Problèmes d'estimation, de sélection de variables et de tests sous contraintes de confidentialité différentielle locale

Amandine Dubois

UNIVERSITE BRETAGNE LOIRE / MATHSTIC

ENSAI École nationale de la statistique et de l'analyse de l'information

THÈSE DE DOCTORAT DE

L'ECOLE NATIONALE DE LA STATISTIQUE
ET DE L'ANALYSE DE L'INFORMATION

ÉCOLE DOCTORALE N° 601
Mathématiques et Sciences et Technologies de l'Information et de la Communication
Spécialité : *Mathématiques et leurs interactions*

Par

Amandine DUBOIS

Problèmes d'estimation, de sélection de variables et de tests sous contraintes de confidentialité différentielle locale

Thèse présentée et soutenue à Bruz, le 21 juin 2021
Unité de recherche : CREST-ENSAI

Rapporteurs avant soutenance :

Béatrice LAURENT-BONNEAU	Professeur, INSA Toulouse
Aad VAN DER VAART	Professeur, Leiden University

Composition du Jury :

Président :	Bernard DELYON	Professeur, Université de Rennes 1
Examinateurs :	Gilles BLANCHARD	Professeur, Université Paris Saclay
	Alexandra CARPENTIER	Professeur, Magdeburg University
	Béatrice LAURENT-BONNEAU	Professeur, INSA Toulouse
	Aad VAN DER VAART	Professeur, Leiden University
	Nicolas VERZELEN	Chercheur, INRAE Montpellier
Dir. de thèse :	Adrien SAUMARD	Enseignant-chercheur, CREST-ENSAI
Co-dir. de thèse :	Cristina BUTUCEA	Professeur, CREST-ENSAE, IP Paris

Remerciements

Je tiens à remercier d'abord mes directeurs de thèse Adrien Saumard et Cristina Butucea. Merci à vous deux de m'avoir fait découvrir le monde de la recherche. Merci aussi pour la grande gentillesse que vous avez toujours eu à mon égard, pour votre patience et votre grande disponibilité. Merci d'avoir relu à de nombreuses reprises mes différentes productions.

Je remercie également Béatrice Laurent et Aad van der Vaart d'avoir accepté de rapporter ma thèse. Merci à Gilles Blanchard, Alexandra Carpentier, Bernard Delyon et Nicolas Verzelen d'avoir accepté de compléter mon jury.

Ce fut un réel plaisir d'effectuer ma thèse à l'ENSAI, où il règne une atmosphère conviviale. Je tiens à remercier l'ensemble des enseignants-chercheurs qui font vivre le laboratoire. Merci à eux pour leur accueil et leur bienveillance. Merci aussi au personnel administratif, notamment à Cécile Terrien pour m'avoir accompagnée dans toutes les démarches administratives liées au doctorat, à Carole Essirard pour s'être occupée de mes nombreux ordres de mission à l'occasion de visites à l'ENSAE ou de conférences, et à Corinne Barzic et Aurélie Duchesne pour l'organisation de mes heures de TD.

L'enseignement aura été pour moi une véritable bouffée d'air pendant ces trois années de thèse. Je tiens donc à remercier Marie du Roy de Chaumaray, Romaric Gaudel et Adrien Saumard de m'avoir fait confiance pour encadrer des TD. Merci aussi à mes élèves. Ces trois années à leur contact auront renforcé mon envie d'enseigner.

Si j'en suis arrivée ici aujourd'hui, c'est en partie grâce aux professeurs que j'ai eu la chance de rencontrer depuis le collège et qui ont su me transmettre leur passion des mathématiques et l'amour de leur métier. Merci à eux. Merci en particulier à M. Delattre, mon professeur de Terminale, pour m'avoir orientée vers une classe préparatoire aux grandes écoles plutôt que vers l'université. Un grand merci à Richard Revret et Bernard Lemaire, mes professeurs de maths en CPGE, sans qui je n'aurais pas intégré l'ENS Rennes. Merci aussi aux enseignants et chercheurs que j'ai eu la chance de cotoyer à l'ENS Rennes et à l'Université de Rennes 1. Merci à eux pour leur enseignement de grande qualité et leur excellente préparation à l'agrégation.

Merci aux autres doctorants de l'ENSAI : Edouard, Steven, Max, Camille, Elie. Ces

trois années de thèse n'auraient pas été les mêmes sans vous. Merci aussi à mes camarades de promo de l'ENS Rennes, ainsi qu'à mes amis du Nord de la France.

Merci à ma famille et à ma belle-famille pour leur soutien infaillible durant ces trois années. Merci enfin à toi, Rémi. Merci pour ton amour et ton soutien au quotidien, merci de partager ma vie.

Table of Contents

List of Figures

List of Tables

Résumé en français

Présentation du contexte

Au cours de ces dernières années, le développement des nouvelles technologies et la digitalisation ont contribué à une forte augmentation de la quantité de données personnelles collectées. Chaque jour, un grand nombre de données sur chacun d'entre nous sont récoltées, stockées et analysées. Cela inclut des données médicales, nos historiques de navigation internet, nos habitudes d'achat, notre activité sur les réseaux sociaux ou encore des informations de localisation de smartphones... La collecte et l'analyse de ces données peuvent profiter à la société. Par exemple, les données de santé peuvent permettre de faire avancer la recherche, et l'analyse de données personnelles par des entreprises leur permet de cibler plus précisément leur clientèle ce qui permet à chaque individu de bénéficier de l'amélioration et du développement de nouveaux services. Cependant, les gens sont de plus en plus soucieux de la protection de leur vie privée et peuvent être réticents à l'idée de partager leurs données (parfois sensibles) avec d'autres. Quant aux entreprises, elles sont soumises à une réglementation de plus en plus stricte en matière de collecte, de traitement et de partage des données, voir par exemple la "Loi pour une République numérique" (France) votée en octobre 2016 et le Règlement général sur la protection des données (UE) qui est entré en vigueur en mai 2018.

Ce contexte souligne la nécessité de développer des méthodes pour manipuler, transformer une base de données en une autre base de données qu'on dira *privatisée (ou confidentielle)*, de telle sorte que la vie privée de chaque individu dans la base de données soit préservée mais aussi de telle sorte qu'il soit encore possible de tirer des conclusions pertinentes à partir de la base de données privatisée. Parmi les nombreux travaux de recherche engendrés par ce problème, la *confidentialité différentielle* s'est démarquée en fournissant un cadre mathématique solide qui offre des garanties rigoureuses en matière de respect de la vie privée. Depuis l'article fondateur de Cynthia Dwork et ses co-auteurs en 2006 [33], la notion de confidentialité différentelle a été largement adoptée en informatique, cryptographie, machine learning et en statistique.

Récemment, des chercheurs se sont intéressés à des problèmes d'inférence statistique sous

contraintes de confidentialité différentielle, voir par exemple [67, 68, 80, 28, 29, 30, 81, 82, 17, 15]. Ces travaux ont pour buts de quantifier le prix à payer (en terme de vitesse d'estimation) pour avoir des garanties de protection de la vie privée, et de développer des mécanismes de privatisation et des procédures d'estimation optimaux. Cette thèse s'inscrit dans cette ligne de recherche.

Confidentialité différentielle

Dans cette thèse, on s'intéresse à des problèmes d'inférence statistique sous des contraintes de confidentialité différentielle locale, mais la confidentialité différentielle a d'abord été introduite dans un cadre global dans [33].

Dans les deux cas, n individus observent chacun une variable aléatoire X_i et autorisent ces données à être utilisées à des fins d'analyse statistique à condition qu'on leur fournisse des garanties solides que leur vie privée sera protégée. Dans le cadre global, ces n individus font confiance à une même autorité qui collecte les données $X_1, \dots, X_n$ et qui génère, à partir de cette information complète, des *données privatisées* $Z = (Z_1, \dots, Z_k)$ qui préservent la vie privée des n individus. Notons que k peut être différent de n. Seules ces données privatisées sont communicables et disponibles pour l'analyse statistique. Notons respectivement $(\mathcal{X}^n, \mathcal{A}^n)$ et $(\mathcal{Z}, \mathcal{B})$ les espaces mesurables dans lesquels $X = (X_1, \dots, X_n)$ et Z prennent leurs valeurs. La loi conditionnelle de Z sachant X est notée $Q(\cdot \mid X)$, c'est à dire $\mathbb{P}(Z \in A \mid X = x) = Q(A \mid X = x)$, où $Q(\cdot \mid \cdot) : \mathcal{B} \times \mathcal{X}^n \to [0, 1]$ est un noyau de Markov. Pour $\alpha \in [0, \infty)$, on dit ([33]) que Q, qu'on appellera *mécanisme de privatisation*, garantit la α-confidentialité différentielle (globale) si

$$Q(A \mid x) \leq e^{\alpha} Q(A \mid x'), \quad \forall A \in \mathcal{B},\ \forall x, x' \in \mathcal{X}^n : d_H(x, x') = 1, \tag{1}$$

où $d_H(x, x') := \#\{i = 1, \dots, n : x_i \neq x'_i\}$ est la distance de Hamming entre x et x', c'est à dire le nombre de coordonnées de x qui diffèrent de celles de x'. Cette définition assure que les mesures de probabilité $Q(\cdot \mid x)$, $x \in \mathcal{X}^n$, sont mutuellement absolument continues. Ainsi, (1) peut se réécrire

$$e^{-\alpha} \leq \frac{Q(A \mid x)}{Q(A \mid x')} \leq e^{\alpha}, \quad \forall A \in \mathcal{B},\ \forall x, x' \in \mathcal{X}^n : d_H(x, x') = 1,$$

avec la convention $\frac{0}{0} = 1$. Cette contrainte impose que la distribution de Z sachant X

ne dépend pas trop d'un individu en particulier dans la base de données. Intuitivement, si la modification d'une entrée dans la base de données X ne modifie pas beaucoup la distribution de Z sachant X alors il devrait être difficile de deviner si une personne donnée est dans la base de données ou non, protégeant ainsi la vie privée de chaque individu dans la base de données (voir Section 1.2.2 ou [80] pour plus de détails). Notons que plus α est petit, plus $e^{-\alpha}$ et e^{α} sont proches de 1, plus la contrainte de confidentialité est forte.

Dans cette thèse, on s'intéressera plutôt à la confidentialité différentielle *locale*. Dans la configuration locale, chacun des n individus peut générer une version privatisée de ses véritables données sur sa propre machine, et seules les données privatisées sont collectées puis analysées. L'avantage est que les propriétaires des données n'ont pas à partager leurs véritables données avec qui que ce soit et qu'aucune tierce partie de confiance n'est nécessaire. Cependant, un certain degré d'interaction entre les n individus peut-être autorisé. En toute généralité, les données privatisées $Z_1, \dots, Z_n$ peuvent être générées les unes après les autres, et l'individu i peut utiliser, en plus de sa vraie donnée X_i, les données qui ont déjà été privatisées $Z_1, \dots, Z_{i-1}$, pour générer Z_i. On parle alors d'*interaction séquentielle*. Précisément, les données $Z_1, \dots, Z_n$ sont obtenues de la manière suivante : sachant $X_i = x_i$ et $Z_1 = z_1, \dots, Z_{i-1} = z_{i-1}$, le i-ème individu génère

$$Z_i \sim Q_i(\cdot \mid x_i, z_1, \dots, z_{i-1})$$

pour un noyau de Markov $Q_i : \mathcal{B} \times (\mathcal{X} \times \mathcal{Z}^{i-1}) \to [0, 1]$, où $(\mathcal{X}, \mathcal{A})$ and $(\mathcal{Z}, \mathcal{B})$ sont les espaces mesurables auxquels appartiennent respectivement X_i et Z_i, $i = 1, \dots, n$. On dira alors que la suite de noyaux de Markov $(Q_i)_{i=1,\dots,n}$ garantit la confidentialité différentielle locale de niveau α si

$$\sup_{A \in \mathcal{B}} \sup_{z_1, \dots, z_{i-1} \in \mathcal{Z}} \sup_{x_i, x_i' \in \mathcal{X}} \frac{Q_i(A \mid x_i, z_1, \dots, z_{i-1})}{Q_i(A \mid x_i', z_1, \dots, z_{i-1})} \leq e^{\alpha}, \quad \text{pour tout } i = 1, \dots, n. \tag{2}$$

Il se peut qu'aucune interaction entre les n individus ne soit autorisée. Dans ce cas, chaque individu génère une version privatisée Z_i de sa vraie donnée X_i indépendamment de tous les autres individus. Précisément, sachant $X_i = x_i$, le i-ème individu génère

$$Z_i \sim Q_i(\cdot \mid x_i),$$

pour un noyau de Markov $Q_i : \mathcal{B} \times \mathcal{X} \to [0,1]$. La contrainte (2) s'écrit alors

$$\sup_{A \in \mathcal{B}} \sup_{x_i, x_i' \in \mathcal{X}} \frac{Q_i(A \mid x_i)}{Q_i(A \mid x_i')} \leq e^{\alpha}, \text{ pour tout } i = 1, \ldots, n,$$

et on parlera de confidentialité différentielle locale *non-interactive*. Le scénario non interactif semble être plus attrayant en pratique puisque dans ce cadre, la collecte de données peut être entièrement parallélisée. Toutefois, le fait de permettre une interaction séquentielle entre les n individus offre une plus grande souplesse dans la construction des mécanismes de privatisation et peut parfois conduire à de meilleures vitesses d'estimation que dans le cadre non interactif. C'est par exemple le cas pour l'estimation de l'intégrale du carré d'une densité de probabilité [15]. Nous renvoyons le lecteur à [43] pour une meilleure compréhension du rôle de l'interactivité pour la confidentialité différentielle locale.

Résumé des contributions

Dans cette thèse, nous nous intéressons à certains problèmes d'estimation, de sélection de variables et de tests sous la contrainte que seules des données privatisées via un mécanisme de privatisation garantissant la confidentialité différentielle locale de niveau α sont disponibles pour l'inférence.

Une première contribution porte sur l'estimation non-paramétrique d'une densité de probabilité à support inclus dans un compact $[-T, T]$. Dans un cadre minimax prenant en compte les contraintes de confidentialité différentielle locale, nous donnons des bornes inférieures sur la vitesse de convergence sur les ellipsoïdes de Besov $\mathcal{B}^s_{pq}(L)$ pour le risque $\mathbb{L}^r$. Nous complétons ces résultats par des bornes supérieures qui coïncident avec les bornes inférieures à un facteur (au plus) logarithmique près. Plus précisément, nous proposons des mécanismes de privatisation qui nous permettent de construire un estimateur linéaire par ondelettes qui est optimal dans le cas $p \geq r$, mais aussi un estimateur non linéaire par ondelettes avec un seuillage correctement choisi qui est optimal (à un facteur logarithmique près) dans tous les cas. De plus, ce deuxième estimateur est adaptatif au sens où il ne dépend pas des paramètres s, p, q et L de l'espace de Besov auquel appartient f. A notre connaissance, nous sommes les premiers à nous être intéressés à des problèmes d'adaptation en estimation sous contraintes de confidentialité différentielle locale. Nos résultats nous permettent de mettre en évidence un changement de régime dans les

vitesses d'estimation (connu sous le nom d'effet coude) analogue à celui observé dans le cadre classique (i.e. sans contrainte de confidentialité, [24, 41]) mais situé à un niveau différent par rapport au cadre classique. De plus, nous quantifions à quel point les vitesses d'estimation sont déteriorées à cause des contraintes de confidentialité. Ces résultats ont fait l'objet d'une publication dans le journal Bernoulli [13] qui constitue le Chapitre 2 de ce manuscrit.

