Classification under local differential privacy
Thomas Berrett, Cristina Butucea

To cite this version:
Thomas Berrett, Cristina Butucea. Classification under local differential privacy. Annales de l’ISUP, 2019, 63 (2-3), pp.191-204. hal-03603855

HAL Id: hal-03603855
https://hal.science/hal-03603855
Submitted on 10 Mar 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Classification under local differential privacy

Thomas Berrett*\textsuperscript{,\textdagger,\textsterling} and Cristina Butucea*\textsuperscript{,\dagger}

CREST, ENSAE, Institut Polytechnique de Paris\textsuperscript{4}

Abstract: We consider the binary classification problem in a setup that preserves the privacy of the original sample. We provide a privacy mechanism that is \(\alpha\)-locally differentially private and then construct a classifier based on the private sample that is universally consistent in Euclidean spaces. Under stronger assumptions, we establish the minimax rates of convergence of the excess risk and see that they are slower than in the case when the original sample is available.

1. Introduction

One of the most frequently studied problems in machine learning and statistics is to make predictions of a binary outcome \(Y\) in \(\{0,1\}\) given the input variable \(X\) in \(\mathbb{R}^d\), typically based on an independent and identically distributed sample from the distribution of \((X,Y)\); see, for example, [6] for an overview of the area. Despite the long history of this problem there are still many open problems and it remains an active topic of research. Recent work has focused on weakening commonly-made assumptions [4], studying situations in which the training data comes from a different distribution to the test data [3, 5], and making predictions under constraints on allowable classifiers [18].

In recent years, it has become clear that in certain studies there is a need to preserve the privacy of the individuals whose data is collected. As a way of formalising the problem, the framework of differential privacy, see [9] and [10], has prevailed as a natural solution. The privacy of the individuals is protected by randomizing the original data to produce the random variables \(Z_1,\ldots,Z_n\) defined on some measurable space \((Z^n,B^n)\), and the following statistical analysis is based solely on \(Z_1,\ldots,Z_n\) without knowledge of the original data. The randomization is performed through a Markov kernel, also known as privacy mechanism, \(Q : B^n \times (\mathbb{R}^d \times \{0,1\})^\otimes n \rightarrow [0,1]\). A privacy mechanism is called \(\alpha\)-differentially private, for \(\alpha > 0\), if

\[
(1.1) \quad \sup_{A \in B^n} \sup_{u,u' : d(u,u') = 1} \frac{Q(A|u)}{Q(A|u')} \leq e^\alpha,
\]

\textsuperscript{*}Financial support from the French National Research Agency (ANR) under the grant Labex Ecodec (ANR-11-LABEX-0047)

\textsuperscript{†}Financial support from the French National Research Agency (ANR) under the grant ANR-17-CE40-0003 HEDITSA

AMS 2000 subject classifications: Primary 62G08; secondary 62H30

Keywords and phrases: classification, local differential privacy, minimax rates, universal consistency
where $d : (\mathbb{R}^d \times \{0, 1\})^\otimes n \times (\mathbb{R}^d \times \{0, 1\})^\otimes n \to \{0, 1, 2, \ldots\}$ is the Hamming distance, counting the number of positions $i \in \{1, \ldots, n\}$ such that $u_i \neq u'_i$.

In the global, also called central, model for differential privacy, the whole sample is trusted to one person/machine in order to produce the randomized sample. However, in certain situations this is not feasible. In the setup of \textit{local} differential privacy that we consider here, the sample is randomized one at a time by different persons/machines so that the $i$th original data point $(X_i, Y_i)$ only needs to be seen by the $i$th individual. Formally, we assume the sequential structure

$$\{X_i, Y_i, Z_1, \ldots, Z_{i-1}\} \to Z_i \quad \text{and} \quad Z_i \perp (X_j, Y_j) \{X_i, Y_i, Z_1, \ldots, Z_{i-1}\} \text{ for } j \neq i.$$ 

With this structure, the full conditional distribution $Q$ can be expressed in terms of the conditional distributions $Q_i : \mathcal{B} \times (\mathbb{R}^d \times \{0, 1\}) \times Z^{i-1} \to [0, 1]$, where

$$Z_i | \{(X_i, Y_i) = u_i, Z_1 = z_1, \ldots, Z_{i-1} = z_{i-1}\} \sim Q_i(\cdot | u_i, z_1, \ldots, z_{i-1})$$

for $i = 1, \ldots, n$. The privacy constraint (1.1) then reduces to

$$\sup_{A \in \mathcal{B}} \sup_{z_1, \ldots, z_{i-1}} \sup_{u_i, u'_i} \frac{Q_i(A | u_i, z_1, \ldots, z_{i-1})}{Q_i(A | u'_i, z_1, \ldots, z_{i-1})} \leq e^\epsilon,$$

for each $i = 1, \ldots, n$; if this holds then the privacy mechanism $Q$ is said to be $\alpha$--locally differentially private ($\alpha$--LDP). Let $Q_\alpha$ denote the set of $\alpha$--LDP Markov kernels.

