). "t-closeness: Privacy beyond k-anonymity and l-diversity". In: *2007 IEEE 23rd international conference on data engineering*. IEEE, pp. 106–115.

Malin, Bradley and Latanya Sweeney (2004). "How (not) to protect genomic data privacy in a distributed network: using trail re-identification to evaluate and design anonymity protection systems". In: *Journal of biomedical informatics* 37.3, pp. 179–192.

Narayanan, Arvind and Vitaly Shmatikov (2008). "Robust de-anonymization of large sparse datasets". In: *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, pp. 111–125.

Sweeney, Latanya (2002). "k-anonymity: A model for protecting privacy". In: *International journal of uncertainty, fuzziness and knowledge-based systems* 10.05, pp. 557–570.

Tsybakov, Alexandre B. (2009). *Introduction to Nonparametric Estimation*. Springer Series in Statistics. New York: Springer. DOI: 10.1007/b13794.

Van Erven, Tim and Peter Harremos (2014). "Rényi divergence and Kullback-Leibler divergence". In: *IEEE Transactions on Information Theory* 60.7, pp. 3797–3820.

A Appendix: Auxiliary results of Section 2

A.1 Justification for the exchange of integrals

In Equation (3.1), the following exchange of integrals takes place,

$$\begin{aligned}&\mathbb{E}_{pq}\left[\int_{\mathcal{X}} m \sum_{k=1}^{m} \frac{W_k}{n} \mathbb{1}_{\Delta_k}(s)(\tilde{p}_n(s) - p(s))ds\right] \\ &= \int_{\mathcal{X}} m \sum_{k=1}^{m} \frac{\mathbb{E}_{pq}\left[W_k\right]}{n} \mathbb{1}_{\Delta_k}(s)\mathbb{E}_{pq}\left[(\tilde{p}_n(s) - p(s))\right] ds.\end{aligned}$$

To ensure the validity of this step, we have to check if the expression is absolutely integrable and that W_k and $\hat{p}_n$ are stochastically independent. The independence of W_k and $\hat{p}_n$ is obvious, as W_k is a random variable from a Lap$(\frac{\epsilon}{2})$ and $\hat{p}_n$ is based on $X_1, \dots, X_n$. Therefore

$$\begin{aligned}&\mathbb{E}_{pq}\left[\int_{\mathcal{X}} \left| m \sum_{k=1}^{m} \frac{W_k}{n} \mathbb{1}_{\Delta_k}(s)(\tilde{p}_n(s) - p(s))\right| ds\right] \\ &\leq \mathbb{E}_{pq}\left[\sum_{j=1}^{m} \int_{\Delta_j} \left| m \sum_{k=1}^{m} \frac{W_k}{n} \mathbb{1}_{\Delta_k}(s)\right| \left|\tilde{p}_n(s) - p(s)\right| ds\right] \\ &= \mathbb{E}_{pq}\left[\sum_{j=1}^{m} \int_{\Delta_j} \left|\frac{m}{n} W_j\right| \left|\tilde{p}_n(s) - p(s)\right| ds\right] \\ &= \mathbb{E}_{pq}\left[\sum_{j=1}^{m} \left|\frac{m}{n} W_j\right| \int_{\Delta_j} \left|\tilde{p}_n(s) - p(s)\right| ds\right].\end{aligned}$$

We will consider the last term inside the expected value separately,

$$\begin{aligned}\int_{\Delta_j} \left|\tilde{p}_n(s) - p(s)\right| ds &= \int_{\Delta_j} \left|\frac{m}{n} \sum_{k=1}^{m} C_k \mathbb{1}_{\Delta_k}(s) - p(s)\right| ds = \int_{\Delta_j} \left|\frac{m}{n} C_j - p(s)\right| ds \\ &\leq \int_{\Delta_j} \left|\frac{m}{n} C_j\right| + |p(s)|\, ds \leq \int_{\Delta_j} |m| + |p(s)|\, ds \\ &= \int_{\Delta_j} m + p(s) ds \leq 2.\end{aligned}$$

With this result, the expected value can now be bounded by

$$\begin{aligned}&\mathbb{E}_{pq}\left[\int_{\mathcal{X}} \left| m \sum_{k=1}^{m} \frac{W_k}{n} \mathbb{1}_{\Delta_k}(s)(\tilde{p}_n(s) - p(s))\right| ds\right] \leq \mathbb{E}_{pq}\left[\sum_{j=1}^{m} \left|\frac{m}{n} W_j\right| 2\right] \\ &= \mathbb{E}_{pq}\left[\frac{2m^2}{n} |W_j|\right] = \frac{2m^2}{n} \mathbb{E}_{pq}\left[|W_j|\right] = \frac{2m^2}{n} \frac{\epsilon}{2} = \frac{m^2 \epsilon}{n} < \infty.\end{aligned}$$

The exchange of integrals is therefore justified.