Une deuxième contribution est consacrée à un problème de sélection de variables. Dans le Chapitre 3, on s'intéresse à l'identification du support de l'espérance d'une variable aléatoire suivant une loi normale d-dimensionnelle sous la contrainte que seules des versions privatisées des données sont disponibles pour l'inférence. Pour cela, nous regardons une modification de la théorie minimax classique prenant en compte les contraintes de confidentialité différentielle locale. Nous donnons des bornes inférieures et des bornes supérieures non-asymptotiques sur le risque minimax d'identification du support, pour le risque lié à la distance de Hamming, sur des classes de vecteurs s-éparses (ou parcimonieux) dont les coordonnées non nulles sont séparées de 0 par une constante $a > 0$. Comme corollaires, nous obtenons des conditions nécessaires et des conditions suffisantes pour que l'identification presque parfaite et l'identification exacte du support soient possibles. Lorsque l'on se restreint à l'utilisation de mécanismes non-interactifs agissant independamment sur chaque coordonnée, notre borne inférieure montre que, contrairement à ce qui a été observé dans le cadre classique non privé [12], l'identification presque parfaite et l'identification exacte du support sont impossibles peu importe la valeur de a dans le régime $n\alpha^2/d^2 \lesssim 1$. Cependant, dans le régime $n\alpha^2/d^2 \gg \log(n\alpha^2/d^2)\log(d)$, nous exhibons une valeur critique a^* (à un facteur logarithmique près) telle que l'identification exacte du support est possible pour tout $a \gg a^*$ et impossible pour $a \leq a^*$. Un résultat similaire est obtenu pour l'identification presque parfaite du support. Nous montrons que ces résultats peuvent être améliorés quand on autorise l'utilisation de n'importe quel mécanisme non-interactif garantissant la α-confidentialité différentielle locale, en ce sens que la transition de phase a alors lieu pour une plus petite valeur critique. Cette thématique de recherche a donné lieu à la rédaction d'un article qui a été soumis [14].

Une troisième contribution porte sur un problème de tests. Dans le chapitre 4, nous supposons que les données sont générées à partir d'une densité de probabilité f appartenant à une clase de Hölder $H(\beta, L)$, $0 < \beta \leq 1$. Etant donné $f_0 \in H(\beta, L)$ on souhaite

tester $H_0 : f \equiv f_0$ contre l'alternative

$$H_1(\rho) : f \in H(\beta, L) \text{ et } \|f - f_0\|_1 \geq \rho,$$

sous la contrainte que seules des données privatisées via un mécanisme de privatisation garantissant la confidentialité différentielle locale de niveau α sont disponibles pour construire une procédure de test. On s'intéresse aux vitesses minimax de séparation quand on autorise seulement l'utilisation de mécanismes de privatisation non interactifs, puis quand on autorise aussi l'utilisation des mécanismes séquentiellement interactifs. Nous proposons des procédures de tests dont l'analyse nous permet d'obtenir des bornes supérieures sur ces vitesses minimax. Ces résultats sont complétés par des bornes inférieures. En comparant les bornes obtenues, nous montrons que les mécanismes de privatisation et les tests proposés sont optimaux dans le scenario séquentiellement interactif, et optimaux à un facteur logarithmique près dans le cadre non interactif, pour un large choix d'hypothèses nulles f_0, incluant la densité de probabilité d'une loi uniforme, normale, Beta, de Cauchy, de Pareto, ou encore exponentielle. Nos résultats nous permettent de quantifier à quel point les vitesses minimax de séparation sont dégradées par rapport au cadre classique de [7]. En outre, on observe que permettre l'utilisation de mécanismes séquentiellement interactifs améliore les résultats obtenus en ne considérant que des mécanismes non interactifs. Ce phénomène, qui n'a pas lieu pour de nombreux problèmes d'estimation (voir par exemple [30],[63] et le Chapitre 2), a déjà été observé pour des problèmes de tests dans [10] et [15]. Un article sur cet axe de recherche a été soumis [25].

Chapter 1

Introduction

In recent years, the development of new technologies and digitalisation have contributed to a sharp increase in the amount of personal data collected. Every day, a large amount of data about each of us is collected, stored and analysed. This includes medical records, internet browsing history, shopping habits, social media activity, location information from smartphones... The collection and analysis of such data can benefit society. For instance, health data can be used to further medical research, and the analysis of personal data by companies enable them to target their customers more precisely, allowing each individual to benefit from the improvement and development of new services. However, people are more and more concerned with the protection of their privacy and might be reluctant to share their (sometimes sensitive) data with others. As for companies, they are subject to stricter and stricter regulations on the collection, processing and sharing of data, see for instance the "Loi pour une République numérique" (France) voted on October 2016 and the General Data Protection Regulation (EU) which came into effect in May 2018.
This context highlights the necessity to develop mechanisms that take as input a database and release a transformed database such that the privacy of each individual in the database is preserved but also such that we can still draw relevant conclusions from the transformed database. From the vast literature that this problem produced, *differential privacy* has emerged as a strong mathematical scheme that provides rigorous privacy guarantees. Since the seminal paper [33], differential privacy has been widely adopted by the computer science, cryptography, machine learning, and statistics communities.
Recently, some papers have studied statistical inference problems under differential privacy constraints. Early work on this topic includes [80, 67, 68]. The first minimax rates of convergence under differential privacy constraints were recently established in [28, 29, 30, 17]. Other papers such as [81, 82, 63, 15] also deal with minimax estimation problems under differential privacy constraints, and [51, 10, 15] tackle minimax goodness-of-fit testing problems. All these papers aim at determining the price (in terms of estimation or testing rates) to be paid for privacy protection and at developing optimal privacy mechanisms.

This thesis enters into this line of research.
After discussing the pitfalls of natural but maybe naive approaches to privacy preserving data analysis, we introduce the notion of differential privacy. We first present *global differential privacy* which requires a trusted third party that collects the true data and who is responsible for the release of a privatized output that preserves the privacy of the individuals to which belong the data. We then introduce *local differential privacy*, setting which will be considered in the rest of the thesis and in which data are privatized before being collected so that the true data are never released. Finally, we present our contributions to locally differentially private minimax adaptive estimation of probability densities, minimax variable selection and minimax goodness-of-fit testing. These contributions will then be developed respectively in Chapter 2, Chapter 3 and Chapter 4.

1.1 First steps towards privacy preserving data analysis

1.1.1 De-identification

A commonly used approach toward data privacy protection is de-identification, which consists in removing from the dataset names and obvious identifiers such as adresses, phone numbers, e-mail adresses, social security numbers, etc. The aim of this technique is to make individuals in the dataset not identifiable. However, there have been a number of cases where persons in a de-identified database have been re-identified.

In 2006 an employee of the internet company AOL released a dataset consisting in a list of 20 million search queries made by about 657000 users over a three-month period, with the hope that it would benefit academic researchers. In order to protect the users' anonyimity, identifiers such as names and IP adresses were removed and replaced by identifier numbers. However, journalists of The New York Times have succeeded in re-identifying an AOL user by analysing her internet searches [9]. This example shows that a person can be re-identified thanks to the richness of the unmasked data.

People in a de-identified dataset can also be re-identified by comparing the de-identified records with records in a different dataset that has not been de-identified. For instance, L. Sweeney used a combination of three attributes (ZIP code, birth date end gender) to re-identify the medical records of the governor of Massachussetts by comparing a de-identified medical dataset with a voter registration list [71]. Another famous example

of de-identification is given by the Netflix Prize. In October 2006, Netflix launched a competition for improving its movie recommendation system [39]. The company offered one million dollars to the first person who would be able to propose a recommendation system that is more accurate than the one they used at that time by at least 10 percent. To help contestants, Netflix gave them access to a database containing more than 100 million ratings (and the dates they were given) collected between October, 1998 and December, 2005. These ratings were given by over 480 thousand customers and concern nearly 18 thousand movies. In order to protect the privacy of its customers, Netflix removed all their personal information and perturbed some ratings (some ratings have been deleted, some alternative ratings and dates have been inserted and some rating dates have been modified) [59]. However, two researchers from the University of Texas at Austin have managed to re-identify two Netflix customers by cross-correlating non-anonymous records from the Internet Movie Database with Netflix de-identified records [56]. Even if these data do not seem sensitive at first glance, these two researchers explain that it is possible to learn sensitive information about a person's political orientation, religious views or even sexual preferences by analyzing the ratings and comments he gave to some movies.

Although de-identification is commonly used, successful re-identifications such as the ones mentioned above can cast doubt on its effectiveness. An attractive property of differential privacy is that it neutralizes attempts to re-identify people using auxiliary information such as the ones mentioned above.

1.1.2 Data aggregation, summary statistics

Data aggregation is a process where data is gathered and expressed in a summary form for statistical analysis. For instance, a company may decide to make a survey to see if people prefer their brand or their competitors' brands. To this aim, they can ask a large number of people which brand they prefer among a given set of brands. They can also ask for other pieces of information such as their names, gender, adress, or age. However, they will present the results to the manager in a summary form. They may only present the counts of votes obtained for each brand to determine which is the most popular. They might also include additional information to determine which brand is the most popular by sexe, age range or in certain regions, but the exact pieces of information obtained for each individual that participated to the survey are never revealed. A common intuition is that privacy of individuals can not be compromised if the data only shows results for groups of individuals. Thus, releasing aggregated data and summary statistics is considered by

many to be safe. However, this conception has to be mitigated.

To illustrate this, let's take an example given by Dwork and Roth [31]. Suppose that Mr. X is in a certain medical database and you're allowed to ask some questions about the database that can be answered by summary statistics. You ask "How many people in the database have cancer ?" The result seems to protect the privacy of each individual in the database. Now, ask "How many people, not named X, in the database have cancer ?". This result, taken alone, also seems safe. However, if you compare the results to these two questions, you can learn if Mr. X has cancer or not. This is called a *differencing attack*. This example shows that doing simple math on aggregate values can give you information on a particular individual in the database. One can think that this kind of problem can be fixed by controling the sequence of questions and answers with the goal of prohibiting the answer to the last question if, in light of the answers already given, it could compromise privacy. However, as it is explained in [31], there are two difficulties with this approach. First, refusing to answer a question can provide pieces of information. Second, it may not even exist an algorithm for deciding if a pair of questions can lead to a differencing attack.

Aggregation can in practice protect privacy but there is no guarantee that it always does.

1.1.3 Randomized response

Even if the notion of differential privacy has been formalized in 2006 in [33], its oldest forms can be traced back to Warner [79] who introduced randomized response which is a technique commonly used in survey research to protect the privacy of respondents and encourage them to answer truthfully to sensitive issues such as sexuality or illegal behaviors for instance.

Let us consider the following case. A survey aims at estimating the proportion of people in the country who regularly use illegal drugs. Thus, we ask a random sample of persons if they regularly use illegal drugs. Those who do not will of course answer "No". The problem is that most of those who do use illegal drugs will lie and answer "No" because answering "Yes" could be detrimental to them. This raises the following question : How can we get accurate answers to a sensitive question which respondents might be reluctant to answer truthfully? Randomized response techniques tackle this problem by adding random noise to individual responses. The following example provides a randomized response technique that can be found in [31] and which is slightly different from Warner's original method.

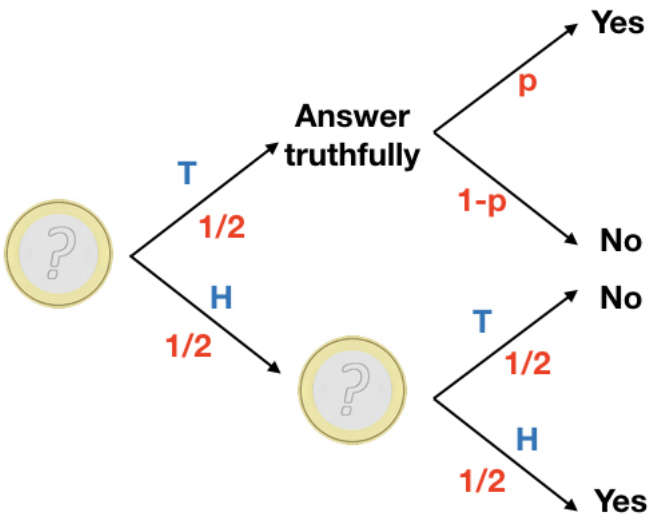

Figure 1.1: A randomized response technique. The letter H stands for Heads, and T stands for Tails.

Example 1.1.1. To deal with the problem mentioned above, let us ask each respondent to follow the following steps before answering the question "Do you regularly use illegal drugs ?" :

1. Flip a coin.

2. If tails, then answer truthfully.

3. If heads, then flip a second coin and answer "Yes" if heads, "No" if tails.

This technique provides *plausible deniability* : a person who answers "Yes" can credibly say that he/she actually does not use illegal drugs since an answer "Yes" may have been given because the two coin flips were both heads, which occurs with probability 1/4. Thus, answering "Yes" can no longer be detrimental to the respondent, which should (in theory) encourage him to answer truthfully. Let us now explain how the true proportion of people who regularly use drugs can be estimated from the "privatized" answers. Let p denote this true proportion. The probability that a respondent who follows the above instructions answers "Yes" is given by $(p/2) + (1/4)$, see Figure 1.1 for a tree diagram. If the number of people surveyed is large enough, then the proportion of people surveyed who answered "Yes" should be close to this theoretical probability. Thus, the true proportion p can be

estimated by the following quantity :

$$2\left[\frac{\text{Number of "Yes" answers}}{\text{Number of people surveyed}} - \frac{1}{4}\right].$$

1.2 Global differential privacy

In this section, we define the notion of global differential privacy (also called central differential privacy) as introduced by Dwork et al. [33], and give some of its properties that can explain why this notion of privacy has been widely adopted by the scientific community as a natural one. We also present some classical privacy mechanisms and discuss some relaxations of the original definition of differential privacy.

1.2.1 Definition

Assume that n individuals each observe a random variable X_i. Assume that they allow these data to be used for statistical analysis on the condition that they are guaranteed strong privacy protections. In the global setting of differential privacy, the n data holders share confidence in a common curator who collects the data $X_1, \dots, X_n$ and who is responsible for the release of a privatized output $Z = (Z_1, \dots, Z_k)$ that preserves the privacy of the n individuals. The statistician does not have access to the original database $X = (X_1, \dots, X_n)$ but only to the privatized output Z. Note that in general k does not need to be equal to n. Let denote respectively $(\mathcal{X}^n, \mathcal{A}^n)$ and $(\mathcal{Z}, \mathcal{B})$ the measurable spaces in which X and Z take values. The conditionnal distribution of Z given X will be denoted by $Q(\cdot \mid X)$, i.e. $\mathbb{P}(Z \in A \mid X = x) = Q(A \mid x)$, where $Q(\cdot \mid \cdot) : \mathcal{B} \times \mathcal{X}^n \to [0, 1]$ is a Markov kernel, that is

- $Q(\cdot \mid x)$ is a probability measure for all $x \in \mathcal{X}^n$
- $Q(A \mid \cdot)$ is $\mathcal{A}^n$-measurable for all $A \in \mathcal{B}$.