Many local privacy mechanisms of interest are of a simpler, non-interactive, form in which $Q_i(\cdot | u_i, z_1, \ldots, z_{i-1})$ does not depend on $z_1, \ldots, z_{i-1}$. In particular, a non-interactive privacy mechanism has a product form:

$$Q(A_1 \times \ldots \times A_n | (u_1, \ldots, u_n)) = \prod_{i=1}^{n} Q_i(A_i | u_i) .$$

Thus, a non-interactive privacy mechanism satisfies $\alpha$--LDP if and only if, for all $i = 1, \ldots, n$,

$$\sup_{A_i \in \mathcal{B}} \sup_{u_i, u'_i} \frac{Q_i(A_i | u_i)}{Q_i(A_i | u'_i)} \leq e^\epsilon .$$

Due to more recent papers such as [7], the attention of the statistical community has been attracted to this field. In [7] it is shown, for example, that the minimax rate of convergence for estimating the mean of a $d$ dimensional vector is slower in the context of privatized data as opposed to the classical problem and information theoretic bounds are established that allow the construction of lower bound results in many other estimation problems. The same authors also considered in [8] nonparametric density estimation and showed that the minimax MISE is of order $n^{-\frac{\beta}{2\beta+2}}$ over Sobolev smooth functions, instead of the classical rate $n^{-\frac{\beta}{2\beta+1}}$. More general linear
functionals of the probability density have been considered by [15] and they showed that the modulus of continuity with respect to the total variation distance drives the rates in presence of privacy, instead of the Hellinger distance. Adaptation to the smoothness of both the privacy mechanism and of the associated estimator has been considered by [2]. They showed a double elbow effect for the adaptive estimation rates for more general integrated risks over Besov class of functions. The sparse regression model has been considered in the context of local privacy by [17]; they give a nearly optimal procedure in the low-dimensional sparse case and consider the case where only the responses are privatized. To the best of our knowledge, classification under local privacy constraints has never been considered from the point of view of statistical inference.

In the sequel, we exhibit a non-interactive $\alpha-$LDP privacy mechanism and construct a classifier that is universally consistent in Euclidean spaces. Under standard assumptions on the probability distribution of the input variables as well as on the regression function (Hölder smoothness $\beta \in [0, 1]$ and margin assumption with parameter $\gamma$), similar to the assumptions in [1], we show that the minimax rate of convergence of the excess risk over all classifiers and all (possibly interactive) $Q \in Q_{\alpha}$ is $(n\alpha^2)\frac{\beta(1+\gamma)}{2\beta+2d}$, and that this rate is achieved by our non-interactive approach. This rate is slower than the minimax rate for classification $n^{-\frac{\beta(1+\gamma)}{2\gamma+d}}$ attainable when the original sample is available [1].

2. Main results

Let $(X, Y)$ be a random vector taking values in $\mathbb{R}^d \times \{0, 1\}$ and let $(X_1, Y_1), \ldots, (X_n, Y_n)$ be independent and identically distributed copies of $(X, Y)$. Our task is to find a mechanism that outputs locally privatised data $Z_1, \ldots, Z_n$ and then to use this privatised data to construct a classifier $C_n : [0, 1]^d \rightarrow \{0, 1\}$ to predict $Y$ from $X$.

The performance of this classifier will be measured through its excess risk, defined as follows. If the distribution $P$ of $(X, Y)$ were known, we could calculate $r(x) = P(Y = 1|X = x)$ and use the Bayes classifier $C_B(x) = I\{r(x) > 1/2\}$. This minimises the risk

$$R_P(C) := P(C(X) \neq Y)$$

over all classifiers $C$. The excess risk of a (data dependent) classifier $C_n$ is then defined to be

$$\mathcal{E}_P(C_n) := R_P(C_n) - R_P(C_B) = \mathbb{E}\left[\{P(C_n(X) = 0|X) - I\{r(X) < 1/2\}\}\{2r(X) - 1\}\right].$$

We now introduce the privacy mechanism and the classifier that we will study in this article. For a bandwidth parameter $h \in (0, \infty)$ and $j = (j_1, \ldots, j_d) \in \mathbb{Z}^d$ set the grid points $x_j := (j_1 h, \ldots, j_d h)$, and for each $x \in [0, 1]^d$ define $j^*(x) := \text{argmin}_{j \in \mathbb{Z}^d} \|x - x_j\|$. With a slight abuse of notation we will assume that our sample
size is even and is given by $2n$. For each $i = 1, \ldots, 2n$, individual $i$ should form the binary array

$$B_i := (1_{\{|x_i - x_j| < h\}})_{j \in \mathbb{Z}^d}$$

and generate a random array $\epsilon_i = (\epsilon_{ij})_{j \in \mathbb{Z}^d}$ with independent and identically distributed Laplace($\alpha/2^{d+1}$) entries. The $Z_i$ are then given by

$$(2.1) \quad Z_i = B_i + \epsilon_i, \quad \text{if } i \in \{1, \ldots, n\}, \quad \text{and } Z_i = Y_i B_i + \epsilon_i, \quad \text{if } i \in \{n + 1, \ldots, 2n\}. $$

Note that this privacy mechanism is local, as each $Z_i$ can be calculated by a different person/machine, and non-interactive, i.e., no other privatized data $Z_j$ with $j \neq i$ are used to encode additional knowledge into $Z_i$.