A.2 Hoeffding's lemma

Lemma A.1. For any random variable Y with $a \leq Y \leq b$ almost surely, we have

$$\mathbb{E}\left[\exp\left(\alpha Y\right)\right] \leq \exp\left(\alpha \mathbb{E}[Y] + \frac{\alpha^2 (b-a)^2}{8}\right),$$

with $\alpha \in \mathbb{R}$. This is known as Hoeffding's lemma.

Proof. First observe that the inequality can be restated as

$$\mathbb{E}\left[\exp\left(\alpha(Y - \mathbb{E}[Y])\right)\right] \leq \exp\left(\frac{\alpha^2 (b-a)^2}{8}\right).$$

Therefore, for the variable $\tilde{Y} = Y - \mathbb{E}[Y]$ is holds that $\mathbb{E}[\tilde{Y}] = 0$. So without loss of generality, we can assume that $\mathbb{E}[Y] = 0$. Because of the convexity of $f(x) = \exp\left(\alpha x\right)$ we have

$$\exp\left(\alpha x\right) \leq \frac{b-x}{b-a}\exp\left(\alpha a\right) + \frac{x-a}{b-a}\exp\left(\alpha b\right),$$

for all $x \in [a, b]$. Therefore

$$\begin{aligned}\mathbb{E}[\exp\left(\alpha Y\right)] &\leq \frac{b - \mathbb{E}[Y]}{b-a}\exp\left(\alpha a\right) + \frac{\mathbb{E}[Y] - a}{b-a}\exp\left(\alpha b\right) \\ &= \frac{b}{b-a}\exp\left(\alpha a\right) + \frac{-a}{b-a}\exp\left(\alpha b\right) = \exp\left(g\left(\alpha(b-a)\right)\right),\end{aligned}$$

where $g(u) = \frac{ua}{b-a} + \ln\left(1 + \frac{a(1-\exp\left(u\right))}{b-a}\right)$. Then for the function g we have

- $g(0) = \ln(1) = 0$,
- $g'(u) = \frac{a}{b-a} + \frac{-\frac{\exp(u)a}{b-a}}{1+\frac{a-\exp(u)a}{b-a}} = \frac{a}{b-a} - \frac{\exp(u)a}{b-a\exp(u)}$,
- $g'(0) = 0$ and
- $g''(u) = -\frac{\exp(u)ab}{(b-a\exp(u))^2}$.

The fact that $\mathbb{E}[Y] = 0$ implies that $a \leq 0 \leq b$ and therefore

$$g''(u) = -\frac{\exp(u)ab}{(b-a\exp(u))^2} \leq \frac{1}{4},$$

which follows from the AM-GM inequality, because

$$\begin{aligned} &-\frac{\exp(u)ab}{(b-a\exp(u))^2} \leq \frac{1}{4} \\ \iff &-\exp(u)ab \leq \frac{(b-a\exp(u))^2}{4} \\ \iff &\sqrt{-\exp(u)ab} \leq \frac{b-a\exp(u)}{2}.\end{aligned}$$

Then, by Taylor's theorem, there exists a $\theta \in [0, 1]$ such that

$$g(u) = g(0) + ug'(0) + \frac{1}{2}u^2 g''(u\theta) = \frac{1}{2}u^2 g''(u\theta) \leq \frac{u^2}{8}.$$

Therefore

$$\mathbb{E}\left[\exp\left(\alpha Y\right)\right] \leq \exp\left(g\left(\alpha(b-a)\right)\right) \leq \exp\left(\frac{\alpha^2(b-a)^2}{8}\right).$$

□

A.3 Hoeffding's inequality

Lemma A.2. (Lemma 2.8 in Tsybakov 2009) For independent random variables $Y_1, \dots, Y_n$ with $a_i \leq Y_i \leq b_i$ for all $i \in \{1, \dots, n\}$, then

$$P\left(\sum_{i=1}^{n}(Y_i - \mathbb{E}[Y_i]) \geq t\right) \leq \exp\left(-\frac{2t^2}{\sum_{i=1}^{n}(b_i - a_i)^2}\right),$$

for all $t \in (0, \infty)$. This is known as Hoeffding's inequality.