The Markov kernel Q is often referred to as a *channel distribution*, a *privatization scheme* or a *privacy mechanism*. We can represent this schematically as in Figure 1.2. Note that in the literature, the term "privacy mechanism" can also refer to the algorithm M such that $Z = M(X)$.

The following definition is due to Dwork et al. [33].

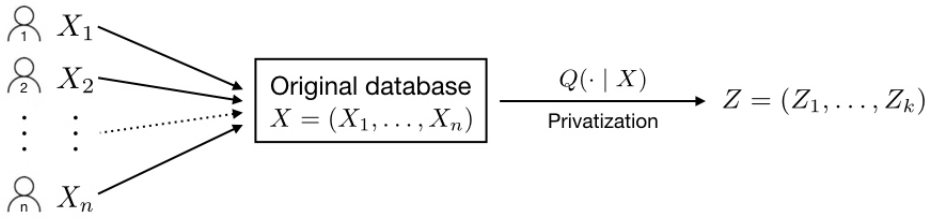

Figure 1.2: Global privacy. The n individuals share confidence in a common curator who gathers their true data and generates a privatized output from this complete information.

Definition 1.2.1. Let $\alpha \in [0, \infty)$. The channel distribution Q is said to provide (global) α-differential privacy if

$$Q(A \mid x) \leq e^{\alpha} Q(A \mid x'), \quad \forall A \in \mathcal{B},\ \forall x, x' \in \mathcal{X}^n : d_H(x, x') = 1, \tag{1.1}$$

where $d_H(x, x') := \#\{i = 1, \ldots, n : x_i \neq x'_i\}$ denotes the number of distinct entries of x and x' also called the Hamming distance.

Note that Definition 1.2.1 ensures thats all the probability measures $Q(\cdot \mid x)$, $x \in \mathcal{X}^n$, are equivalent. Thus, (1.1) can be rewritten

$$e^{-\alpha} \leq \frac{Q(A \mid x)}{Q(A \mid x')} \leq e^{\alpha}, \quad \forall A \in \mathcal{B},\ \forall x, x' \in \mathcal{X}^n : d_H(x, x') = 1,$$

where we interpret $\frac{0}{0}$ as equal to 1.

This notion of privacy requires that the distribution of the privatized output Z does not depend too much on any single element of the database. Intuitively, if changing one entry in the database X does not change the conditional distribution of Z given X too much, then it should be difficult to guess if one given person is in the database or not. The differential privacy constraint should thereby protect the privacy of each individual in the database. See Section 1.2.2 or [80] for more discussion. Note that the smaller α, the closer $e^{-\alpha}$ and e^{α} are to one, and thus the stronger is the privacy constraint.

Example 1.2.2. Let $X_1, \ldots, X_n$ be n independent and identically distributed random variables from an unknown distribution P with support $\mathcal{X}$ included in $[-M, M]$. We want to estimate $\theta := \mathbb{E}_P[X_1]$ while protecting privacy. A classical estimator of θ is the sample mean $\overline{X}_n = (1/n)\sum_{i=1}^n X_i$. However, this is a summary statistics and we have seen in Section 1.1.2 that releasing summary statistics does not guarantee privacy. In

order to ensure differential privacy, one can add properly chosen noise to the sample mean. Precisely, consider

$$Z = \overline{X}_n + \frac{2M}{n\alpha} W, \quad W \sim \mathrm{Lap}(1), \tag{1.2}$$

where W is independent of the X_i's and

$$f_{\mathrm{Lap}(b)}(x) = \frac{1}{2b} \cdot \exp\left(-\frac{|x|}{b}\right),$$

and let us check that this mechanism is α-differentially private. The density of Z given $X = x$, where $X = (X_1, \ldots, X_n)$ is given by

$$q^{Z|X=x}(z) = \frac{n\alpha}{4M} \exp\left(-\frac{n\alpha}{2M}|z - \overline{x}_n|\right), \quad \text{where } \overline{x}_n = \frac{1}{n}\sum_{i=1}^{n} x_i.$$

Thus, for every $x, x' \in \mathcal{X}^n$ with $\mathrm{Card}\{i : x_i \neq x'_i\} = 1$ it holds

$$\begin{aligned}
\frac{q^{Z|X=x}(z)}{q^{Z|X=x'}(z)} &= \exp\left(\frac{n\alpha}{2M}\left[|z - \overline{x'}_n| - |z - \overline{x}_n|\right]\right) \\
&\leq \exp\left(\frac{n\alpha}{2M}|\overline{x'}_n - \overline{x}_n|\right) \\
&= \exp\left(\frac{n\alpha}{2M}\left|\frac{x'_{i_0} - x_{i_0}}{n}\right|\right) \quad \text{for some } i_0 \in [\![1, n]\!] \\
&\leq \exp(\alpha)
\end{aligned}$$

which proves that the mechanism defined by (1.2) provides α-differential privacy. Note that, like the sample mean, Z is an unbiased estimator of θ, however the variance of Z is deteriorated compared to the variance of the sample mean since

$$\mathrm{Var}(Z) = \mathrm{Var}(\overline{X}_n) + \frac{8M^2}{n\alpha^2} = \frac{1}{n}\mathrm{Var}(X_1) + \frac{8M^2}{n^2\alpha^2}.$$

In particular, if one allows α to depend on n, we see that if α is chosen too small, namely $\alpha = o(1/n)$, then the variance of Z explodes. This example highlights the fact that under differential privacy, there will be a trade-off to make between statistical utility and the chosen level of privacy : choosing α too large can lead to good statistical utility but may compromise privacy while taking α too small ensures a high level of privacy but can degrade a lot statistical utility.

1.2.2 Basic properties

Differential privacy has several appealing properties that can explain why this notion of privacy has been widely adopted by researchers in the computer science, machine learning, and statistics communities. We summarize here some of these properties.

- Definition 1.2.1 provides a strong privacy guarantee even in the presence of an adversary who would have almost full knowledge of the true database. Indeed, given the full knowledge of Z, P (the distribution of X_i, $i = 1, \dots, n$), and Q, Wasserman and Zhou (Theorem 2.4, [80]) proved that under differential privacy, any test of level γ to test $H_0 : Z \sim Q(\cdot \mid x)$ against the alternative $H_1 : Z \sim Q(\cdot \mid x')$ (where x and x' are two elements that differ in one entry) has power bounded from above by γe^{α}. Thus, if an adversary has access to the privatized database Z, knows how the data have been privatized, and knows every entry of the true database X except the i-th one, then it would be impossible for him to determine if X_i is the data of individual A or individual B since such a test has either a large first type error probability or a large second type error probability.

- Differential privacy is immune to post-processing: the composition of any function with an α-differentially private mechanism is also α-differentially private, see for instance Proposition 2.1 in [31]. This means that if an adversary has access to a differentially private database then he can not manipulate it to make it less differentially private.

- The release of several independent differentially private outputs is still differentially private and it is easy to understand how the level of privacy degrades with the number of outputs. Indeed, assume that the person responsible for the release of privatized output does not only want to publish a privatized output Z_1 but also a second privatized output Z_2. It has been proved (see for instance [31], Theorem 3.14) that if Z_i, $i = 1, 2$, are α_i-differentially private and independent (conditionnaly on X) views of X then releasing (Z_1, Z_2) is $(\alpha_1 + \alpha_2)$-differentially private. Of course, this result can be applied repeatedly. In particular, to release $(Z_1, \dots, Z_k)$ while satisfying α-differential privacy, it is sufficient that each Z_i, $i = 1, \dots, k$, is an α/k differentially private view of X.

- Differential privacy guarantees can be amplified by subsampling [47, 66, 73]. Let $X = (X_1, \dots, X_n) \in \mathcal{X}^n$ be a dataset. For $m \in [\![1, n]\!]$, let $\mathbf{Subsample}_m(X)$ be a

subset of X that is chosen uniformly at random among all the subsets of X of size m. If a mechanism M defined on $\mathcal{X}^m$ is α-differentially private on $\mathcal{X}^m$ then the mechanism $M \circ \mathbf{Subsample}_m$ defined on $\mathcal{X}^n$ is $\frac{m}{n}(e^\alpha - 1)$-differentially private [73]. Such results are essential for analysing privacy guarantees of procedures involving subsampling steps, as is the case for stochastic gradient descent, which is one of the most popular algorithm in machine learning.

- Differential privacy neutralizes linkage attacks, that is any attempt to re-identify individuals in an anonymized database by combining this database with auxiliary information (such as another dataset for instance).

1.2.3 Usual differentially private mechanisms

In this section we present some classical mechanisms that satisfy the differential privacy constraint.

1.2.3.1 The Laplace mechanism

Early work on differential privacy focused on designing privacy mechanisms for answering basic queries while satisfying differential privacy constraints. For instance, given a dataset $X \in \mathcal{X}^n$ and a function $f : \mathcal{X}^n \to \mathbb{R}^d$, one could ask what the value of $f(X)$ is. Due to Dwork et al. [33], the *Laplace machanism*, which consists in adding Laplace noise to the true answer $f(X)$ with a properly chosen noise level, allows to answer this question while preserving privacy. Precisely, let denote by Δf the global L_1-sensitivity of f, that is $\Delta f = \max \|f(x) - f(x')\|_1$, where the maximum is taken over all elements $x, x' \in \mathcal{X}^n$ differing in a single entry. This quantity measures the maximum change in the value of f due to the change of one entry in any dataset. Dwork et al. [33] proved that releasing $Z = f(X) + (Y_1, \ldots, Y_d)$ where Y_i are drawn i.i.d. from $\mathrm{Lap}(\Delta f/\alpha)$ is α-differentially private. They apply this mechanism for the differentially private release of sums and histograms. Perturbed (with Laplace noise) histograms have further been used for the differentially private estimation of a Lipschitz-continuous density function [80]. With some extra work, the Laplace mechanism can also be used to release contingency tables while satisfying differential privacy constraints [8].

1.2.3.2 Adding noise according to the local sensitivity

The Laplace mechanism works well for functions with small global sensitivity. However, for many functions, such as the median, this approach yields high noise. This issue has been tackled in [60] where the authors suggest to calibrate the magnitude of the noise added to $f(X)$ according to the *local sensitivity* of f at X, which measures the maximum change in the value of $f(X)$ due to the change of one entry in the dataset X. However, this scheme is too naïve. Indeed, the noise magnitude will depend on the database and could leak information about it, violating differential privacy. To prevent this, they instead calibrate the noise level according to a *smooth upper bound* on the local sensitivity. Note that the noise is not sampled from a Laplace distribution. We refer the reader to [60] for more information about smooth upper bounds and about the choice of the noise distribution, but also for applications of their mechanism to the release of the median and the release of the cost of a minimum spanning tree of a graph. More recently, [5] has adapted the idea of smooth sensitivity calibration to propose a private median estimator with subgaussian type deviations. Unlike most prior work on differentially private median estimators, their result also holds for unbounded random variables without any finite moment assumptions.

1.2.3.3 The sample and aggregate method

To apply the framework described in section 1.2.3.2, one must efficiently compute or approximate a smooth upper bound on the sensitivity of f. However, this task can be non-trivial and, for some functions f, NP-hard. To circumvent these difficulties, [60] proposes the *sample and aggregate method* . It works by replacing f with a related function $\bar{f}$ for which a smooth upper bound on the sensitivity is efficiently computable. The first step of the method consists in randomly partitionning the database X into m databases $\tilde{X}_1, \ldots, \tilde{X}_m$. Then, f is evaluated on each of these m databases, which gives outputs $z_1, \ldots, z_m$. For a properly chosen function g, called the *center of attention*, we then compute $\bar{f}(X) = g(z_1, \ldots, z_m)$ and finally release $A(X) = g(z_1, \ldots, z_m) + Y$ where the noise Y is calibrated according to a slight generalization of the smooth sensitivity framework of section 1.2.3.2. Nissim et al. proved that the sample and aggregate mechanism is differentially private and that the released value $A(X)$ is close to the true answer $f(X)$ for databases X such that $f(X)$ is well-approximated by evaluating f on the random subsamples. They apply their method to k-means and learning mixture of gaussians.

1.2.3.4 The exponential mechanism

The exponential mechanism [53] has been introduced to deal with situations where adding noise to the true answer of a query does not make sense (non-numerical queries) or can completely destroy its value (see the example below).

Example 1.2.3 (Auction pricing, adapted from Example 3.5 in [31])**.** Suppose that an auctioneer has an unlimited supply of some good. Assume that on the one hand several bidders each propose a buying price for one good and on the other hand the auctioneer chooses a selling price. The bidders who proposed a buying price higher than the selling price get one good. The auctioneer wants to find the selling price that will maximize the revenue. Assume that there are four bidders A, B, C, D and that they respectively bid 1, 1, 1 and 4.10. If the selling price is $p \in]0, 1]$ then all the bidders will get a good and the revenue will be $4p$. If the selling price is $p \in]1;\ 4.10]$ then only bidder D will get a good and the revenue will be p. If the selling price is $p > 4.10$ then no bidder gets a good and the revenue is 0. Thus, the revenue is maximized when the selling price is set to 4.10 and the addition of noise to this optimal selling price can completely change the revenue since the addition of a positive noise to it will make the revenue fall to 0.

Fix a range $\mathcal{Z}$ of possible outputs. The exponential mechanism relies on the existence of a utility function $q : \mathcal{X}^n \times \mathcal{Z} \to \mathbb{R}$ which maps a database $X \in \mathcal{X}^n$ and a possible output $Z \in \mathcal{Z}$ to a real number $q(X, Z)$. Intuitively, $q(X, Z)$ measures the quality of the output Z if the database is X. For instance, in Example 1.2.3, X could be the buying prices proposed by each bidder, Z could be the selling price fixed by the auctioneer, and $q(X, Z)$ could be the resulting revenue. Given $X \in \mathcal{X}^n$, the goal of the mechanism is to return a $Z \in \mathcal{Z}$ such that $q(X, Z)$ is (approximately) maximized while guaranteeing differential privacy. Precisely, this mechanism consists in selecting $Z \in \mathcal{Z}$ with probability proportional to $\exp(\alpha q(X, Z)/(2\Delta q))$, where here Δq is the largest possible difference in the utility function when applied to two databases that differ in one entry, for all z, that is

$$\Delta q = \max_{z \in \mathcal{Z}} \max_{x, x' \in \mathcal{X}^n : d_H(x, x') = 1} |q(x, z) - q(x', z)|.$$

This mechanism satisfies the α-differential privacy constraints [53].
Let us mention some applications of the exponential mechanism. It has first been applied to several problems in unlimited supply auctions and pricing [53]. It has further been studied in [80] where the authors derive some general results about the accuracy of this mechanism and apply the method to differentially private density estimation. Kifer *et al.*

[49] discusses the use of the exponential mechanism to estimate the support of a vector as a first step for high dimensional sparse regression under privacy constraints. Hall *et al.* [40] discusses the use of the exponential mechanism for releasing a function in a way that guarantees differential privacy.