Our first claim is that the privacy mechanism (2.1) respects the $\alpha$-LDP constraint.

**Theorem 2.1.** Let $Q$ be the privacy mechanism that takes $(X_1, Y_1), \ldots, (X_{2n}, Y_{2n})$ as input and outputs $Z_1, \ldots, Z_{2n}$, as described above. Then $Q \in Q_\alpha$.

Now let $X = x_0$ be the test point we wish to classify. Calculate

$$(2.2) \quad T_n(x_0) := \frac{1}{n} \sum_{i=n+1}^{2n} Z_{i*}(x_0) - \frac{1}{2n} \sum_{i=1}^{n} Z_{ij*}(x_0),$$

and define the classifier $C_n(x_0) := 1\{T_n(x_0) > 0\}$. This classifier is inspired by kernel classifiers that have previously been considered in the classical, non-private classification problem. The rates of convergence of such procedures were studied in [13].

We remark here that there are multiple ways to privatize data and build optimal estimators. As the referee suggested, a similar but simpler procedure can also be used, which does not rely on splitting the sample due to the change of labels into symmetric values -1/2 and 1/2. More precisely, for $i = 1, \ldots, 2n$, we can generate

$$\tilde{Z}_i = (Y_i - 1/2)B_i + \epsilon_i,$$

where $(\epsilon_i)_{i=1}^{2n}$ is the same array of Laplace random variable as above. Given the test point $x_0$, and setting

$$\tilde{T}_n(x_0) := \frac{1}{2n} \sum_{i=1}^{2n} Z_{i*}(x_0),$$

we can define the classifier $\tilde{C}_n(x_0) := 1\{\tilde{T}_n(x_0) > 0\}$. Our following upper bound results (Theorems 2.2 and 2.3) still hold for this method.

Our first main result is that the classifier (2.2) using private data (2.1) is universally consistent, in the following sense.

**Theorem 2.2.** Suppose that $h \to 0$ and $n\alpha^2h^{2d} \to \infty$ as $n \to \infty$. Then, for any probability distribution $P$ on $\mathbb{R}^d \times \{0, 1\}$, we have that $E_P(C_n) \to 0$ as $n \to \infty$. 
In comparison with classical universal consistency results, see for example Theorem 6.2 of [6], we see that we take $n\alpha^2 h^{2d} \to \infty$ rather than $nh^d \to \infty$. The change in the exponent of $h$ seems to be an unavoidable consequence of the privacy constraints.

Our remaining results study the minimax rate of convergence of the excess risk of our classifier over certain classes of distributions $P$, and also show that this matches the minimax optimal rate of convergence under an $\alpha$-LDP constraint. For a class $\mathcal{P}$ of distributions of $(X, Y)$, for a privacy parameter $\alpha > 0$ and for a sample size $n \in \mathbb{N}$, we will write

$$R_{n, \alpha}(\mathcal{P}) := \inf_{Q \in \mathcal{Q}_{\alpha}} \sup_{C_n \in \mathcal{P}} \mathcal{E}_P(C_n)$$

for the minimax excess risk, where the infimum is taken over all Markov kernels $Q \in \mathcal{Q}_\alpha$ and all classifiers $C_n$ depending only on the privatized data $Z_1, \ldots, Z_n$.

We now introduce the classes of distributions over which our results will hold, and note that they are very similar to those considered in [1]. Given $\beta \in (0, 1]$ and $L > 0$ we will say that the distribution of $(X, Y)$ satisfies the $(\beta, L)$-Hölder smoothness condition if

$$|\eta(x') - \eta(x)| \leq L \|x - x'\|^\beta$$

for all $x, x' \in [0, 1]^d$. Given $\alpha \geq 0$ and $C_0 > 0$ we will say that the distribution of $(X, Y)$ satisfies the $(\gamma, C_0)$-margin condition if

$$P(0 < |\eta(X) - 1/2| \leq t) \leq C_0 t^\gamma$$

for all $t > 0$. For $c_0, r_0 > 0$ we say that a Lebesgue measurable set $A \subset [0, 1]^d$ is $(c_0, r_0)$-regular if

$$\lambda(A \cap B_x(r)) \geq c_0 \lambda(B_x(r))$$

for all $r \in (0, r_0)$ and $x \in A$. Then for $c_0, r_0, \mu > 0$ we will finally say that the distribution of $(X, Y)$ satisfies the $(c_0, r_0, \mu)$-strong density assumption if $X$ has a density $f$ such that $\text{supp}(f) := \{x : f(x) > 0\} \subseteq [0, 1]^d$ is $(c_0, r_0)$-regular and $f(x) \geq \mu$ for all $x \in \text{supp}(f)$. We then write $\theta = (\beta, \gamma, C_0, L, c_0, r_0, \mu)$ and $\mathcal{P}(\theta)$ for the class of all distribution of $(X, Y)$ that satisfy the $(\beta, L)$-Hölder smoothness condition, the $(\gamma, C_0)$-margin condition, the $(c_0, r_0, \mu)$-strong density assumption. Our main theorem concerning minimax rates of convergence is the following.