Proof. First consider $s \in (0, \infty)$ and

$$\begin{aligned} P\left(\sum_{i=1}^{n}(Y_i - \mathbb{E}[Y_i]) \geq t\right) &= P\left(\exp\left(s\sum_{i=1}^{n}(Y_i - \mathbb{E}[Y_i])\right) \geq \exp(st)\right) \\ &\leq \frac{\mathbb{E}[\exp\left(s\sum_{i=1}^{n}(Y_i - \mathbb{E}[Y_i])\right)]}{\exp(st)}, \end{aligned}$$

with Markov's inequality. Further

$$\begin{aligned} P\left(\sum_{i=1}^{n}(Y_i - \mathbb{E}[Y_i]) \geq t\right) &\leq \frac{\prod_{i=1}^{n}\mathbb{E}[\exp\left(s(Y_i - \mathbb{E}[Y_i])\right)]}{\exp(st)} \\ &\leq \frac{\prod_{i=1}^{n}\exp\left(s^2\frac{(b_i-a_i)^2}{8}\right)}{\exp(st)}, \end{aligned}$$

where Hoeffding's lemma (A.1) was used. Finally

$$P\left(\sum_{i=1}^{n}(Y_i - \mathbb{E}[Y_i]) \geq t\right) \leq \exp\left(\frac{s^2\sum_{i=1}^{n}(b_i - a_i)^2}{8} - st\right).$$

Now consider the function $f(s) = \frac{s^2\sum_{i=1}^{n}(b_i-a_i)^2}{8} - st$. Then for the first and second derivatives of f it holds that $f'(s) = \frac{2s\sum_{i=1}^{n}(b_i-a_i)^2}{8} - t$ and $f''(s) = \frac{2\sum_{i=1}^{n}(b_i-a_i)^2}{8} \geq 0$ for all $s \in \mathbb{R}$. Setting the first derivative equal to 0 results in $s_{min} = \frac{4t}{\sum_{i=1}^{n}(b_i-a_i)^2}$, and therefore

$$\begin{aligned} P\left(\sum_{i=1}^{n}(Y_i - \mathbb{E}[Y_i]) \geq t\right) &\leq \exp\left(\frac{\frac{(4t)^2\sum_{i=1}^{n}(b_i-a_i)^2}{(\sum_{i=1}^{n}(b_i-a_i)^2)^2}}{8} - \frac{4t^2}{\sum_{i=1}^{n}(b_i - a_i)^2}\right) \\ &= \exp\left(-\frac{2t^2}{\sum_{i=1}^{n}(b_i - a_i)^2}\right). \end{aligned}$$

□

B Appendix: Proofs of Section 2

B.1 Proof of Theorem 2.9

Proof. First consider the set $\Omega_1 := \{\omega \in \Omega : d_{ham}(\omega, \omega^{(0)}) > \lfloor \frac{n}{8} \rfloor\}$, a subset of Ω without all ω in a $\lfloor \frac{n}{8} \rfloor$-neighbourhood around $\omega^{(0)}$. Now consider a $\omega^{(1)} \in \Omega_1$ and construct $\Omega_2 := \{\omega \in \Omega_1 : d_{ham}(\omega, \omega^{(1)}) > \lfloor \frac{n}{8} \rfloor\}$. We continue in this fashion to define

$$\Omega_i := \{\omega \in \Omega_{i-1} : d_{ham}(\omega, \omega^{(i-1)}) > \left\lfloor \frac{n}{8} \right\rfloor\},$$

for all $i \in \{1, \dots, N\}$ and take $\Omega_0 := \Omega$. This procedure generates the set $D := \{\omega^{(0)}, \dots, \omega^{(N)}\}$, under the restriction that N is the smallest natural number that satisfies $\Omega_{N+1} = \varnothing$. Define