1.2.4 Relaxations of global differential privacy

Some relaxations of the original definition of differential privacy have been proposed in the literature. Maybe the most popular one is *approximate differential privacy*. The setting is the same as for α-differential privacy but we say that the privacy mechanism Q provides (ε, δ)-approximate differential privacy [32], $\varepsilon \geq 0$, $\delta \geq 0$, if, instead of (1.1), it holds

$$Q(A \mid x) \leq e^{\varepsilon} Q(A \mid x') + \delta, \quad \forall A, \quad \forall x, x' \,:\, d_H(x, x') = 1.$$

This definition of privacy was initially proposed to allow for the addition of Gaussian noise instead of Laplace noise when releasing the evaluation of a function $f : \mathcal{X}^n \to \mathbb{R}^d$ on a database $X \in \mathcal{X}^n$. Specifically, the Gaussian mechanism consists in adding Gaussian noise to the value $f(X)$ with a noise level calibrated according to the L_2-sensitivity of f. It appears that the Gaussian mechanism can not meet α-differential privacy for any α but is approximate differentially private. A weakness of this notion of privacy is the non-optimality or complexity of existing composition results. It is well known that the composition of k mechanisms which are (ε, δ)-differentially private is $(\tilde{\varepsilon}, \tilde{\delta})$-differentially private with $\tilde{\varepsilon} = k\varepsilon$, and $\tilde{\delta} = k\delta$ [32]. Moreover, this bound can not be tightened if no slack in $\tilde{\delta}$ is allowed. However, Dwork et al. [34] proved that one can obtain a better privacy guarantee in terms of $\tilde{\varepsilon}$ if we allow for a slightly larger value of $\tilde{\delta}$. Indeed, they prove that for all $\delta' > 0$, the composition of k mechanisms which are (ε, δ)-differentially private is $(\tilde{\varepsilon}_{\delta'}, k\delta + \delta')$-differentially private with $\tilde{\varepsilon}_{\delta'} = O(k\varepsilon^2 + \varepsilon\sqrt{k \log(1/\delta')})$. In [46] the authors prove a tighter bound and they exactly characterize, for any fixed $\tilde{\delta} \in [0, 1)$, the optimal $\tilde{\varepsilon}$ such that the composition of k mechanisms which are (ε, δ)-differentially private is $(\tilde{\varepsilon}, \tilde{\delta})$-differentially private. This result has been extended in [55] to the non-homogeneous case where the i-th mechanism, $i = 1, \ldots, k$, is $(\varepsilon_i, \delta_i)$-differentially private, and the authors prove that computing the optimal $\tilde{\varepsilon}$ is computationally hard.

Mironov [54] has proposed another relaxation of α-differential privacy based on the Renyi divergence. Let P_1 and P_2 be two distributions on a measurable space $(\mathcal{Z}, \mathcal{B})$.

Assume that they have densities p_1 and p_2 with respect to a common σ-finite dominating measure μ. The Renyi divergence of order $1 < b < \infty$ and of order $b = \infty$ of P_1 from P_2 are then respectively given by

$$D_b(P_1\|P_2) = \frac{1}{b-1}\int \left(\frac{p_1(z)}{p_2(z)}\right)^b p_2(z)d\mu(z), \text{ and } D_\infty(P_1\|P_2) = \ln\left(\sup_{A\in\mathcal{B}} \frac{P_1(A)}{P_2(A)}\right),$$

with the conventions that $0/0 = 0$ and $x/0 = \infty$ for $x > 0$. Consider the notations introduced to define α (global) differential privacy. The Markov kernel Q provides α-differential privacy if and only if

$$D_\infty\left(Q(\cdot \mid x)\|Q(\cdot \mid x')\right) \leq \alpha \quad \text{for all } x, x' \in \mathcal{X}^n \text{ with } d_H(x, x') = 1.$$

The idea of Renyi differential privacy is to allow for the use of the Renyi divergence of order $1 < b < \infty$. Precisely, the Markov kernel will be said to provide (b, α)-Renyi differential privacy, $b > 1$ if

$$D_b\left(Q(\cdot \mid x)\|Q(\cdot \mid x')\right) \leq \alpha \quad \text{for all } x, x' \in \mathcal{X}^n \text{ with } d_H(x, x') = 1.$$

This notion privacy shares attractive properties with α-differential privacy such as immunity to post-processing and a simple composition theorem. Moreover, like approximate differential privacy, it allows for the use of the Gaussian mechanism. However, unlike both α-(global) differential privacy and approximate (ε, δ)-differential privacy, the statement and analysis of a form of privacy amplification by subsampling for Renyi differential privacy are complex [78].

More recently, a new relaxation of differential privacy, called *f-differential privacy* has been introduced in [22]. It is inspired by an hypothesis testing formulation of privacy as follows. For a testing problem of the form $H_0 : P = P_0$ versus $H_1 : P = P_1$, where P, P_0 and P_1 are three distributions, and for a rejection rule $\phi \in [0, 1]$, we denote by $\alpha_\phi = \mathbb{E}_{P_0}[\phi]$ and $\beta_\phi = 1 - \mathbb{E}_{P_1}[\phi]$ the first and second type error probabilities respectively. We then define the function $T(P_0, P_1) : [0, 1] \to [0, 1]$ by

$$T(P_0, P_1)(\alpha) = \inf_\phi\{\beta_\phi : \alpha_\phi \leq \alpha\},$$

where the infimum is taken over all rejection rules. The greater this function is, the harder

it is to distinguish between P_0 and P_1. Consider once again the notations introduced to define α-(global) differential privacy. Given a function $f : [0,1] \to [0,1]$ that is equal to $T(P_0, P_1)$ for some distributions P_0 and P_1, the Markov kernel Q is said to provide f-differential privacy if

$$T(Q(\cdot \mid x), Q(\cdot \mid x')) \geq f.$$

Letting P_0 and P_1 be such that $f = T(P_0, P_1)$, f-differential privacy requires that testing $H_0 : Z \sim Q(\cdot \mid x)$ against the alternative $H_1 : Z \sim Q(\cdot \mid x')$ is at least as difficult as distinguishing P_0 from P_1 based on a single draw. When P_0 and P_1 are the normal distributions $\mathcal{N}(0,1)$ and $\mathcal{N}(\mu,1)$, we talk about *μ-Gaussian differential privacy*. The notion of f-differential privacy is immune to post processing, and the Gaussian mechanism with a properly scaled noise level is Gaussian-differentially private. Moreover, this new notion of privacy presents some advantages compared to the two previous relaxations. Indeed, the authors present a tight composition theorem for f-differential privacy and a simple and easy-to-interpret theorem of privacy amplification by subsambling. They also prove that any definition of privacy that is based on an hypothesis testing interpretation converges to Gaussian differential privacy in the limit under composition.

1.3 Local differential privacy (LDP)

The global model of differential privacy described in the previous section requires that the data-holders share confidence in a common curator who has access to the original data $X_1, \ldots, X_n$ and generates a privatized output from this complete information. We present here a stronger privacy condition called local differential privacy. All the results of this thesis will be obtained in this local setting of differential privacy. In the local setup, each individual can generate a privatized version of its true data on its own machine, and only the privatized data are collected for analysis. The advantage is that data-owners do not have to share their true data with anyone else and and no trusted third party is needed. The local model of differential privacy has been adopted in recent years by major technology companies including Google [35], Microsoft [21] and Apple [20] to collect statistics about the activity of their users and improve user experience. In this section, we introduce two specific classes of locally differentially private mechanisms that will be of interest throughout this thesis : *non-interactive mechanisms* for which no interaction between data-holders is allowed (see Figure 1.3), and *sequentially interactive mechanisms* for which some amount of interaction between data-holders is allowed (see Figure 1.4

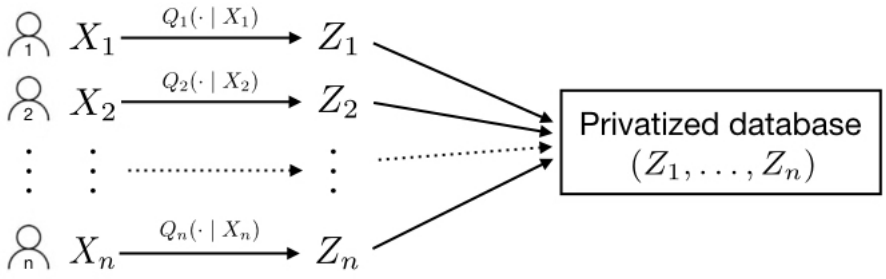

Figure 1.3: Non-interactive local privacy. Each of the n individuals generates a private view Z_i of its original data X_i on its own machine independently of all the other individuals. Only the privatized data $(Z_1, \ldots, Z_n)$ are collected and available for statistical analyses.

below).

1.3.1 The non-interactive scenario

In the local non-interactive scenario, each individual generates a private view Z_i of its original data X_i on its own machine independently of all the other individuals. Precisely, given $X_i = x_i$, the i-th data-holder draws

$$Z_i \sim Q_i(\cdot \mid x_i),$$

for some Markov kernel $Q_i : \mathcal{B} \times \mathcal{X} \to [0, 1]$ where the measure spaces of the non-private and private data are denoted with $(\mathcal{X}, \mathcal{A})$ and $(\mathcal{Z}, \mathcal{B})$, respectively. In this case, we say that the sequence of Markov kernels $(Q_i)_{i=1,\ldots,n}$ provides α-local differential privacy or that $Z_1, \ldots, Z_n$ are α-local differentially private views of $X_1, \ldots, X_n$ if

$$\sup_{A \in \mathcal{B}} \sup_{x_i, x_i' \in \mathcal{X}} \frac{Q_i(A \mid x_i)}{Q_i(A \mid x_i')} \leq e^{\alpha}, \text{ for all } i = 1, \ldots, n. \tag{1.3}$$

Only the privatized data $(Z_1, \ldots, Z_n)$ are available for statistical analyses.
Note that the conditional distribution of $Z = (Z_1, \ldots, Z_n)$ given $X = (X_1, \ldots, X_n)$ is given by the Markov kernel $Q : \mathcal{B}^n \times \mathcal{X}^n \to [0, 1]$ such that

$$Q(A_1 \times \cdots \times A_n \mid x_1, \ldots, x_n) = \prod_{i=1}^{n} Q_i(A_i \mid x_i), \ \forall A_i \in \mathcal{B}, \ \forall x_i \in \mathcal{X}.$$

Thus, if $Q_1, \dots, Q_n$ satisfy (1.3), then Q provides global α-differential privacy.

The following example shows that the randomized response technique introduced in Example 1.1.1 is a locally differentially private privacy mechanism.

Example 1.3.1. The version of randomized response described in Example 1.1.1 is $\ln(3)$-locally differentially private ([31], Claim 3.5).

Let us consider once again the mean estimation framework of Example 1.2.2.

Example 1.3.2. Let $X_1, \dots, X_n$ be n independent and identically distributed random variables from an unknown distribution P with support $\mathcal{X}$ included in $[-M, M]$. We want to estimate $\theta := \mathbb{E}_P[X_1]$ while protecting privacy. To ensure global differential privacy, we suggested in Example 1.2.2 to add Laplace noise to the sample mean. This requires a trusted third party who collects $X_1, \dots, X_n$, computes the sample mean $\overline{X}_n$ and adds the Laplace noise. In the local scenario, such a trusted third party does not exist. Instead, each X_i will be privatized by addition of Laplace noise and only the privatized data Z_i, $i = 1, \dots, n$, will be collected and used to estimate θ. Precisely, for all $i \in [\![1, n]\!]$, generate

$$Z_i = X_i + \frac{2M}{\alpha} W_i, \quad W_i \sim \mathrm{Lap}(1),\ W_i \perp\!\!\!\perp X_i.$$

The density of Z_i given $X_i = x$ is given by

$$q^{Z_i|X_i=x}(z) = \frac{\alpha}{4M} \exp\left(-\frac{\alpha}{2M}|z - x|\right).$$

Thus, for every $x, x' \in \mathcal{X}$ it holds

$$\frac{q^{Z_i|X_i=x}(z)}{q^{Z_i|X_i=x'}(z)} = \exp\left(\frac{\alpha}{2M}\left[|z - x'| - |z - x|\right]\right) \leq \exp\left(\frac{\alpha}{2M}|x' - x|\right) \leq \exp(\alpha),$$

which proves that Z_i is an α-differentially private view of X_i for all $i \in [\![1, n]\!]$. We can then estimate θ by $\overline{Z}_n = (1/n)\sum_{i=1}^n Z_i$. Note that $\overline{Z}_n$ is an unbiased estimator of θ, however the variance of $\overline{Z}_n$ is deteriored compared to the variance of the sample mean but also compared to the globally differentially private estimator proposed in Example 1.2.2 since

$$\mathrm{Var}(\overline{Z}_n) = \mathrm{Var}(\overline{X}_n) + \mathrm{Var}(\overline{W}_n) = \frac{1}{n}\mathrm{Var}(X_1) + \frac{8M^2}{n\alpha^2}.$$

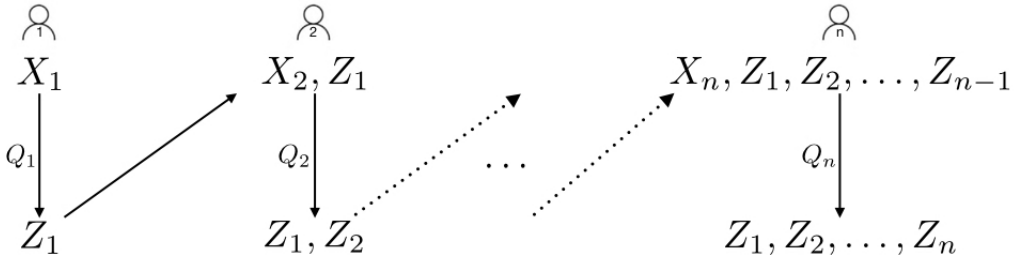

Figure 1.4: Sequentially-interactive local privacy. The privatized data $Z_1, \ldots, Z_n$ are generated one after the other. Individual i has access to the previously privatized data $Z_1, \ldots, Z_{i-1}$ in order to generate its own Z_i. Only the privatized data $(Z_1, \ldots, Z_n)$ are collected and available for statistical analyses.

1.3.2 The sequentially interactive scenario

In the local setting of differential privacy, even though data-owners do not share their true data with anyone else, some interaction between individuals can be allowed. In the so-called sequentially interactive scenario, the privatized data $Z_1, \ldots, Z_n$ are generated one after the other and the i-th individual has access to the previously privatized data $Z_1, \ldots, Z_{i-1}$ in order to generate its own Z_i. Precisely, $Z_1, \ldots, Z_n$ are obtained by successively applying suitable Markov kernels : given $X_i = x_i$ and $Z_1 = z_1, \ldots, Z_{i-1} = z_{i-1}$, the i-th data-holder draws

$$Z_i \sim Q_i(\cdot \mid x_i, z_1, \ldots, z_{i-1})$$

for some Markov kernel $Q_i : \mathcal{B} \times (\mathcal{X} \times \mathcal{Z}^{i-1}) \to [0,1]$ where the measure spaces of the non-private and private data are denoted with $(\mathcal{X}, \mathcal{A})$ and $(\mathcal{Z}, \mathcal{B})$, respectively.