**Theorem 2.3.** Fix $\theta = (\beta, \gamma, C_0, L, c_0, r_0, \mu)$ with $\beta \in (0, 1], \gamma \in [0, \infty)$ and $C_0, L, c_0, r_0, \mu \in (0, \infty)$ such that $\beta \gamma \leq d$. Then there exist $c = c(d, \theta)$ and $C = C(d, \theta)$ such that, for all $n \in \mathbb{N}$ and $\alpha \in (0, 1]$, we have

$$c(n\alpha^2)^{-\frac{\beta(1+\gamma)}{2\beta + 2d}} \leq R_{n, \alpha}(\mathcal{P}(\theta)) \leq C(n\alpha^2)^{-\frac{\beta(1+\gamma)}{2\beta + 2d}}$$

Note that the rates are slower in the privatized setup than the rates obtained by [1], $n^{-\frac{\beta(1+\gamma)}{2\beta + 2d}}$, in the classical setup. Such a loss was already noticed for minimax estimation of a probability density function with privatized data, see e.g. [8]. Theorem 2.3 is a consequence of Theorems 2.4 and 2.5 below.
The following result bounds the excess risk of this classifier and thus establishes the upper bound on $R_{n,\alpha}(\mathcal{P}(\theta))$ in Theorem 2.3. Note that the restriction to the case $\beta \in (0,1]$ is mainly due to the regessogram that defines our classifier. A smoother version should allow to cover cases for $\beta > 1$.

**Theorem 2.4.** Fix $\theta = (\beta, \gamma, C_0, L, c_0, r_0, \mu)$ with $\beta \in (0,1], \gamma \in [0, \infty)$ and $C_0, L, c_0, r_0, \mu \in (0, \infty)$. Then there exists $A = A(d, \beta, \gamma, c_0, r_0, \mu) > 0$ such that

$$\sup_{P \in \mathcal{P}(\theta)} \mathcal{E}(C_n) \leq AC_0 \left\{ \frac{L^d}{(na^2)^{3/2}} \right\}^{\frac{1+\gamma}{d+3}}.$$

The following lower bound complements our previous upper bound and completes the proof of Theorem 2.3.

**Theorem 2.5.** Fix $\beta \in (0,1], \gamma \in [0, \infty)$ and $C_0, L \in (0, \infty)$ such that $\beta \gamma \leq d$. Then there exists $c = c(d, \beta, \gamma, C_0, L)$ such that, for all $c_0, r_0, \mu \in (0, c)$, $n \in \mathbb{N}$ and $\alpha \in (0,1]$ we have

$$R_{n,\alpha}(\mathcal{P}(\beta, \gamma, C_0, L, \mu)) \geq c(na^2)^{-\frac{\beta(1+\gamma)}{2d+2d}}.$$

3. Proofs

**Proof of Theorem 2.1.** First consider $i \in \{1, \ldots, n\}$. Any possible value of $X_i$ produces a value $B_i$ that is a binary array with at most $2^d$ non-zero entries; let $b$ and $b'$ be any two such possible values. Then, writing $f_{Z|X}(z|x)$ for the conditional density of $Z_i$ given $X_i$, for any $z \in \mathbb{R}^d$ we have

$$f_{Z|X}(z|x) = \prod_{j \in \mathbb{Z}^d} \alpha_{2^d+1} \alpha_{2^d+2} e^{-\alpha|z_j-b_j|/2^{d+1}} \leq \exp\left(\frac{\alpha}{2^{d+1}} \sum_{j \in \mathbb{Z}^d} (|z_j-b_j|-|z_j-b_j|)\right) \leq \exp\left(\frac{\alpha}{2^{d+1}} \sum_{j \in \mathbb{Z}^d} |b_j-b_j|\right) \leq e^\alpha.$$
Using the fact that the moment generating function of a Laplace($\alpha/2^{d+1}$) random variable is given by $\lambda \mapsto 1/(1 - 2^{d+2}\lambda^2/\alpha^2)$ on $(-\alpha/2^{d+1}, \alpha/2^{d+1})$, for $\lambda \in (-n\alpha/2^{d+1}, n\alpha/2^{d+1})$ we have that

$$E\{e^{\lambda(T_n - ET_n)}\} = [E\{e^{(\lambda/n)(W - U/2 - EW - EU/2)}\}]^n \leq \left(1 - \frac{2^{d+2}\lambda^2}{n^2\alpha^2}\right)^n \left(1 - \frac{2^{d+2}\lambda^2}{n^2\alpha^2}\right).$$

It therefore follows that, for $t \in (0, 1]$,

$$P(T_n - ET_n \geq t) \leq \inf_{\lambda \in (0, n\alpha/2^{d+1})} \exp(-\lambda t + \frac{5\lambda^2}{32n} - n \log\left(1 - \frac{2^{d+2}\lambda^2}{n^2\alpha^2}\right) - n \log\left(1 - \frac{2^{d+2}\lambda^2}{n^2\alpha^2}\right)) \leq \exp\left(-\frac{n\alpha^2t^2}{2^{2d+4}} + \frac{5n\alpha^4t^2}{2^{2d+9}} - n \log\left(1 - \frac{\alpha^2t^2}{2^{2d+6}}\right) - n \log\left(1 - \frac{\alpha^2t^2}{2^{2d+8}}\right)\right) \leq \exp\left(-\frac{n\alpha^2t^2}{2^{2d+6}}\right),$$

and similarly that the same bound applies to $P(T_n - ET_n \leq -t)$.