$$A_i := \{\omega \in \Omega_i : d_{ham}(\omega, \omega^{(i)}) \leq \left\lfloor \frac{n}{8} \right\rfloor\},$$

for all $i \in \{0, \dots, N\}$. A_i is then the set of $\omega \in \Omega$ that where removed in the construction of Ω_i. Observe that the A_i are pairwise disjoint and $\bigcup_{i=0}^{N} A_i = \Omega$. Further define $a_i := |A_i|$. As A_i contains the $\omega \in \Omega_i$ which have a Hamming distance to $\omega^{(i)}$ of at most $\lfloor \frac{n}{8} \rfloor$, the size of this set can be bounded by the sum of all $\omega \in \Omega$ which have a Hamming distance of $0, 1, \dots, \lfloor \frac{n}{8} \rfloor$, therefore

$$a_i \leq \sum_{j=0}^{\lfloor \frac{n}{8} \rfloor} \binom{n}{j},$$

for all $i \in \{0, \dots, N\}$. Now since $\sum_{i=0}^{N} a_i = |\Omega| = 2^n$, we can bound

$$(N+1) \sum_{j=0}^{\lfloor \frac{n}{8} \rfloor} \binom{n}{j} \geq 2^n,$$

or equivalently

$$N + 1 \geq \frac{2^n}{\sum_{j=0}^{\lfloor \frac{n}{8} \rfloor} \binom{n}{j}}.$$

The right-hand side term is therefore

$$\frac{2^n}{\sum_{j=0}^{\lfloor \frac{n}{8} \rfloor} \binom{n}{j}} =: \frac{1}{q^*},$$

where $q^* = P(Z < \lfloor \frac{n}{8} \rfloor)$ and $Z \sim \text{Binom}\left(n, \frac{1}{2}\right)$. Evidently we have that $Z = \sum_{i=1}^{n} Z_i$, where $Z_1, \dots, Z_n$ are independent and identically distributed Bernoulli($\frac{1}{2}$) random variables. With Hoeffding's inequality (Lemma A.2) and the fact that $\mathbb{E}[Z_i] = \frac{1}{2}$ and $0 \leq Z_i \leq 1$ for all $i \in \{1, \dots, n\}$ it holds that

$$\begin{aligned} q^* &= P\left(\sum_{i=1}^{n} Z_i \leq \left\lfloor \frac{n}{8} \right\rfloor\right) = P\left(\sum_{i=1}^{n} Z_i - \frac{n}{2} \leq \left\lfloor \frac{n}{8} \right\rfloor - \frac{n}{2}\right) \\ &\leq P\left(\sum_{i=1}^{n} (Z_i - \mathbb{E}[Z_i]) \leq \frac{-3n}{8}\right), \end{aligned}$$

then, with the symmetry of $Z_i - \mathbb{E}[Z_i]$ for all $i \in \{1, \dots, n\}$,

$$q^* \leq P\left(\sum_{i=1}^{n}(Z_i - \mathbb{E}[Z_i]) \geq \frac{3n}{8}\right) \leq \exp\left(-\frac{2\frac{9n^2}{64}}{n}\right) = \exp\left(-\frac{9n}{32}\right) < 2^{-\frac{n}{4}}.$$

Therefore

$$N + 1 \geq \frac{1}{q^*} \geq 2^{\frac{n}{4}} \geq 2^{\frac{n}{8}} + 1,$$

for $n \geq 8$. The claim follows with this and the observation that

$$d_{ham}(\omega^{(i)}, \omega^{(j)}) \geq \left\lfloor \frac{n}{8} \right\rfloor + 1 \geq \frac{n}{8},$$

for all $\omega^{(i)}, \omega^{(j)} \in D$ with $i \neq j$. ☐

B.2 Pinsker's inequality

To prove Lemma 2.4 (second Pinsker's inequality), we first introduce the total variation distance.

Definition 6. Consider the measurable space $(\mathcal{X}, \mathcal{F})$, then the total variation distance between two probability measures P and Q on this measurable space has the following definition:

$$\delta(P, Q) = \sup_{A \in \mathcal{F}} |P(A) - Q(A)|.$$

Lemma B.1. (Lemma 2.1 in Tsybakov 2009) Scheffé's theorem states that

$$\delta(P, Q) = \frac{1}{2}\int |p - q| d\mu,$$

where μ is a σ-finite probability measure on $(\mathcal{X}, \mathcal{F})$ with $P \ll \mu$ and $Q \ll \mu$. Further $p := \frac{dP}{d\mu}$ and $q := \frac{dQ}{d\mu}$.