We say that the sequence of Markov kernels $(Q_i)_{i=1,\ldots,n}$ provides α-local differential privacy or that $Z_1, \ldots, Z_n$ are α-local differentially private views of $X_1, \ldots, X_n$ if

$$\sup_{A \in \mathcal{B}} \sup_{z_1, \ldots, z_{i-1} \in \mathcal{Z}} \sup_{x_i, x_i' \in \mathcal{X}} \frac{Q_i(A \mid x_i, z_1, \ldots, z_{i-1})}{Q_i(A \mid x_i', z_1, \ldots, z_{i-1})} \leq e^{\alpha}, \quad \text{for all } i = 1, \ldots, n. \tag{1.4}$$

Note that the conditional distribution of $Z = (Z_1, \ldots, Z_n)$ given $X = (X_1, \ldots, X_n)$ is given by the Markov kernel $Q : \mathcal{B}^n \times \mathcal{X}^n \to [0,1]$ such that for all $x = (x_1, \ldots, x_n) \in \mathcal{X}^n$

$$Q(dz \mid x) = Q_1(dz_1 \mid x_1) Q_2(dz_2 \mid x_2, z_1) \cdots Q_n(dz_n \mid x_n, z_1, \ldots, z_{n-1}).$$

Thus, if $Q_1, \ldots, Q_n$ satisfy (1.4), then Q provides global α-differential privacy.

The non-interactive scenario seems to be more attractive in practice since in this setting the collection of data can be fully parallelized. However, allowing for sequential interaction between data-holders offers more flexibility in the construction of privacy mechanisms and can sometimes lead to better estimation rates than the ones obtained in the non-interactive setting. This is for instance the case for the estimation of the integrated square of a density [15]. We refer the reader to [43] and references therein for a deeper understanding of the role of interactivity in local differential privacy.

1.4 Contributions to minimax adaptive LDP estimation of probability densities

The problems of density estimation and variable selection studied respectively in Chapters 2 and 3 can be considered as particular cases of a more general statistical problem called minimax estimation. In this section, we present a modification of the non-private minimax framework that takes into account privacy constraints and we summarise our contributions to minimax adaptive density estimation under local differential privacy constraints.

1.4.1 LDP minimax risk

Consider n random variables $X_1, \dots, X_n$, assumed to be i.i.d. from some probability distribution $P \in \mathcal{P}$. Suppose that we want to estimate a parameter of interest $\theta(P) \in \Theta \subset \mathcal{F}$. For instance, for the univariate mean estimation problem considered in Examples 1.2.2 and 1.3.2, $\mathcal{P}$ could be the set of all the probability distributions with support included in $[-M, M]$, and the parameter of interest is $\theta(P) = \mathbb{E}[X_1] \in [-M, M] \subset \mathbb{R}$. Note that $\mathcal{F}$ can be an infinite dimensional function space if the parameter of interest is a density function for instance.

In the non-private case, the statistician has direct access to $(X_1, ..., X_n)$ and we call *estimator* any measurable function of $X_1, ..., X_n$ taking values in $\mathcal{F}$. The quality of an estimator $\hat{\theta}$ can be measured by the following quantity

$$\mathbb{E}_{P^{\otimes n}}\left[\Phi\left(\rho(\hat{\theta}(X_1, \dots, X_n), \theta(P))\right)\right],$$

where ρ is some semi-metric on $\mathcal{F} \times \mathcal{F}$, and $\Phi : \mathbb{R}_+ \to \mathbb{R}_+$ is a non-decreasing loss function with $\Phi(0) = 0$. This quantity is called the *risk* of $\hat{\theta}$ for the estimation of $\theta(P)$. Classical

choices of function Φ and metric ρ are given by $\Phi : x \mapsto x^2$ and $\rho(\hat{\theta}, \theta) = |\hat{\theta} - \theta|$ if $\theta, \hat{\theta} \in \mathbb{R}$ and $\rho(\hat{\theta}, \theta) = \|\hat{\theta} - \theta\|_2$ if $\theta, \hat{\theta} \in \mathbb{L}^2(\mathbb{R}^d)$. The corresponding risks are respectively called *mean squared error* (MSE) and *mean integrated squared error* (MISE). If we know a priori that P belongs to some set of distributions $\mathcal{P}$, then the maximal risk of an estimator $\hat{\theta}$ is

$$r_n(\hat{\theta}, \mathcal{P}, \theta) = \sup_{P \in \mathcal{P}} \mathbb{E}_{P^{\otimes n}} \left[\Phi \left(\rho(\hat{\theta}(X_1, \dots, X_n), \theta(P)) \right) \right].$$

It is then natural to choose an estimator whose maximal risk is minimal, yielding the minimax risk

$$\mathcal{R}_n(\mathcal{P}, \theta) = \inf_{\hat{\theta}} \sup_{P \in \mathcal{P}} \mathbb{E}_{P^{\otimes n}} \left[\Phi \left(\rho(\hat{\theta}(X_1, \dots, X_n), \theta(P)) \right) \right],$$

where the infimum runs over all estimators $\hat{\theta}$ taking $(X_1, \dots, X_n)$ as input. Note that minimaxity is a criterion of optimality which is sometimes considered in the literature as being too pessimistic in the sense that it provides the best estimator for the worst value of the parameter. However, it remains one of the only criteria making it possible to compare estimation procedures.

Duchi, Jordan and Wainwright [28, 29, 30] have been the first to propose a modification of the minimax risk that takes into account privacy constraints. We describe it here. In the private setting, the statistician has only access to privatized versions $Z_1, \dots, Z_n$ of $X_1, \dots, X_n$ and estimators are thus measurable functions of $Z_1, \dots, Z_n$. Let $\mathcal{Q}_\alpha$ denote the set of all α-locally differentially private mechanisms. Assume that $Z = (Z_1, \dots, Z_n)$ has been produced via a privacy mechanism $Q \in \mathcal{Q}_\alpha$. This leads to the following modified minimax risk

$$\mathcal{R}_n(Q, \mathcal{P}, \theta) = \inf_{\hat{\theta}} \sup_{P \in \mathcal{P}} \mathbb{E}_{QP^{\otimes n}} \left[\Phi \left(\rho(\hat{\theta}(Z_1, \dots, Z_n), \theta(P)) \right) \right],$$

where $QP^{\otimes n}$ denotes the distribution of Z. It is then natural to search for a privacy mechanism $Q \in \mathcal{Q}_\alpha$ that minimizes this quantity. The α-private minimax risk is finally defined as follows

$$\mathcal{R}_{n,\alpha}(\mathcal{P}, \theta) = \inf_{Q \in \mathcal{Q}_\alpha} \inf_{\hat{\theta}} \sup_{P \in \mathcal{P}} \mathbb{E}_{QP^{\otimes n}} \left[\Phi \left(\rho(\hat{\theta}(Z_1, \dots, Z_n), \theta(P)) \right) \right], \tag{1.5}$$

where the infimum is taken over all estimators taking $(Z_1, \dots, Z_n)$ as input and all privacy mechanisms guaranteeing α-local differential privacy. A tuple $(Q, \hat{\theta})$ will be said *rate*

optimal if

$$\sup_{P\in\mathcal{P}} \mathbb{E}_{QP^{\otimes n}}\left[\Phi\left(\rho(\hat{\theta},\theta(P))\right)\right] \leq C(\Phi\circ\rho,\mathcal{P})\mathcal{R}_{n,\alpha}(\mathcal{P},\theta).$$

The study of the private minimax risk (1.5) and the construction of optimal privacy mechanisms and estimators are still at their beginnings. In [28, 29, 30], the authors derive lower bounds and matching upper bounds on the α-private minimax risk (1.5) for several statistical problems including mean estimation, median estimation, density estimation over Sobolev ellipsoids, and generalized linear models. They obtain the lower bounds by developing and applying private versions of the classical Le Cam, Fano and Assouad methods, see [83] for the non-private version of these methods. They obtain matching upper bounds by exhibiting and analysing specific privacy-preserving estimation procedures. The α-private minimax risk (1.5) has further been studied in [63] in the case where the parameter of interest $\theta(P)$ is a real parameter and the metric ρ is given by $\rho(x,y) = |x-y|$. They characterize the rate at which $\mathcal{R}_{n,\alpha}(\mathcal{P},\theta)$ converges to zero as $n\to\infty$ in high generality. Precisely, if ω_{TV} denotes the modulus of continuity of the functional θ over $\mathcal{P}$ with respect to total variation distance, they prove that for a large class of functions Φ, the α-private minimax risk (1.5) scales as $\Phi\left(\omega_{TV}((n\alpha^2)^{-1/2})\right)$ under regularity conditions that are satisfied in particular if θ is linear and $\mathcal{P}$ is convex. They also exhibit a minimax sample mean estimator based on binary privatized observations that achieves the minimax rate. They apply their results to classical examples including moment estimation, estimation of a density at a fixed point and estimation of the endpoint of a uniform distribution. Butucea *et al.* [15] investigates minimax estimation of the integrated square of a density. Let us also mention [27] which aims at taking into account the pessimistic nature of minimax risk (1.5) and develop instead a *local minimax approach*. The results obtained in the above mentioned papers allow, by comparing private and non-private minimax rates, to quantify the price (in terms of estimation rates) that has to be paid for privacy protection for a large number of estimation problems and can also be used to determine which privacy mechanisms are optimal.

In this spirit, we study in Chapter 2 minimax adaptive density estimation over Besov ellipsoids. In the next section, we present the existing results on minimax non-parametric density estimation under differential privacy constraints and sum up our contributions to this topic.

1.4.2 Minimax adaptive LDP estimation of probability densities

The work on non-parametric density estimation under differential privacy constraints has been initiated in [80] in the global framework described in Section 1.2. The authors discuss the private estimation of Lipschitz continuous densities supported on $[0,1]^r$ via histograms and the estimation of densities supported in $[0,1]$ and belonging to a Sobolev ellipsoid via orthogonal series. In [40] the authors develop methods for releasing functions while preserving global (ε, δ)-approximate differential privacy (which is a relaxation of the global differential privacy framework introduced in Section 1.2.4) and discuss kernel density estimators as the main example. Interestingly, in [80] and [40] the authors exhibit density estimators whose mean integrated squared error achieve the non-private minimax rate of convergence. The effects of local differential privacy on minimax rates appear to be more severe [29, 30, 63]. In [29] and [30] the authors study the estimation of a density function supported on $[0,1]$ and provide minimax rates of convergence for the mean integrated squared error over Sobolev ellipsoids with arbitrary smoothness parameter $\beta \geq 1$. They prove that the non-private minimax rate $n^{-2\beta/(2\beta+1)}$ deteriorates to $(n\alpha^2)^{-2\beta/(2\beta+2)}$ when imposing α-local differential privacy constraints and they exhibit private estimators whose mean integrated squared error achieve this rate. In [63] the authors apply the general theory they have developed to several examples including minimax density estimation at a point $x_0 \in \mathbb{R}^d$ over the anisotropic class $\mathcal{H}_{\beta,L}(\mathbb{R}^d)$ of Lebesgue densities on $\mathbb{R}^d$ such that for every $j \in [\![1,d]\!]$ and every $x, x' \in \mathbb{R}^d$,

$$\left|f(x_1,\dots,x_{j-1},x'_j,x_{j+1},\dots,x_d) - f(x)\right| \leq L_j|x'_j - x_j|^{\beta_j}.$$

Their results shows that the minimax rate for mean squared error degrades from $n^{-1/(1+\bar{r}/2)}$ where $\bar{r} = \sum_{j=1}^d 1/\beta_j$ in the non-private setting to $(n\alpha^2)^{-1/(1+\bar{r})}$ under α-local differential privacy constraints. All these results exhibit smoothness dependent privacy mechanisms and estimators.

In Chapter 2 we pursue the work on non-parametric density estimation under local differential privacy constraints initiated in the above mentioned papers by considering density estimation over Besov ellipsoids and general $\mathbb{L}^r$-risk. Moreover, we address adaptation to the smoothness parameter. Our contributions to this topic are summed up below and were published in [13].

We assume that for $i = 1,\dots,n$ the i-th data holder observes a real-valued random variable X_i distributed according to a probability density function f whose support is included

in some compact set $[-T,T]$. The aim is that every data-holder releases an α-locally differentially private view Z_i of X_i such that the density f can be estimated from the data $Z_1,\dots,Z_n$ in an optimal way. We study the following α-private minimax risk

$$\mathcal{R}_{n,\alpha}(\|\cdot\|,\mathcal{D}^s_{pq}(L,T)) = \inf_{Q\in\mathcal{Q}_\alpha}\inf_{\hat{f}}\sup_{f\in\mathcal{D}^s_{pq}(L,T)}\mathbb{E}\left[\|\hat{f}-f\|_r^r\right],$$

where $\mathcal{Q}_\alpha$ denotes the set of all α-locally differentially private privacy mechanisms and $\mathcal{D}^s_{pq}(L,T)$ denotes the set of all densities supported on a subset of $[-T,T]$ and belonging to some Besov ellipsoids $\mathcal{B}^s_{pq}(L)$. Wavelet methods have turned out particularly convenient to study the non-private version of this minimax risk which is known ([24], [41]) to have lower bound $\mathfrak{r}_n$ where

$$\mathfrak{r}_n = \begin{cases} n^{-\frac{rs}{2s+1}}, & \text{if } p > \frac{r}{2s+1}, \\ (n/\log n)^{-\frac{r(s-1/p+1/r)}{2(s-1/p)+1}}, & \text{if } p \le \frac{r}{2s+1} \text{ and } s \ge \frac{1}{p}. \end{cases}$$

Moreover, these rates are optimal or suboptimal by a logarithmic factor only (see [41] for an extensive discussion). The structural change of the rate between *dense zone* (where $p > r/(2s+1)$) and *sparse zone* (where $p \le r/(2s+1)$) is sometimes called an *elbow effect*. Moreover, in the dense case, we can distinguish the *homogeneous* zone when $p \ge r$ and the *non-homogeneous* zone where $r/(2s+1) < p < r$. In the homogeneous case, *linear* wavelet estimators are rate optimal whereas linear procedures are necessarily sub-optimal in the non-homogeneous case (see [41] and references therein). In this latter scenario as well as in the sparse case, non-linear estimators based on wavelet thresholding turn out to be optimal at least up to logarithmic factors. When α-local differential privacy constraints are imposed, we derive the following lower bound on the α-private minimax risk :

$$\mathcal{R}_{n,\alpha}(\|\cdot\|_r^r,\mathcal{D}^s_{pq}) \gtrsim \mathfrak{r}^*_{n,\alpha},$$
$$\text{where } \mathfrak{r}^*_{n,\alpha} = \begin{cases} (n(e^\alpha-1)^2)^{-\frac{rs}{2s+2}}, & \text{if } p > \frac{r}{s+1}, \\ \left(\frac{n(e^\alpha-1)^2}{\log(n(e^\alpha-1)^2)}\right)^{-\frac{r(s-1/p+1/r)}{2(s-1/p)+2}}, & \text{if } p \le \frac{r}{s+1} \text{ and } s \ge \frac{1}{p}. \end{cases}$$

This lower bound is complemented by corresponding upper bound results. As in the non-private case, we prove that a linear wavelet estimator (based on the privatized data $Z_1,\dots,Z_n$) attains the given rate in the homogeneous case, that is, whenever $p \ge r$, and we show that non-linear estimators based on wavelet thresholding can attain the lower

bound up to logarithmic factors both in the dense and in the sparse zone. Interestingly, the non-linear estimator we propose does not depend on the parameters s, p, q, L. We can make the following comments.