Now, writing $X_{x_0}^* := \{x \in \mathbb{R}^d : \|x - x_{j^*}(x_0)\|_\infty < h\}$, we have that

$$E(T_n) = E(W_1 - \frac{1}{2}U_1) = E[I_{X_{x_0}^*}(\eta(X) - 1/2)].$$

Define the set

$$\Omega_0 := \left\{x_0 \in \mathbb{R}^d : \liminf_{h \to 0} \frac{P(\|X - x_0\|_\infty < h)}{h^d} > 0\right\},$$

and note that, for $x_0 \in \Omega_0$ we have that $n\alpha^2P(X \in X_{x_0}^*)^2 \geq n\alpha^2P(\|X - x_0\|_\infty \leq h/2)^2 \to \infty$, since we are assuming that $n\alpha^2h^{2d} \to \infty$. We will now establish that $P(X \in \Omega_0) = 1$. By the Lebesgue decomposition theorem [e.g. Theorem 6.10(a), 16], there exist measures $\mu, \nu$ on $\mathbb{R}^d$ such that $\mu$ is absolutely continuous with respect to Lebesgue measure and $\nu$ is singular with respect to Lebesgue measure, and such that

$$P(X \in A) = \mu(A) + \nu(A)$$

for all measurable $A \subseteq \mathbb{R}^d$. Define the sets

$$\Omega_\mu := \left\{x_0 \in \mathbb{R}^d : \liminf_{h \to 0} \frac{\mu(B_{x_0}(h))}{h^d} > 0\right\}$$

and

$$\Omega_\nu := \left\{x_0 \in \mathbb{R}^d : \liminf_{h \to 0} \frac{\nu(B_{x_0}(h))}{h^d} > 0\right\}$$

so that $\Omega_0 = \Omega_\mu \cup \Omega_\nu$. We now proceed by proving that $P(X \in \Omega_0) = 1$. In a related problem where $\mathbb{R}^d$ is partitioned, a similar equality is stated in [Lemma 24.10
for completeness, we provide a proof here. First, we have that $\mathbb{P}(X \notin \Omega_0) \leq \mu(\Omega_\nu) + \nu(\Omega_\nu)$, and, since $\mu$ is absolutely continuous, it has a density $f_\mu$ and we have that $\Omega_\mu = \{x_0 \in \mathbb{R}^d : f_\mu(x_0) > 0\}$ and $\mu(\Omega_\nu) = 0$.

We now turn to the singular part $\nu$ and write $\lambda$ for Lebesgue measure. Since $\nu$ is singular there exists a measurable set $A \subseteq \mathbb{R}^d$ such that $\nu(A^c) = 0$ and $\lambda(A) = 0$. Fixing an arbitrary $\epsilon > 0$ we can always find an open set $O_\epsilon$ such that $A \subseteq O_\epsilon$ and $\lambda(O_\epsilon) < \epsilon$. Now for each $x \in \Omega_\nu^c \cap A$ we may choose $r_x \in (0,1)$ such that $B_x(r_x) \subseteq O_\epsilon$ and $\nu(B_x(5r_x)) \leq \lambda(B_x(5r_x))$. By the Vitali covering lemma [e.g. Theorem 1.24, 11] there exists a countable subset $\mathcal{I} \subset \Omega_\nu^c \cap A$ such that the balls $(B_x(r_x))_{x \in \mathcal{I}}$ are disjoint and such that $\Omega_\nu^c \cap A \subseteq \bigcup_{x \in \mathcal{I}} B_x(5r_x)$. Hence

$$
\nu(\Omega_\nu) = \nu(\Omega_\nu^c \cap A) \leq \sum_{x \in \mathcal{I}} \nu(B_x(5r_x)) \leq \sum_{x \in \mathcal{I}} \lambda(B_x(5r_x)) \leq 5^d \sum_{x \in \mathcal{I}} \lambda(B_x(5r_x)) = 5^d \lambda(O_\epsilon) < 5^d \epsilon.
$$

Since $\epsilon > 0$ was arbitrary, we have that $\nu(\Omega_\nu^c) = 0$ and hence that $\mathbb{P}(X \in \Omega_0) = 1$.