Proof. First observe that we can rewrite the total variation distance in terms of p and q, $\delta(P, Q) = \sup_{A \in \mathcal{F}} \left|\int_A (p - q) d\mu\right|$. Then define $B := \{x \in \mathcal{X} : q(x) \geq p(x)\}$. Now consider

$$\delta(P, Q) \geq Q(B) - P(B) = \int_B (q - p) d\mu = \frac{1}{2}\int |p - q| d\mu.$$

To prove the inequality in the other direction first let $A \in \mathcal{F}$, then

$$\begin{aligned}\left|\int_A (q - p) d\mu\right| &= \left|\int_{A \cap B} (q - p) d\mu + \int_{A \cap B^c} (q - p) d\mu\right| \\ &\leq \max\left\{\int_B (q - p) d\mu, \int_{B^c} (p - q) d\mu\right\} = \frac{1}{2}\int |p - q| d\mu.\end{aligned}$$

☐

Lemma B.2. (Lemma 2.5 in Tsybakov 2009) The first Pinsker's inequality states

$$\delta(P, Q) \leq \sqrt{\frac{D_{KL}(P, Q)}{2}}$$

Proof. First consider the function $\xi(x) := x \ln x - x + 1$ for all non-negative x. Further define $0 \ln 0 := 0$. Then the following holds:

- $\xi(0) = 1$,
- $\xi(1) = 0$,
- $\xi'(x) = \ln x$,
- $\xi'(1) = 0$ and
- $\xi''(x) = \frac{1}{x} \geq 0$ for all $x \in (0, \infty)$.

Therefore $\xi(x) \geq 0$ for all $x \in (0, \infty)$. Now consider the function $\psi(x) := (x-1)^2 - \left(\frac{4}{3} + \frac{2}{3}x\right)\xi(x)$. Then for ψ it holds that:

- $\psi(0) = 1 - \frac{4}{3} = -\frac{1}{3} \leq 0$,
- $\psi(1) = -2\xi(1) = 0$,
- $\psi'(x) = 2x - 2 - \frac{2}{3}\xi(x) - \left(\frac{4}{3} + \frac{2}{3}x\right)\xi'(x)$,
- $\psi'(1) = 0$ and
- $\psi''(x) = 2 - \frac{4}{3}\xi'(x) - \left(\frac{4}{3} + \frac{2}{3}x\right)\xi''(x) = -\frac{4\xi(x)}{3x} \leq 0$ for all $x \in (0, \infty)$.

Then, by Taylor's theorem, there exists a $\theta > 0$ with $|\theta - 1| < |x - 1|$ such that

$$\psi(x) = \psi(1) + \psi'(1)(x-1) + \frac{\psi''(\theta)}{2}(x-1)^2 = -\frac{4\xi(\theta)}{3\theta}(x-1)^2 \leq 0,$$

for all $x \in (0, \infty)$. With this we have shown that

$$(x-1)^2 \leq \left(\frac{4}{3} + \frac{2}{3}x\right)\xi(x), \tag{B.1}$$

for all $x \in [0, \infty)$. Now for the main statement of the lemma. In the case where P is not absolutely continuous with respect to Q, the inequality obviously holds. If $P \ll Q$ on the other hand, then with Scheffé's Theorem (Lemma B.1), we get

$$\delta(P, Q) = \frac{1}{2}\int |p - q| d\mu = \frac{1}{2}\int_{q>0} q \left|\frac{p}{q} - 1\right| d\mu,$$

then with (B.1) it follows that

$$\begin{aligned}
\delta(P, Q) &\leq \frac{1}{2}\int_{q>0} q\sqrt{\left(\frac{4}{3} + \frac{2p}{3q}\right)\xi\left(\frac{p}{q}\right)} d\mu \\
&\leq \frac{1}{2}\sqrt{\int \left(\frac{4q}{3} + \frac{2p}{3}\right) d\mu}\sqrt{\int_{q>0} q\xi\left(\frac{p}{q}\right) d\mu} \\
&= \sqrt{\frac{1}{2}\int_{pq>0} p \ln \frac{p}{q} d\mu} = \sqrt{\frac{D_{KL}}{2}},
\end{aligned}$$