- The lower bound in the private setting is deteriorated compared to the non-private one but reveals a similar elbow effect.
- In allowing for general $\mathbb{L}^r$-risk and Besov ellipsoids, we have widened the range of results on density estimation under privacy constraints which merely focused on $\mathbb{L}^2$-risk and Sobolev ellipsoids or Lipschitz-continuous densities until now.
- To the best of our knowledge, we are the first to consider adaptation to smoothness in the framework of locally differentially private estimation.

This research theme has led to the writing of the paper [14] that has been submitted. In a work subsequent to ours and inspired by the results of [40], M. Kroll [50] has studied pointwise kernel density estimation over Sobolev classes in the local setting of (α, β)-approximate differential privacy and has investigated adaptivity to the smoothness parameter.

1.5 Contributions to LDP variable selection

A few papers tackle selection problems under privacy constraints. In the global (ε, δ)-approximate differential privacy setting, [70] and [6] study top-k selection, which consists in selecting the k largest coordinates of a vector of dimension d. This problem has also been studied under local differential privacy constraints in [74].

In Chapter 3, we address another selection problem, namely *support recovery* in the Gaussian mean model in $\mathbb{R}^d$ under the additional constraint that only privatised data are available for inference. Let X^i, $i = 1, \dots, n$ be i.i.d $\mathcal{N}(\theta, \sigma^2 I_d)$ random vectors of $\mathbb{R}^d$. We assume that the vectors $X^i = (X^i_j)_{j=1,\dots,d}$ for $i = 1, \dots, n$ are observed by n distinct data holders who refuse to share their respective observations, and that the mean vector θ is (s, a)-sparse in the sense that θ belongs to one of the following sets:

$$\Theta_d^+(s, a) = \{\theta \in \mathbb{R}^d : \text{there exists a set } S \subseteq \{1, \dots, d\} \text{ with at most } s \text{ elements such that } \theta_j \geq a \text{ for all } j \in S, \text{ and } \theta_j = 0 \text{ for all } j \notin S\},$$

or

$$\Theta_d(s,a) = \{\theta \in \mathbb{R}^d : \text{there exists a set } S \subseteq \{1,\dots,d\} \text{ with at most } s \text{ elements such that } |\theta_j| \geq a \text{ for all } j \in S, \text{ and } \theta_j = 0 \text{ for all } j \notin S\}.$$

We want to recover the support of θ, which means that we want to find where the non-zero coefficients of θ are located. The parameter of interest is thus the vector $\eta \in \mathbb{R}^d$ defined by

$$\eta = \eta(P_\theta) = (I(\theta_j \neq 0))_{j=1,\dots,d},$$

where $I(\cdot)$ is the indicator function. Working under local differential privacy constraints, the statistician does not have access to the true data to estimate η but only to α-locally differentially private views $Z^1,\dots,Z^n$ of $X^1,\dots,X^n$. Our goal is to estimate the vector η by a *selector* $\hat{\eta}$, that is a measurable function $\hat{\eta} = \hat{\eta}(Z^1,\dots,Z^n)$ taking values in $\{0,1\}^d$. We judge the quality of a selector $\hat{\eta}$ as an estimator of η by the Hamming loss between $\hat{\eta}$ and η which counts the number of positions at which $\hat{\eta}$ and η differ :

$$|\hat{\eta} - \eta| := \sum_{j=1}^{d} |\hat{\eta}_j - \eta_j| = \sum_{j=1}^{d} I(\hat{\eta}_j \neq \eta_j).$$

For the support recovery problem, we consider only α-locally differentially private mechanisms which transform each $X^i \in \mathbb{R}^d$ into a private release Z^i taking also values in $\mathbb{R}^d$, and we focus here on non-interactive mechanisms. However, we distinguish between privacy mechanisms that act on each coordinate of X^i either locally (separately) or globally. More specifically, we will consider the two following scenarios:

- **Coordinate Local (CL) Privacy Mechanisms** : there is a sequence $Q = (Q^i)_{i=1,\dots,n}$ of Markov kernels providing α-local differential privacy such that $Z^i \sim Q^i(\cdot \mid X^i = x^i)$ for all $i \in [\![1,n]\!]$, and Q^i is obtained as product of coordinate-wise kernels as follows:

  $$\text{for all } i \in [\![1,n]\!] \text{ and all } j \in [\![1,d]\!], Z^i_j \sim Q^i_j(\cdot \mid X^i_j = x)$$

  for some (α/d)-differentially private mechanism Q^i_j. We denote by $\mathcal{Q}^{CL}_\alpha$ the set of all privacy mechanisms $Q = (Q^1,\dots,Q^n)$ satisfying these assumptions.

- **Coordinate Global (CG) Privacy Mechanisms** : there is a sequence $Q = (Q^i)_{i=1,\dots,n}$ of Markov kernels providing α-local differential privacy such that $Z^i \sim$

$Q^i(\cdot \mid X^i = x^i)$ for all $i \in [\![1, n]\!]$. We denote by $\mathcal{Q}_\alpha$ the set of all privacy mechanisms $Q = (Q^1, \dots, Q^n)$ satisfying this assumption.

In other words, in the Coordinate Local case, we consider only non-interactive α-locally differentially private mechanisms that act coordinate by coordinate with the same amount of privacy on each coordinate, while in the second scenario any non-interactive α-locally differentially private mechanism is allowed to be used.
For both scenarios, if P_θ denotes the distribution of X^i then the distribution of $(Z^1, \dots, Z^n)$ will be denoted by $Q(P_\theta^{\otimes n})$. We say that a selector $\hat{\eta} = (\hat{\eta}_1, \dots, \hat{\eta}_d)$ is *separable* if for all $j = 1, \dots, d$ its jth component $\hat{\eta}_j$ depends only on $(Z_j^i)_{i=1,\dots,n}$. We denote by $\mathcal{T}$ the set of all separable selectors. We are interested in the study of the following private minimax risks

$$\mathcal{R}_n^{CL}(\alpha, \Theta) = \inf_{Q \in \mathcal{Q}_\alpha^{CL}} \inf_{\hat{\eta} = \hat{\eta}(Z^1, \dots, Z^n) \in \mathcal{T}} \sup_{\theta \in \Theta} \frac{1}{s} \mathbb{E}_{Q(P_\theta^{\otimes n})} |\hat{\eta}(Z^1, \dots, Z^n) - \eta|, \tag{1.6}$$

in the coordinate local case, and

$$\mathcal{R}_n(\alpha, \Theta) = \inf_{Q \in \mathcal{Q}_\alpha} \inf_{\hat{\eta} = \hat{\eta}(Z^1, \dots, Z^n) \in \mathcal{T}} \sup_{\theta \in \Theta} \frac{1}{s} \mathbb{E}_{Q(P_\theta^{\otimes n})} |\hat{\eta}(Z^1, \dots, Z^n) - \eta|, \tag{1.7}$$

in the coordinate global case, for $\Theta = \Theta_d^+(s, a)$ and $\Theta = \Theta_d(s, a)$. Note that these minimax risks are special forms of minimax risk (1.5) with the metric ρ chosen as the Hamming distance, and $\Phi : x \mapsto x/s$.
We provide lower bounds on minimax risks (1.6) and (1.7). Analyzing specific private estimation procedures, we also provide upper bounds. As corollaries, we derive necessary and sufficient conditions for exact recovery and almost full recovery to be possible. The definition of exact recovery and almost full recovery we use are the ones used in [12]. Let $(\Theta_d^+(s_d, a_d))_{d \geq 1}$ be a sequence of classes of sparse vectors. We will say that *almost full recovery is possible* for $(\Theta_d^+(s_d, a_d))_{d \geq 1}$ in the Coordinate Local case if there exists $Q \in \mathcal{Q}_\alpha^{CL}$ and a selector $\hat{\eta}$ such that

$$\lim_{d \to \infty} \sup_{\theta \in \Theta_d^+(s_d, a_d)} \frac{1}{s_d} \mathbb{E}_{Q(P_\theta^{\otimes n})} |\hat{\eta} - \eta| = 0.$$

We will say that *almost full recovery is impossible* for $(\Theta_d^+(s_d, a_d))_{d \geq 1}$ in the Coordinate Local case if

$$\liminf_{d \to +\infty} \inf_{Q \in \mathcal{Q}_\alpha^{CL}} \inf_{\hat{\eta} = \hat{\eta}(Z^1, \dots, Z^n) \in \mathcal{T}} \sup_{\theta \in \Theta_d^+(s,a)} \frac{1}{s_d} \mathbb{E}_{Q(P_\theta^{\otimes n})} |\hat{\eta} - \eta| > 0.$$

	$a \lesssim \frac{\sigma}{\sqrt{N}}$	$\frac{\sigma}{\sqrt{N}} \ll a \leq 2\sigma$	$a \geq 2\sigma$
$N := \frac{n\alpha^2}{d^2} \lesssim 1$	impossible	impossible	impossible
$N := \frac{n\alpha^2}{d^2} \gg 1$	impossible	possible, as soon as $a \gg \frac{\sigma}{\sqrt{N}}\sqrt{\log(N)\log(d)}$, if moreover $N \gg \log(N)\log(d)$	possible, if $N \gg \log(d)$

Table 1.1: Exact recovery in the Coordinate Local case. Similar results hold for almost full recovery with $\log(d)$ replaced by $\log(d/s)$.

We will say that *exact recovery is possible* for $(\Theta_d^+(s_d, a_d))_{d\geq 1}$ in the Coordinate Local case if there exists $Q \in \mathcal{Q}_\alpha^{CL}$ and a selector $\hat{\eta}$ such that

$$\lim_{d\to\infty} \sup_{\theta\in\Theta_d^+(s_d,a_d)} \mathbb{E}_{Q(P_\theta^{\otimes n})}|\hat{\eta} - \eta| = 0.$$

We will say that *exact recovery is impossible* for $(\Theta_d^+(s_d, a_d))_{d\geq 1}$ in the Coordinate Local case if

$$\liminf_{d\to+\infty} \inf_{Q\in\mathcal{Q}_\alpha^{CL}} \inf_{\hat{\eta}=\hat{\eta}(Z^1,\dots,Z^n)\in\mathcal{T}} \sup_{\theta\in\Theta_d^+(s,a)} \mathbb{E}_{Q(P_\theta^{\otimes n})}|\hat{\eta} - \eta| > 0.$$

We use similar definitions in the Coordinate Global case with $\mathcal{Q}_\alpha^{CL}$ replaced by $\mathcal{Q}_\alpha$.
The conditions for exact recovery to be possible are summarized in Table 1.1 for the Coordinate Local case and in Table 1.2 for the Coordinate Global case. In particular, our results show the following.

- In the Coordinate Local case, almost full recovery and exact recovery are impossible whatever the value of a if $n\alpha^2/d^2$ is bounded from above. This is in particular the case in the high-dimensional setting where $n \leq d$. This underlines a strong difference between the private setting and the classical setting, since [12] proved that in the non-private setting almost full recovery and exact recovery are possible for a large enough even if $n = 1$.

- However, in the regime $n\alpha^2/d^2 \to \infty$ with $n\alpha^2/d^2 \gg \log(n\alpha^2/d^2)\log(d)$ we observe a phase transition result (up to log factors) for exact recovery at the value $a^* = \sigma d/(\alpha\sqrt{n})$. Indeed, we get that exact recovery is impossible in the Coordinate Local

	$a \lesssim \sigma\sqrt{\frac{\log d}{Nd}}$	$\sigma\sqrt{\frac{\log d}{Nd}} \ll a \leq 2\sigma$	$a \geq 2\sigma$
$\frac{Nd}{\log d} \lesssim 1$	impossible	impossible	impossible if $a \leq \sigma\sqrt{\log\left(1+\frac{\log d}{16Nd}\right)}$
$\frac{Nd}{\log d} \gg 1$	impossible	possible, as soon as $a \gg \sigma\sqrt{\frac{\log d}{Nd}}\sqrt{\log(Nd)}$, if moreover $Nd \gg \log(Nd)\log(d)$	possible

Table 1.2: Exact recovery in the Coordinate Global case. We have set $N = n\alpha^2/d^2$ for a better comparison with the Coordinate Local case.

case for all $a \leq Ca^*$ and is possible for all $a \gg a^* \log^{1/2}(n\alpha^2/d^2)\log^{1/2}(d)$. A similar result holds for almost full recovery with $\log(d)$ replaced by $\log(d/s)$. Once again, this highlights a gap between the private and non-private cases since the phase transition occurs at $a^* = (\sigma/\sqrt{n})\sqrt{2\log(d/s-1)}$ (resp. $a^* = (\sigma/\sqrt{n})[\sqrt{2\log(d-s)} + \sqrt{2\log(s)}]$) in the non private setting for almost full recovery (resp. exact recovery), see [12].

- These results can be improved when allowing for all non-interactive (Coordinate Global) α-locally differentially private mechanims in the sense that almost full recovery and exact recovery are possible under weaker conditions and phase transitions occur at lower levels.

Our results can be a benchmark for working on more realistic models such as high-dimensional linear regression and clustering of high-dimensional vectors, see [58] and [57].

1.6 Contributions to LDP goodness-of-fit testing

1.6.1 State of the art

Goodness-of-fit testing problems consist in testing whether a given set of samples was drawn from a distribution P_0 or from any other distribution P with $d(P_0, P) \geq \rho$ for some distance between distributions d and some separation parameter $\rho > 0$. In Chapter 4, we

tackle this problem under local differential privacy constraints in the case where P and P_0 are assumed to have Hölder continuous densities f and f_0 and $d(P_0, P) = \|f - f_0\|_1$. Specifically, we will study the local minimax testing radius which corresponds to the smallest separation parameter for which there exists a private testing procedure whose firs type and second type error probabilities are bounded from above by a constant fixed in advance.

Goodness-of-fit testing for separation norm $\|\cdot\|_1$ has recently received great attention in the non-private setting. Working with discrete distributions, [75] and [19] provide upper and lower bounds on the number of samples that are necessary to distinguish $P = P_0$ from $\|P - P_0\|_1 \geq \rho$ with high probability. Balakrishnan and Wasserman [7] has revisited this problem in a minimax framework similar to the one considered in Chapter 4. Their results show that the local minimax testing radius strongly depends on the null distribution. They also investigate the continuous case, focusing on the case of Hölder continuous densities, providing results that are optimal for many choices of the null density f_0. We extend their result to the private setting.