For $x_0 \in \Omega_0$ we have that $\mathbb{P}(X \in \mathcal{X}_{x_0}^*) > 0$ and we may consider the event

$$
\Omega_1 := \left\{ x_0 \in \Omega_0 : \limsup_{h \to 0} \left| \frac{E(T_n)}{\mathbb{P}(X \in \mathcal{X}_{x_0}^*)} - \eta(x_0) - 1/2 \right| = 0 \right\}.
$$

By the Lebesgue differentiation theorem [e.g. Lemma 4.1.2, 14] we have that $\mathbb{P}(X \in \Omega_1) = 1$. For $x_0 \in \Omega_1$ such that $\eta(x_0) \neq 1/2$ we now have, writing $\delta = \frac{1}{2} |\eta(x_0) - 1/2|\mathbb{P}(X \in \mathcal{X}_{x_0}^*)$, that

$$(3.2) \quad \delta^{-1} E T_n(x_0) \to 2 \text{ sign} (2\eta(x_0) - 1).$$

Moreover, for $x_0 \in \Omega_1$, using (3.1) we also have

$$
\{P[T_n(x_0) < 0] - 1_{\{\eta(x_0) < 1/2\}}\} \{2\eta(x_0) - 1\} \{E T_n \geq 2\eta(x_0) > 1\} \{E T_n \leq -2\eta(x_0) < 1\} \leq \mathbb{P}(T_n(x_0) < 0) 1_{\{E T_n \geq -2\eta(x_0) > 1\}} + \mathbb{P}(T_n(x_0) \geq 0) 1_{\{E T_n \leq -2\eta(x_0) < 1\}} \leq \mathbb{P}(|T_n(x_0) - E T_n(x_0)| \geq \delta) 1_{\{2\eta(x_0) \neq 1\}} \leq 2 \exp\left(-\frac{n\alpha^2 \delta^2}{2d+6}\right) 1_{\{2\eta(x_0) \neq 1\}} \to 0,
$$

where for the final convergence statement we have used the facts that $x_0 \in \Omega_0$ and $n\alpha^2 h^2 \to \infty$. It now follows from this and from (3.2) that for $x_0 \in \Omega_1$ we have

$$
\{P[T_n(x_0) < 0] - 1_{\{\eta(x_0) < 1/2\}}\} \{2\eta(x_0) - 1\} \leq 2 \exp\left(-\frac{n\alpha^2 \delta^2}{2d+6}\right) 1_{\{2\eta(x_0) \neq 1\}} + 1_{\{E T_n \geq 2\eta(x_0) < 1\}} + 1_{\{E T_n \leq -2\eta(x_0) > 1\}} \leq 2 \exp\left(-\frac{n\alpha^2 \delta^2}{2d+6}\right) 1_{\{2\eta(x_0) \neq 1\}} + 21_{\{E T_n(x_0) \delta \leq -1,2\eta(x_0) \neq 1\}} \to 0.
$$
Hence, by the dominated convergence theorem [e.g. Theorem 1.34, 16], we have that
\[ \mathcal{E}_P(C_n) = \mathbb{E} \left[ \{ \mathbb{P}(T_n(X) < 0|X) - 1_{\{\eta(X)<1/2\}} \} \{2\eta(X) - 1\} \right] \to 0, \]
as required. \qed

**Proof of Theorem 2.4.** We adopt the same notation as in the proof of Theorem 2.2 and recall that
\[ \mathbb{E}(T_n) = \mathbb{E} \left( W_1 - \frac{1}{2} U_1 \right) = \int_{X_{x_0}^*} f(x) \{ \eta(x) - 1/2 \} \, dx. \]
Now, if \( x \) belongs to \( B_{x_0}(h/2) \) and given that \( \|x_0 - x_{j^*}(x_0)\|_{\infty} < h/2 \), we get that \( \|x - x_{j^*}(x_0)\|_{\infty} < h \). This implies that \( B_{x_0}(h/2) \subseteq X_{x_0}^* \), so \( \mathbb{P}(X_1 \in X_{x_0}^*) \geq c_0 \mu(h/2)^d \) whenever \( x_0 \in \text{supp}(f) \) and \( h/2 \leq r_0 \). Thus, if \( \eta(x_0) \geq 1/2 + L(2hd^{1/2})^\beta \) we therefore have that
\[ \mathbb{E}(T_n) \geq \int_{X_{x_0}^*} f(x) \{ \eta(x_0) - 1/2 - L(2hd^{1/2})^\beta \} \, dx \]
and similarly if \( \eta(x_0) \leq 1/2 - L(2hd^{1/2})^\beta \) we have \( \mathbb{E}(T_n) \leq -c_0 \mu(h/2)^d \{1/2 - \eta(x_0) - L(2hd^{1/2})^\beta \} \). We can now bound the excess risk of our classifier by appropriately partitioning \( \{x \in [0,1]^d : \eta(x) \neq 1/2\} \) according to the size of \( |\eta(x) - 1/2| \). To this end, define
\[ X_0 := \{x \in [0,1]^d : 0 < |\eta(x) - 1/2| \leq 2L(2hd^{1/2})^\beta \} \]
and, for each \( j = 1, 2, \ldots \),
\[ X_j := \{x \in [0,1]^d : 2^j L(2hd^{1/2})^\beta < |\eta(x) - 1/2| \leq 2^{j+1} L(2hd^{1/2})^\beta \}. \]
Combining (3.1) and (3.3) we can now see that
\[ \mathcal{E}_P(C_n) = \int_{\text{supp}(f)} f(x_0) \{ \mathbb{P}(T_n(x_0) < 0) - 1_{\{\eta(x_0)<1/2\}} \} \{2\eta(x_0) - 1\} \, dx_0 \]
\[ \leq 4L(2hd^{1/2})^2 \mathbb{P}(X \in X_0) \]
\[ + \sum_{j=1}^{\infty} \int_{X_j} f(x_0) \{2\eta(x_0) - 1\} \exp \left( -\frac{n\alpha^2}{2^{2d+6}} \mathbb{E} \{T_n(x_0)\}^2 \right) \, dx_0 \]
\[ \leq 4L(2hd^{1/2})^2 \mathbb{P}(X \in X_0) \]
\[ + \sum_{j=1}^{\infty} 2^{j+2} L(2hd^{1/2})^\beta \mathbb{P}(X \in X_j) \exp \left( -\frac{n\alpha^2}{2^{4d+6-2\beta}} d^2 \right) c_0 \mu^2 L^2 h^{2d+2\beta} 2^{2j} \].
This motivates the choice of bandwidth \( h = (n\alpha^2L^2\mu^2)^{-1/(2d+2\beta)} \). With this choice, there exists \( A = A(d, \beta) > 0 \) such that