where the Cauchy–Schwarz inequality was used in the last inequality. $\square$

Lemma B.3. (Lemma 2.2 in Tsybakov 2009) If $P \ll Q$, then

$$-\int \min\left\{0, \ln \frac{dP}{dQ}\right\} dP = -\int_{pq>0} p \min\left\{0, \ln \frac{p}{q}\right\} d\mu \leq \delta(P,Q),$$

where μ is a σ-finite measure such that $P \ll \mu$ and $Q \ll \mu$. Further $p := \frac{dP}{d\mu}$ and $q := \frac{dQ}{d\mu}$.

Proof. First observe that from the fact that $P \ll Q$, it follows that

$$\begin{aligned} P_p(\{pq > 0\}) &= 1 - P_p(\{pq = 0\}) = 1 - P_p(\{p = 0\} \cup \{q = 0\}) \\ &\geq 1 - (P_p(\{p = 0\}) + P_p(\{q = 0\})) = 1. \end{aligned}$$

Therefore we have

$$\begin{aligned} -\int \min\left\{0, \ln \frac{dP}{dQ}\right\} dP &= -\int_{p>0} \min\left\{0, \ln \frac{dP}{dQ}\right\} dP \\ &= -\int_{pq>0} \min\left\{0, \ln \frac{dP}{dQ}\right\} dP \\ &= -\int_{pq>0} p \min\left\{0, \ln \frac{p}{q}\right\} d\mu. \end{aligned}$$

Now define $B_1 := \{q \geq p > 0\}$, then

$$\begin{aligned} -\int_{pq>0} p \min\left\{0, \ln \frac{p}{q}\right\} d\mu &= \int_{pq>0} p \max\left\{0, \ln \frac{q}{p}\right\} d\mu \\ &= \int_{B_1} p \max\left\{0, \ln \frac{q}{p}\right\} d\mu = \int_{B_1} p \ln \frac{q}{p} d\mu \\ &\leq \int_{B_1} (q - p) d\mu = Q(B_1) - P(B_1) \leq \delta(P,Q). \end{aligned}$$

□

Now recall the statement of Lemma 2.4, if $P \ll Q$, then

$$\int \max\left\{0, \ln \frac{dP}{dQ}\right\} dP \leq D_{KL}(P,Q) + \sqrt{\frac{D_{KL}(P,Q)}{2}}.$$

Proof.

$$\begin{aligned} \int \max\left\{0, \ln \frac{dP}{dQ}\right\} dP &= \int_{pq>0} p \max\left\{0, \ln \frac{p}{q}\right\} d\mu \\ &= \int_{pq>0} p \max\left\{0, \ln \frac{p}{q}\right\} d\mu + \int_{pq>0} p \min\left\{0, \ln \frac{p}{q}\right\} d\mu \\ &\qquad - \int_{pq>0} p \min\left\{0, \ln \frac{p}{q}\right\} d\mu \\ &= D_{KL}(P,Q) - \int_{pq>0} p \min\left\{0, \ln \frac{p}{q}\right\} d\mu \\ &\leq D_{KL}(P,Q) + \delta(P,Q), \end{aligned}$$

with Lemma B.3. Finally

$$\int \max\left\{0, \ln\frac{dP}{dQ}\right\} dP \leq D_{KL}(P,Q) + \sqrt{\frac{D_{KL}(P,Q)}{2}},$$

where Lemma B.2 was used in the last inequality. $\square$

Definition 7. The $\mathcal{X}^2$ divergence between two probability measures P and Q is defined by

$$\mathcal{X}^2(P,Q) := \begin{cases} \int \left(\frac{dP}{dQ} - 1\right)^2 dQ, & if P \ll Q, \\ +\infty, & otherwise. \end{cases}$$