Several papers have tackled goodness-of-fit problems under global differential privacy constraints, focusing on the case of multinomial distributions [37, 77, 62] or more general but finitely supported discrete distributions [16, 2, 4]. Early research on goodness-of-fit testing in the local setting of differential privacy include [36, 65, 3, 1]. Working with multinomial distributions, [36] study the asymptotic distributions of several test statistics. In [3] and the extended version [1], the authors provide upper and lower bounds on the number of samples necessary to distinguish $P = P_0 := \mathcal{U}(\llbracket 1, d \rrbracket)$ from $\mathrm{TV}(P, P_0) \geq \rho$ with high probability, and [65] investigates this problem for more general discrete null hypotheses. However, [3, 1, 65] obtain lower bounds over all test statistics based on data that have been privatized via a fixed specific privacy mechanism, while in Chapter 4 we will investigate optimality over all test statistics but also over all privacy mechanisms which satisfy the local differential privacy constraints.

Minimax goodness-of-fit under local differential privacy constraints has first been studied in [51] for discrete random variables. Upper and lower bounds on the minimax testing radius have been obtained. However, the authors consider only non-interactive mechanisms and the lower bound is only proven when P_0 is the uniform distribution. Minimax goodness-of-fit testing for discrete random variables (not necessarily finite supported) under local differential privacy constraints has further been studied in [10], where the authors aim at computing the minimax testing rates when $d(P, P_0) = \sum_{j=1}^{d} |P(j) - P_0(j)|^i$,

$i \in \{1, 2\}$. Interestingly, the authors show that the minimax testing rates are improved when allowing for sequentially interactive mechanisms compared to the case where only non-interactive mechanisms are allowed to be used to privatize the data.
Lam-Weil *et al.* [51] are also the first to tackle goodness-of-fit testing for continuous random variables under local differential privacy constraints. They consider $\|\cdot\|_2$ separation norm and study the minimax testing radius for the problem of goodness-of-fit for compactly supported densities over Besov balls $\mathcal{B}^s_{2,\infty}(L)$ in the special case of non-interactive local differential privacy. In a parallel work, [15] study the estimation of the integrated square of a density and prove that allowing for sequential interaction improves over minimax estimation rates obtained in the non-interactive scenario. As an application, they discuss non interactive and sequentially interactive $\mathbb{L}_2$ goodness-of-fit testing for densities, extending the results obtained in [51] to more general Besov balls $\mathcal{B}^s_{p,q}(L)$, to the interactive scenario, and to the case where f_0 is not assumed to be the uniform distribution but has to be compactly supported and bounded from below on its support.
In Chapter 4 we pursue these works on minimax density testing under local differential privacy constraints by considering densities in a Hölder class and the separation norm $\|\cdot\|_1$. Moreover, we allow for densities that tend to 0 on their support, with possibly unbounded support.

Let us mention that apart from goodness-of-fit, other testing problems have been studied over the past few years under differential privacy constraints, including independence testing, simple hypothesis testing and closeness testing. In the global setting, [37, 77, 62] study independence testing for categorical data, and [2, 4] consider closeness testing for discrete random variables. In the local setting of differential privacy, independence testing has been studied in [36] for categorical data and in [65, 1, 3] for more general discrete random variables, and [44, 45, 43] investigate simple hypothesis testing.

1.6.2 Contributions to goodness-of-fit testing for densities

In Chapter 4 we continue the work on minimax goodness-of-fit testing for densities initiated in [51] and [15]. While these papers focus on compactly supported densities which belong to a Besov ball, we investigate the case of Hölder continuous densities and we do not restrict ourselves to compactly supported functions.

Let $(X_1, ..., X_n) \in \mathcal{X}^n$ be i.i.d. with common probability density function (pdf) $f : \mathcal{X} \to \mathbb{R}_+$. We assume that f belongs to the smoothness class $H(\beta, L)$ for some smoothness

$0 < \beta \leq 1$ and $L > 0$, where

$$H(\beta, L) = \left\{ f : \mathcal{X} \to \mathbb{R}_+ \ : \ |f(x) - f(y)| \leq L|x - y|^\beta, \quad \forall x, y \in \mathcal{X} \right\}.$$

Given a probability density function f_0 in $H(\beta, L)$, we want to solve the goodness-of-fit test

$$\begin{aligned} H_0 \ &: \ f \equiv f_0 \\ H_1(\rho) \ &: \ f \in H(\beta, L) \text{ and } \|f - f_0\|_1 \geq \rho, \end{aligned}$$

where $\rho > 0$ under an α-local differential privacy constraint. We will consider the case where only non-interactive privacy mechanisms are allowed to be used and the case where both non-interactive and sequentially interactive mechanisms can be used for privatisation.

We adopt the following minimax framework. Given an α-LDP privacy mechanism Q, let $\Phi_Q = \{\phi : \mathcal{Z}^n \to \{0, 1\}\}$ denote the set of all tests based on $Z_1, \dots Z_n$, that is the set of all measurable functions of the privatized sample $Z_1, \dots Z_n$ which take value in $\{0, 1\}$ and are such that H_0 is rejected if $\phi(Z_1, \dots, Z_n) = 1$. The risk measure of a test ϕ for a given α-locally differentially private mechanism Q is defined by

$$\mathcal{R}_n(f_0, \rho, Q, \phi) := \sup_{f \in H_1(\rho)} \left\{ \mathbb{P}_{Q_{f_0}^n}(\phi = 1) + \mathbb{P}_{Q_f^n}(\phi = 0) \right\},$$

where Q_f^n denotes the distribution of $(Z_1, \dots, Z_n)$ when $X_1, ..., X_n$ have common probability density function f. If we denote by $\mathcal{Q}_\alpha$ the set of all α-locally differentially private (α-LDP) sequentially interactive mechanisms, then the sequentially interactive α-LDP minimax testing risk is defined by

$$\mathcal{R}_{n,\alpha}(f_0, \rho) := \inf_{Q \in \mathcal{Q}_\alpha} \inf_{\phi \in \Phi_Q} \mathcal{R}_n(f_0, \rho, Q, \phi).$$

We define similarly the non-interactive α-LDP minimax testing risk $\mathcal{R}_{n,\alpha}^{\mathrm{NI}}(f_0, \rho)$, where the first infimum is taken over the set $\mathcal{Q}_\alpha^{\mathrm{NI}}$ of all α-LDP non-interactive mechanisms instead of $\mathcal{Q}_\alpha$. Given $\gamma \in (0, 1)$, we study the α-LDP minimax testing radius defined by

$$\mathcal{E}_{n,\alpha}(f_0, \gamma) := \inf \left\{ \rho > 0 : \mathcal{R}_{n,\alpha}(f_0, \rho) \leq \gamma \right\},$$

and we define similarly $\mathcal{E}_{n,\alpha}^{\mathrm{NI}}(f_0, \gamma)$.

Our contributions can be summarized as follows and were submitted in [25]. First, when non-interactive privacy mechanisms are used, we present an α-locally differentially private such mechanism and construct a testing procedure based on the privatized data. In the non-private case, [7] suggests to combine a $\mathbb{L}_2$ procedure on a bulk set B where the density f_0 is bounded away from 0 by some small quantity and an $\mathbb{L}_1$ procedure on the tail $\overline{B} = \mathcal{X} \setminus B$. Following this recommendations, our procedure consists in the following steps :

1. Consider a compact set $B \subset \mathbb{R}$ (its choice depends on f_0, and on values of n and α).
2. Using the first half of the (privatized) data, define an estimator S_B of $\int_B (f - f_0)^2$.
3. Using the second half of the (privatized) data, define an estimator T_B of $\int_{\bar{B}} (f - f_0)$.
4. Reject H_0 if either $S_B \geq t_1$ or $T_B \geq t_2$.

Note that our procedure translates to the case of continuous distributions the one proposed in [10] for locally differentially private goodness-of-fit testing of discrete distributions. The study of the first and second type error probabilities of our test enables us to obtain an upper bound on the non-interactive testing radius $\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0, \gamma)$. This result is further complemented with a lower bound.

Next, we prove that these bounds can be improved when allowing for sequential interaction. This phenomenon, which can be observed neither for many estimation problems (see for instance [30],[63] and Chapter 2) nor for simple hypothesis testing [43], has recently been observed for the estimation of the integrated square of a density [15] and goodness-of-fit testing problems [10, 15].

Finally, we investigate the optimality of our results. We show that our lower bounds and upper bounds match up to a constant in the sequentially interactive scenario, and up to a logarithmic factor in the non-interactive scenario, for several choices of the null density f_0 including densities from uniform, normal, Beta, Cauchy, Pareto, exponential distributions. The results obtained for these examples are summarised in Table 1.3 for $\beta = 1$ and compared to the non-private separation rates.

	Non-private separation rate	Private separation rate, non-interactive scenario (up to a log factor)	Private separation rate, interactive scenario
$\mathcal{U}([a,b])$	$n^{-2/5}$	$(n\alpha^2)^{-2/7}$	$(n\alpha^2)^{-1/3}$
$\mathcal{N}(0,1)$	$n^{-2/5}$	$\log(n\alpha^2)^{3/7}(n\alpha^2)^{-2/7}$	$\log(n\alpha^2)^{1/3}(n\alpha^2)^{-1/3}$
Beta(a,b)	$n^{-2/5}$	$(n\alpha^2)^{-2/7}$	$(n\alpha^2)^{-1/3}$
Spiky null	$n^{-2/5}$	$(n\alpha^2)^{-2/7}$	$(n\alpha^2)^{-1/3}$
Cauchy$(0,a)$	$(\log n)^{4/5}n^{-2/5}$	$(n\alpha^2)^{-2/13}$	$(n\alpha^2)^{-1/5}$
Pareto(a,k)	$n^{-2k/(2+3k)}$	$(n\alpha^2)^{-2k/(7k+6)}$	$(n\alpha^2)^{-k/(3k+2)}$
Exp(λ)	$n^{-2/5}$	$\log(n\alpha^2)^{6/7}(n\alpha^2)^{-2/7}$	$\log(n\alpha^2)^{2/3}(n\alpha^2)^{-1/3}$

Table 1.3: Some examples of separation rates for different choices of densities f_0 and $\beta = 1$. The non-private separation rates can be found in [7]

Chapter 2

Local differential privacy: Elbow effect in optimal density estimation and adaptation over Besov ellipsoids

---

Abstract: *We address the problem of non-parametric density estimation under the additional constraint that only privatised data are allowed to be published and available for inference. For this purpose, we adopt a recent generalisation of classical minimax theory to the framework of local α-differential privacy and provide a lower bound on the rate of convergence over Besov spaces $\mathcal{B}^s_{pq}$ under mean integrated $\mathbb{L}^r$-risk. This lower bound is deteriorated compared to the standard setup without privacy, and reveals a twofold elbow effect. In order to fulfil the privacy requirement, we suggest adding suitably scaled Laplace noise to empirical wavelet coefficients. Upper bounds within (at most) a logarithmic factor are derived under the assumption that α stays bounded as n increases: A linear but non-adaptive wavelet estimator is shown to attain the lower bound whenever $p \geq r$ but provides a slower rate of convergence otherwise. An adaptive non-linear wavelet estimator with appropriately chosen smoothing parameters and thresholding is shown to attain the lower bound within a logarithmic factor for all cases.*

Based on [13].

2.1 Introduction

Problem statement

In the modern information age, increasingly more institutions are collecting and storing data. Provided that a certain amount of privacy is guaranteed, some of these institutions

might be willing to provide access to selected data sets. Examples of such data may include information about participants in a medical study, clients of a web service, or persons interviewed in a scientific survey. In this framework, the following questions arise naturally: How can data be sufficiently anonymised, given a rigorous definition of privacy, and what are the consequences for subsequent data analyses resulting from the chosen anonymisation procedure? The answer to these questions depends on several interacting parameters, namely the privacy definition at hand, the potential extent of collaboration of the involved data holding entities, and the kind of data mining tasks that should be feasible based on the private data.

In this paper, we consider the problem of non-parametric density estimation under local differential privacy as a special instance of the general problem sketched in the previous paragraph: For $i = 1, \dots, n$, the i-th data holder observes a real-valued random variable X_i distributed according to a probability density function f. The aim is that every data holder releases an anonymised view Z_i of X_i such that the privacy notion of *local differential privacy*, that is introduced next, is satisfied and that the density f can be estimated from the data $Z_1, \dots, Z_n$ in an optimal way.

Local differential private estimation

The notion of *local differential privacy* aggregates two different concepts, namely *local* privacy and *differential* privacy, that we explain in the sequel.

The qualitative notion of *local* privacy characterises how the different entities holding the data $X_1, \dots, X_n$ might interact to generate a private release Z. It is opposed to the concept of *global* privacy where the respective data holders share confidence in a common curator who has access to the ensemble of non-masked data $X_1, \dots, X_n$ and generates the releasable data from this complete information. In the *local* setup, such an authority that is trusted by all the parties, does not exist. However, some amount of interaction between the different parties is still allowed. The releasable data $Z_1, \dots, Z_n$ are obtained by successively applying suitable Markov kernels. Given $X_i = x_i$ and $Z_1 = z_1, \dots, Z_{i-1} = z_{i-1}$, the i-th dataholder draws

$$Z_i \sim Q_i(\cdot \mid X_i = x_i, Z_1 = z_1, \dots, Z_{i-1} = z_{i-1})$$

for some Markov kernel $Q_i : \mathscr{Z} \times \mathcal{X} \times \mathcal{Z}^{i-1} \to [0, 1]$ where the measure spaces of the non-private and private data are denoted with $(\mathcal{X}, \mathscr{X})$ and $(\mathcal{Z}, \mathscr{Z})$, respectively. An important special case is that of *non-interactive* local privacy where the random value of Z_i depends

on X_i only and must not depend on preceding values of Z. More precisely, in the non-interactive case we have

$$Z_i \sim Q(\cdot \mid X_i = x_i)$$

for some Markov kernel Q that does no longer depend on the index i. The non-interactive scenario comes along with some advantages in practice since it is balanced in the sense that the data holders play a symmetric role in the privatisation process, that can also be parallelized in this case. One should notice however that a restriction to non-interactive scenarios might result in slower rates of convergence for statistical inference. But as will be presented below, this is not the case in our density estimation framework, where rates are already optimal for estimators based on non-interactively privatised data.

From a mathematical point of view, however, allowing also interactive procedures does not lead to more technical proofs. Thus, we potentially allow non-interactive methods in our minimax analysis, although the anonymisation techniques proposed in this paper are exclusively non-interactive. Let us mention that for some tasks, however, interactive mechanisms provide natural and attractive alternatives (for instance, for private estimation in generalized linear models; see [30], Section 5.2.1).

The notion of *differential* privacy is a quantitative one and introduces a condition that makes the problem at hand mathematically tractable. We provide its definition for the locally private case only and refer the reader to [80] for a definition in the global case.