\[
E_P(C_n) \leq \frac{A}{2^{\beta(1+\gamma)}} C_0(Lh^\beta)^{1+\gamma} \leq AC_0 \left\{ \frac{L^d}{(n\alpha^2\mu^2)^{3/2}} \right\}^{1/4+3/4}. 
\]

Proof of Theorem 2.5. This result is proved by applying Theorem 3 of Duchi, Jordan and Wainwright [8], which provides a private version of Assouad’s lemma, to the construction used to establish the lower bound in Audibert and Tsybakov [1]. For \( q \in \mathbb{N} \) define \( \mathcal{J} := \{0, 1, \ldots, q\}^d \) and consider the grid

\[
G_q := \left\{ x_j = \left( \frac{2j_1 + 1}{4q}, \ldots, \frac{2j_d + 1}{4q} \right) : j \in \mathcal{J} \right\}. 
\]

Write \( n_q(x) := \arg\min_{x' \in G_q} \|x - x'\| \) and for each \( j \in \mathcal{J} \) let \( \tilde{X}_j = \{ x \in [0, 1/2]^d : j^*(x) = j \} \). For an integer \( m \leq q^d \) let \( \{j^{(1)}, \ldots, j^{(m)}\} \subseteq \mathcal{J} \) be any subset of size \( m \), write \( X_i := \tilde{X}_{j^{(i)}} \) for \( i = 1, \ldots, m \) and write \( X_0 := [0, 1]^d \setminus \bigcup_{i=1}^m X_i \) so that \( X_0, X_1, \ldots, X_m \) forms a partition of \([0, 1]^d\). Further, let \( u : [0, \infty) \to [0, \infty) \) be non-increasing and smooth such that

\[
u(x) = 1 \text{ for } x \in [0, 1/8] \quad \text{and} \quad \nu(x) = 0 \text{ for } x \in [1/4, \infty). 
\]

Define \( \phi(x) = LC_\phi \nu(||x||) \) with \( C_\phi \) chosen small enough that \( \phi \) is \((\beta, L)\)-Hölder smooth.

For each \( \sigma \in \{-1, +1\}^m \) we now define a distribution \( P_\sigma \) of \((X, Y)\). Each of these distributions has the same marginal distribution which, for some \( A_0 \subseteq \mathcal{X}_0 \) sufficiently regular with positive Lebesgue measure and \( w \in (0, 1/m] \), has a density given by

\[
f(x) := \begin{cases} 
(8q)^{d/2} \frac{V_d}{\nu(1/(8q))} & \text{if } x \in B_{j^{(i)}}(1/(8q)) \text{ for some } i = 1, \ldots, m \\
\frac{1 - mw}{\lambda(A_0)} & \text{if } x \in A_0 \\
0 & \text{otherwise}
\end{cases} 
\]

where we write \( V_d := \lambda(B_0(1)) = \frac{\pi^{d/2}}{\Gamma(1+d/2)} \). We define the conditional distribution of \( X|Y \) by writing \( \varphi(x) = q^{-\beta} \phi(q(x - n_q(x))) \), \( \eta_\sigma(x) := 1/2 \) when \( x \in \mathcal{X}_0 \) and

\[
\eta_\sigma(x) := \frac{1 + \sigma_i \varphi(x)}{2} 
\]

when \( x \in \mathcal{X}_i \) for \( i = 1, \ldots, m \). With \( C_\phi \) chosen sufficiently small we have that \( \eta_\sigma \) is \((\beta, L)\)-Hölder smooth for all values of \( \sigma \in \{-1, +1\}^m \). Moreover

\[
P_\sigma(0 < |\eta_\sigma(X) - 1/2| \leq t) = mP_\sigma(0 < \phi(q(X - x_{j^{(1)}})) \leq 2tq^\beta) = mw1_{2tq^\beta \leq LC_\phi}, 
\]