Lemma B.4. (Lemma 2.7 in Tsybakov 2009) If $P \ll Q$, then

$$D_{KL}(P,Q) \leq \mathcal{X}^2(P,Q).$$

Proof. First consider $\xi(x) := x\ln x - x + 1$ and observe that

$$0 \leq \int_0^1 \frac{t}{t + (1-t)x} dt \leq 1,$$

for all $x \geq 0$. Then

$$\begin{aligned} (x-1)^2 &\geq (x-1)^2 \int_0^1 \frac{t}{t+(1-t)x} dt \\ &= (x-1)^2 \left[\frac{-x\ln((1-x)t + x) - (x-1)t}{(x-1)^2}\right]_{t=0}^{t=1} \\ &= x\ln x - x + 1 = \xi(x), \end{aligned} \tag{B.2}$$

for all $x \in (0,1) \cup (1,\infty)$. Now consider

$$\begin{aligned} \mathcal{X}^2(P,Q) &= \int \left(\frac{dP}{dQ} - 1\right)^2 dQ \\ &= \int_{\frac{dP}{dQ}>0} \left(\frac{dP}{dQ} - 1\right)^2 dQ + \int_{\frac{dP}{dQ}=0} \left(\frac{dP}{dQ} - 1\right)^2 dQ \\ &= \int_{\frac{dP}{dQ}>0} \left(\frac{dP}{dQ} - 1\right)^2 dQ, \end{aligned}$$

where the second term is equal to 0 because of the absolute continuity of P with respect to Q. Then proceed by cases. Case 1: $\frac{dP}{dQ} = 1$.

$$\mathcal{X}^2(P,Q) = \int \left(\frac{dP}{dQ} - 1\right)^2 dQ = 0 = \int \ln\frac{dP}{dQ} dP = D_{KL}(P,Q).$$

Case 2: $\frac{dP}{dQ} \in (0,1) \cup (1,\infty)$. Consider the integral of (B.2) with respect to Q and with $x = \frac{dP}{dQ}$, then

$$\begin{aligned} \mathcal{X}^2(P,Q) &= \int \left(\frac{dP}{dQ} - 1\right)^2 dQ \geq \int \left(\frac{dP}{dQ}\ln\frac{dP}{dQ} - \frac{dP}{dQ} + 1\right) dQ \\ &= \int \ln\frac{dP}{dQ} dP = D_{KL}(P,Q). \end{aligned}$$

$\square$

C Appendix: Proofs and auxiliary results of Section 3

Lemma C.1. (Lemma 6 in Lalanne, Garivier, and Gribonval 2023) If a privacy channel Q is ϵ-DP, then for all $x, x' \in \mathcal{X}^n$ it holds that

$$D_{KL}(Q(\cdot|x), Q(\cdot|x')) \leq \epsilon d_{ham}(x, x').$$

Lemma C.2. (Theorem 3.1 in Giraud 2021) Consider probability measures $P_0, P_1, P_2, \ldots, P_h$ on $(\mathcal{X}^n, \mathcal{F}^n)$. Then for any probability measure R with $P_j \ll R$ for all $j \in \{0, \ldots, h\}$ and any test τ

$$\frac{1}{h+1}\sum_{j=0}^{h} P_j(\tau \neq j) \geq 1 - \frac{1 + \frac{1}{h+1}\sum_{j=0}^{h} D_{KL}(P_j, R)}{\ln(h+1)}.$$

This is known as Fano's Lemma.

Lemma C.3. (Lemma 10 in Lalanne, Garivier, and Gribonval 2023) Consider a privacy channel Q and probability measures $P_0, P_1, P_2, \ldots, P_h$, then

$$\inf_{\tau}\sum_{j=0}^{h} P_{p_j q}(\tau \neq j) \geq \inf_{\tau}\sum_{j=0}^{h} P_{p_j}(\tau \neq j).$$

Lemma C.4. (Lemma 2 in Lalanne, Garivier, and Gribonval 2023) Consider n-fold product probability measures $P_0^n = P_0^{\bigotimes n}, P_1^n = P_1^{\bigotimes n}, \ldots, P_h^n = P_h^{\bigotimes n}$ and a coupling $R \in \Pi(P_0^{\bigotimes n}, P_1^{\bigotimes n}, \ldots, P_h^{\bigotimes n})$, then

$$nP_R(X_i \neq X_j) = \mathbb{E}_R(d_{ham}(X^{(i)}, X^{(j)}))$$

for all $i, j \in \{0, 1, \ldots, h\}$.

Lemma C.5. (Fact 4 in Lalanne, Garivier, and Gribonval 2023) Let $P_0, \ldots, P_h$ be probability measures on $(\mathcal{X}^n, \mathcal{F})$. Then there exists a coupling $R \in \Pi(P_0, P_1, \ldots, P_h)$ such that

$$P_R(X_i \neq X_j) \leq \frac{2\delta(P_i, P_j)}{1 + \delta(P_i, P_j)}.$$

C.1 Proof of Theorem 3.3

With Lemma C.2 we get

$$\frac{1}{h+1}\sum_{j=0}^{h} Q(\tau \neq j|X^{(j)}) \geq 1 - \frac{1 + \frac{1}{h+1}\sum_{j=0}^{h} D_{KL}(Q(\cdot|X^{(j)}), \frac{1}{h+1}\sum_{i=0}^{h} Q(\cdot|X^{(i)}))}{\ln(h+1)}.$$

Then by the convexity of the Kullback-Leibler Divergence in its second argument (Theorem 12 in Van Erven and Harremos 2014)

$$\begin{aligned}\frac{1}{h+1}\sum_{j=0}^{h}&Q(\tau \neq j|X^{(j)}) \\ &\geq 1-\frac{1+\frac{1}{(h+1)^2}\sum_{j=0}^{h}\sum_{i=0}^{h}D_{KL}(Q(\cdot|X^{(j)}),Q(\cdot|X^{(i)}))}{\ln(h+1)},\end{aligned}$$

finally, with Lemma C.1,

$$\frac{1}{h+1}\sum_{j=0}^{h}Q(\tau \neq j|X^{(j)}) \geq 1-\frac{1+\frac{\epsilon}{(h+1)^2}\sum_{j=0}^{h}\sum_{i=0}^{h}d_{ham}(X^{(i)},X^{(j)})}{\ln(h+1)}.$$

□

C.2 Proof of Theorem 3.5

We start by considering the first inequality. First observe that

$$\inf_{\tau}\max_{0\geq j\geq h}P_{p_j q}(\tau\neq j)\geq\frac{1}{h+1}\inf_{\tau}\sum_{j=0}^{h}P_{p_j q}(\tau\neq j).$$

With Lemma C.3 it follows that

$$\frac{1}{h+1}\inf_{\tau}\sum_{j=0}^{h}P_{p_j q}(\tau\neq j)\geq\frac{1}{h+1}\inf_{\tau}\sum_{j=0}^{h}P_{p_j}(\tau\neq j),$$

and with Lemma C.2 we get

$$\inf_{\tau}\max_{0\geq j\geq h}P_{p_j q}(\tau\neq j)\geq 1-\frac{1+\frac{1}{h+1}\sum_{j=0}^{h}D_{KL}(P_{p_j},R)}{\ln(h+1)}.$$

For the second inequality we use Theorem 3.4, then for a coupling $R\in\Pi(P_{p_0}^{\bigotimes n},\ldots,P_{p_h}^{\bigotimes n})$ as in Lemma C.5 we have

$$\begin{aligned}\inf_{\tau}\max_{0\geq j\geq h}P_{p_j q}(\tau\neq j)&\geq\int 1-\frac{1+\frac{\epsilon}{(h+1)^2}\sum_{i=0}^{h}\sum_{j=0}^{h}d_{ham}(X^{(i)},X^{(j)})}{\ln(h+1)}dR\\ &=1-\frac{1+\frac{\epsilon}{(h+1)^2}\sum_{i=0}^{h}\sum_{j=0}^{h}\mathbb{E}_R\left[d_{ham}(X^{(i)},X^{(j)})\right]}{\ln(h+1)}.\end{aligned}$$

With Lemma C.4

$$\inf_{\tau}\max_{0\geq j\geq h}P_{p_j q}(\tau\neq j)\geq 1-\frac{1+\frac{\epsilon}{(h+1)^2}\sum_{i=0}^{h}\sum_{j=0}^{h}nP_R(X_i\neq X_j)}{\ln(h+1)},$$

and finally with Lemma C.5

$$\inf_{\tau}\max_{0\geq j\geq h}P_{p_j q}(\tau\neq j)\geq 1-\frac{1+\frac{n\epsilon}{(h+1)^2}\sum_{j=0}^{h}\sum_{i=0}^{h}\frac{2\delta(P_{p_i},P_{p_j})}{1+\delta(P_{p_i},P_{p_j})}}{\ln(h+1)}.$$

□