so that the \((\gamma, C_0)\)-margin condition is satisfied when \( mw \leq C_0 \frac{L^\gamma}{2tq^\beta} \).
Now let $C_n$ be any classifier only depending on $Z_1, \ldots, Z_n$ and let $Q \in \mathcal{Q}_\alpha$ be any privacy mechanism that satisfies $\alpha$-LDP. If $(X, Y) \sim P_\sigma$ then write $M_{\sigma, r}^{(n)}$ for the distribution of the privatised data $(Z_1, \ldots, Z_n)$. For any $\sigma \in \{-1, +1\}^m$, $k = 1, \ldots, m$ and $r \in \{-1, 0, +1\}$ we will write $\sigma_{k, r} := (\sigma_1, \ldots, \sigma_{k-1}, r, \sigma_{k+1}, \ldots, \sigma_m)$ and we will write $L_{k, r}$ for the likelihood ratio of $M_{\sigma_{k, r}}^{(n)}$ to $M_{\sigma_{k, 0}}^{(n)}$. Then

$$\sup_{P \in P(\theta)} \mathcal{E}_P(C_n) \geq 2^{-m} \sum_{\sigma \in \{-1, +1\}^m} \mathcal{E}_{P_\sigma}(C_n)$$

$$= 2^{-m} \sum_{\sigma \in \{-1, +1\}^m} \sum_{k=1}^m \sigma_k \int_{X_k} \{P_\sigma(C_n(x) = 0) - \mathbb{1}_{\{\sigma_k < 0\}}\} \varphi(x) f(x) \, dx$$

$$\geq 2^{-m} \sum_{\sigma \in \{-1, +1\}^m} \sum_{k=1}^m \int_{X_k} \mathbb{E}_{\sigma_{k, 0}} \{L_{k, 1} \mathbb{1}_{\{C_n(x) = 0\}} + L_{k, -1} \mathbb{1}_{\{C_n(x) = 1\}}\} \varphi(x) f(x) \, dx$$

$$\geq 2^{-m} \sum_{\sigma \in \{-1, +1\}^m} \sum_{k=1}^m \int_{X_k} \mathbb{E}_{\sigma_{k, 0}} \{\min(L_{k, 1}, L_{k, -1})\} \varphi(x) f(x) \, dx$$

$$= \frac{1}{2} \sum_{k=1}^m \{1 - d_{TV}(M_{+k}^{(n)}, M_{-k}^{(n)})\} \int_{X_k} \varphi(x) f(x) \, dx,$$

where we write $M_{\sigma_{k, r}}^{(n)} = 2^{-(m-1)} \sum_{\sigma : \sigma_{k, r} = r} M_{\sigma}^{(n)}$. With our choice of $\varphi$ we have that

$$\int_{X_k} \varphi(x) f(x) \, dx = \frac{(8q)^d w}{V_d} \int_{B_0(1/(8q))} q^{-\beta} \phi(qx) \, dx = wLC_\phi q^{-\beta}.$$

Now write $P_{\sigma} = 2^{-(m-1)} \sum_{\sigma : \sigma_{k, r} = r} P_\sigma$. Using Cauchy–Schwarz, Pinsker’s inequality and Theorem 3 of Duchi, Jordan and Wainwright [8] we can see that

$$\left\{ \frac{1}{m} \sum_{k=1}^m d_{TV}(M_{+k}^{(n)}, M_{-k}^{(n)}) \right\}^2 \leq \frac{1}{4m} \sum_{k=1}^m \{d_{KL}(M_{+k}^{(n)}, M_{-k}^{(n)}) + d_{KL}(M_{-k}^{(n)}, M_{+k}^{(n)})\}$$

$$\leq \frac{2n(e^\alpha - 1)^2}{m} \sum_{k=1}^m d_{TV}(P_{+k}, P_{-k})^2 = 2n(e^\alpha - 1)^2 w^2 L^2 C_\phi^2 q^{-2\beta}.$$

Take $q = [C_1(na^2)/(2\beta + 2d)]$, $w = c_2 q^{-d}$ and $m = [C_3 q^{-\beta \gamma}]$ for some constants $C_1, c_2, C_3$. If $C_1$ and $C_3$ are chosen large enough then we have $q \geq 1$ and $m \geq 2$. Moreover, $mw \leq c_2 C_3 q^{-\alpha \beta}$ so, for $c_2$ small enough we have both $w \in (0, 1/m]$ and $mw \leq C_0(C_3 q^{-\beta \gamma})^\gamma$. Furthermore, if $c_2$ is chosen small enough then we have $2n(e^\alpha - 1)^2 w^2 L^2 C_\phi^2 q^{-2\beta} \leq 8n a^2 c_2^2 L^2 C_\phi^2 q^{-2\beta - 2d} \leq 8c_2^2 L^2 C_\phi^2 \leq 1/2$. For these choices of $q, w, m$ we then have

$$\sup_{P \in P(\theta)} \mathcal{E}_P(C_n) \geq \frac{mwLC_\phi}{4q^\beta} \geq \frac{C_3 c_2 LC_\phi}{8q^\beta(1+\gamma)} \geq 2^{-\beta(1+\gamma)-3} C_3 c_2 LC_\phi (na^2)^{\beta(1+\gamma)/(2\beta + 2d)}.$$
Acknowledgements

Cristina Butucea is grateful to Denis Bosq for the gentle encouragements to pursue the academic career. His constant interest to emerging research topics is a model to all of his former students. The authors would also like to thank László Győrfi and the anonymous referee for interesting and helpful correspondence.

References