Definition 2.1.1. bla A sequence of Markov kernels $Q_i : \mathscr{Z} \times \mathcal{X} \times \mathcal{Z}^{i-1} \to [0,1]$ provides α-differential privacy if

$$\sup_{A \in \mathscr{Z}} \frac{Q_i(A \mid X_i = x, Z_1 = z_1, \ldots, Z_{i-1} = z_{i-1})}{Q_i(A \mid X_i = x', Z_1 = z_1, \ldots, Z_{i-1} = z_{i-1})} \leq \exp(\alpha) \quad \text{for all } x, x' \in \mathcal{X}.$$

In the non-interactive case, this condition is replaced with

$$\sup_{A \in \mathscr{Z}} \frac{Q(A \mid X_i = x)}{Q(A \mid X_i = x')} \leq \exp(\alpha) \quad \text{for all } x, x' \in \mathcal{X}.$$

We denote with $\mathcal{Q}_\alpha$ the set of all local α-differential private Markov kernels.

Thus, the parameter α quantifies the amount of privacy that is guaranteed: setting $\alpha = 0$ ensures perfect privacy whereas letting α tend to infinity softens the privacy restriction. In the non-interactive case, the defining property of α-differential privacy above ensures that all the probability measures $Q(\mathrm{d}z|X_i = x)$, $x \in \mathcal{X}$ are equivalent.

Hence, they admit densities $q(\cdot \mid X_i = x)$ with respect to a dominating measure (that can be chosen to be equal to $Q(\mathrm{d}z|X_i = x^*)$, for any $x^* \in \mathcal{X}$). In case of existence of such densities, we say that the property of α-differential privacy is satisfied if

$$\sup_{z\in\mathcal{Z}} \frac{q(z \mid X_i = x)}{q(z \mid X_i = x')} \leq \exp(\alpha) \quad \text{for all } x, x' \in \mathcal{X}. \tag{2.1}$$

A consequence from the definition of α-differential privacy is *plausible deniability* of the data in the following sense: Given the private view Z_i only, the power of any test of the null hypothesis $H_0 : X_i = x$ against the alternative $H_1 : X_i = x'$ with prescribed first error probability γ has power bounded from above by $\gamma \exp(\alpha)$ (see [80], Theorem 2.4).

Rate optimal density estimation over Besov ellipsoids

Let us briefly review some well-known results on non-parametric density estimation in the *non-private* setup where $X_1, \ldots, X_n$ can be observed. This classical model provides a natural benchmark for the model where additional privacy restrictions are imposed, and having in mind the results for this benchmark model turns out to be useful for understanding the ones for the model with privacy.

Density estimation from a sample $X_1, \ldots, X_n$ of observations is one of the paradigmatic problems in non-parametric statistics. A popular framework is that of minimax optimal estimation: Given a loss function ℓ (that is, a function mapping a pair of density functions (f, g) to some non-negative real number) and any class $\mathcal{F}$ of candidate density functions, the quantity of interest is the minimax risk

$$\mathcal{R}_n(\ell, \mathcal{F}) = \inf_{\widetilde{f}} \sup_{f\in\mathcal{F}} \mathbb{E}[\ell(\widetilde{f}, f)] \tag{2.2}$$

where the infimum is taken over all estimators (that is, $\sigma(X_1, \ldots, X_n)$-measurable functions). In this setup, an estimator $\widehat{f}$ is called *rate optimal* if

$$\sup_{f\in\mathcal{F}} \mathbb{E}[\ell(\widehat{f}, f)] \leq C(\ell, \mathcal{F})\mathcal{R}_n(\ell, \mathcal{F}).$$

Several function classes, loss functions and types of estimators have been intensively studied for the density estimation problem (see [72] and [38] for comprehensive overviews of the topic). Throughout this paper, we consider the integrated risk associated to $\mathbb{L}^r$-loss defined by $\ell(f, g) = \|f - g\|_r^r$ for $r \geq 1$. For the Besov spaces to be considered in the sequel,

wavelet methods have turned out particularly convenient. Given a father wavelet φ and a mother wavelet ψ associated to it, verifying some sufficient conditions (see conditions (5.10)–(5.12) in [41]), and an integer $j_0 \in \mathbb{Z}$, a wavelet basis of $\mathbb{L}^2(\mathbb{R})$ is given by

$$\{\varphi_{j_0 k} = 2^{j_0/2}\varphi(2^{j_0}(\cdot) - k) \colon k \in \mathbb{Z}\} \cup \{\psi_{jk} = 2^{j/2}\psi(2^j(\cdot) - k) \colon j \geq j_0, k \in \mathbb{Z}\}. \tag{2.3}$$

Given such a basis, the probability density f admits the following formal expansion (in $\mathbb{L}^2$ sense):

$$f = \sum_{k\in\mathbb{Z}} \alpha_{j_0 k}\varphi_{j_0 k} + \sum_{j\geq j_0}\sum_{k\in\mathbb{Z}} \beta_{jk}\psi_{jk} \tag{2.4}$$

where the wavelet coefficients are defined as

$$\alpha_{j_0 k} = \int_{\mathbb{R}} f(x)\varphi_{j_0 k}(x)\mathrm{d}x \qquad \text{and} \qquad \beta_{jk} = \int_{\mathbb{R}} f(x)\psi_{jk}(x)\mathrm{d}x.$$

An attractive property of wavelet expansions as (2.4) is that the membership of Besov spaces can be characterised in terms of its wavelet coefficients with respect to a well chosen wavelet basis. In the sequel, we will work under the following assumption on the father wavelet φ.

Assumption 2.1.2. Following [41], we assume that the father wavelet function φ generates a multiresolution analysis of $\mathbb{L}^2(\mathbb{R})$, that it is $N+1$ times weakly differentiable for some integer N, and that its derivative satisfies $\sup_x \sum_k |\varphi^{(N+1)}(x-k)| < \infty$ a.e. Moreover, we assume that there exists a bounded, non-increasing function Φ on $\mathbb{R}_+$ such that $|\varphi(u)| \leq \Phi(|u|)$ and that both $\int \Phi(|u|)\mathrm{d}u < \infty$ and $\int \Phi(|u|)|u|^N \mathrm{d}u < \infty$.

Note that no assumption is needed on the mother wavelet ψ since it is defined using the father wavelet. If the father wavelet function φ verifies Assumption 2.1.2 then, given parameters $0 < s < N+1$ and $1 \leq p, q \leq \infty$, the fact that f belongs to the Besov space $\mathcal{B}^s_{pq}$ is equivalent to $J_{spq}(f) < \infty$ where

$$J_{spq}(f) := \|\alpha_{0\cdot}\|_p + \left(\sum_{j\geq 0} (2^{j(s+1/2-1/p)}\|\beta_{j\cdot}\|_p)^q\right)^{1/q}$$

for $1 \leq q < \infty$ and the usual modification if $q = \infty$. Fixing such a wavelet basis, we consider Besov ellipsoids defined as

$$\mathcal{B}^s_{pq}(L) = \{f \colon \mathbb{R} \to \mathbb{R} : J_{spq}(f) \leq L\}.$$

Since our interest is in density estimation, a quite natural class to consider is

$$\mathcal{D}_{pq}^s = \mathcal{D}_{pq}^s(L,T) = \{f : f \in \mathcal{B}_{pq}^s(L), f \geq 0, \int_{\mathbb{R}} f(x)\mathrm{d}x = 1 \text{ and } \mathrm{supp}(f) \subseteq [-T,T]\},$$

where $\mathrm{supp}(f)$ denotes the support of the function f. Note that we consider here the Besov smoothness of f as a function defined on the whole real line, or, equivalently, that f belongs to a periodic Besov class. It would equally be possible to define Besov smoothness over the support $[-T,T]$. Then the wavelet basis has to be boundary corrected so that it detects the smoothness on this interval only and not the potential lack of smoothness of f at its boundary. We refer the reader to [38] for boundary corrected wavelets, that also dispose of all the properties that we need in the sequel.

It is well-known [38, 41, 24] that

$$\mathcal{R}_n(\|\cdot\|_r^r, \mathcal{D}_{pq}^s) \gtrsim \mathfrak{r}_n, \text{ where } \mathfrak{r}_n = \begin{cases} n^{-\frac{rs}{2s+1}}, & \text{if } p > \frac{r}{2s+1}, \\ (n/\log n)^{-\frac{r(s-1/p+1/r)}{2(s-1/p)+1}}, & \text{if } p \leq \frac{r}{2s+1} \text{ and } s \geq \frac{1}{p}, \end{cases} \tag{2.5}$$

and these rates are optimal or suboptimal by a logarithmic factor only (see [41] for an extensive discussion). The structural change of the rate between *dense zone* (where $p > r/(2s+1)$) and *sparse zone* (where $p \leq r/(2s+1)$) is sometimes called an *elbow effect*.

Moreover, in the dense case, we can distinguish the *homogeneous* zone when $p \geq r$ and the *non-homogeneous* zone where $r/(2s+1) < p < r$. In the homogeneous case, *linear* wavelet estimators of the form

$$\sum_{k\in\mathbb{Z}} \alpha'_{j_0k}\varphi_{j_0k}(x) + \sum_{j=j_0}^{j_1}\sum_{k\in\mathbb{Z}} \beta'_{jk}\psi_{jk}(x)$$

with $\alpha'_{j_0k} = \frac{1}{n}\sum_{i=1}^n \varphi_{j_0k}(X_i)$, $\beta'_{jk} = \frac{1}{n}\sum_{i=1}^n \psi_{jk}(X_i)$, and appropriately chosen j_0, j_1 are rate optimal whereas linear procedures are necessarily sub-optimal in the non-homogeneous case (see [41] and references therein). In this latter scenario as well as in the sparse case, non-linear estimators based on wavelet thresholding turn out to be optimal at least up to logarithmic factors.

Minimax framework under privacy constraints

Let us now describe how to extend the classical minimax setup in order to encompass the framework of local differential privacy. Since not only the estimation procedure but

also the Markov kernels guaranteeing local α-differential privacy can freely be chosen, it is natural to replace (2.2) with the local α-differential minimax risk defined as

$$\mathcal{R}^*_{n,\alpha}(\ell, \mathcal{F}) = \inf_{\substack{\widetilde{f} \\ Q \in \mathcal{Q}_\alpha}} \sup_{f \in \mathcal{F}} \mathbb{E}_{f,Q}[\ell(f, \widetilde{f})].$$

Here the infimum is taken both over all $(\mathcal{Z}, \mathscr{Z})$-measurable estimators of f and all Markov kernels guaranteeing local α-differential privacy. A tuple $(\widehat{Q}, \widehat{f})$ consisting of a privacy mechanism and an estimator $\widehat{f}$ is rate optimal (with respect to the local α-differential private risk) if

$$\sup_{f \in \mathcal{F}} \mathbb{E}_{f,\widehat{Q}}\left[\ell(f, \widehat{f})\right] \leq C(\ell, \mathcal{F}) \mathcal{R}^*_{n,\alpha}(\ell, \mathcal{F}).$$

The quantity $\mathcal{R}^*_{n,\alpha}(\ell, \mathcal{F})$ as well as the construction of optimal privacy mechanism and estimators represent the principal interest of the rest of the paper.

Related work

Research on statistical estimation under privacy constraints is rather recent. A landmark paper is [80] where research on the subject has been initiated and density estimation via histograms and orthogonal series in the global privacy setup have been discussed. In the same global framework, the article [40] considers anonymisation of functional data and discusses kernel density estimators as the main example. Local α-differential privacy was intensively studied in [29] and the companion article [30]. In [29] the authors show that the well-known technique of randomized response from survey statistics can be interpreted under the umbrella of local α-differential privacy. In the context of density estimation, [29] established minimax rates of convergence for the mean integrated squared error over Sobolev classes with arbitrary smoothness parameter $\beta \geq 1$. They establish the minimax rate of order $n^{-\beta/(\beta+1)}$ for the mean integrated squared error over Sobolev classes with $\beta = 1$ and show that this optimal rate can be attained by Laplace perturbation of empirical histogram coefficients. The papers [29, 30] provide also results for Sobolev classes with higher degrees of smoothness ($\beta > 1$) but in this case a mere perturbation of the empirical Fourier coefficients does not lead to a rate optimal method (see [29], Observation 1 for the non-optimality of this approach). By means of a more sophisticated sampling technique (see [29], or [30], Section 5.2.2), however, the authors derive the minimax rate of convergence that is $(n\alpha^2)^{-\beta/(\beta+1)}$ also in the general case. Furthermore, [29] provides private versions of classical information-theoretical bounds that allow to apply standard lower

bound techniques also in the private setup. In [63], the estimation of linear functionals in the framework of local privacy is considered and a characterisation of the rates of convergence in terms of moduli of continuity is obtained which is in parallel to well-known results for the non-private setup [23]. This general analysis contains the private estimation of a probability density at a fixed point under mean squared error as a special case.

Main results

In Section 2.2, in addition and in formal analogy to (2.5), we derive the following lower bound on the private minimax risk:

$$\mathcal{R}^*_{n,\alpha}(\|\cdot\|_r^r, \mathcal{D}^s_{pq}) \gtrsim \mathfrak{r}^*_{n,\alpha}, \tag{2.6}$$

$$\text{where } \mathfrak{r}^*_{n,\alpha} = \begin{cases} (n(e^\alpha-1)^2)^{-\frac{rs}{2s+2}}, & \text{if } p > \frac{r}{s+1}, \\ \left(\frac{n(e^\alpha-1)^2}{\log(n(e^\alpha-1)^2)}\right)^{-\frac{r(s-1/p+1/r)}{2(s-1/p)+2}}, & \text{if } p \le \frac{r}{s+1} \text{ and } s \ge \frac{1}{p}. \end{cases}$$

This lower bound is complemented by corresponding upper bound results: The anonymisation technique used to create the private views of the non-releasable data $X_1, \dots, X_n$ consists in an appropriately scaled version of the classical Laplace mechanism applied on the empirical wavelet coefficients (Section 2.3). The wavelet estimators considered in Sections 2.4 and 2.5 are based on the availability of the privatised data $Z_1, \dots, Z_n$ only. As in the non-private case, a linear wavelet estimator attains the given rate in the homogeneous case, that is, whenever $p \ge r$ (Section 2.4). In Section 2.5, we study non-linear estimators and show that an estimator using hard thresholding can nearly attain the lower bounds both in the dense and in the sparse zone.

Notational conventions

For real numbers a, b we write $[\![a, b]\!] = [a, b] \cap \mathbb{Z}$. We denote with C a generic constant that might change with every appearance. For two sequences $\{a_n\}_n$, $\{b_n\}_n$, we denote by $a_n \lesssim b_n$ that there exist some constant $C > 0$ and a fixed integer number N such that $a_n \le C b_n$, for all $n \ge N$. We say that $a_n \asymp b_n$, if both $a_n \lesssim b_n$ and $b_n \lesssim a_n$. If $b_n > 0$, we denote by $a_n \simeq b_n$ the fact that $a_n/b_n \to 1$ as $n \to \infty$. We recall that a centred Laplace distribution with parameter $\lambda > 0$ has the probability density function $p_\lambda(x) = \frac{1}{2\lambda}\exp(-\frac{|x|}{\lambda})$, for all real number x. In particular, if $X \sim p_\lambda$, then $\mathbb{E}|X|^k = k!\lambda^k$ for all $k \in \mathbb{N}$.

2.2 Lower bounds

The purpose of this section is to derive (2.6) and hence providing an analogue of (2.5) under local α-differential privacy. To this purpose, we proceed in two steps. The first lower bound, given in Proposition 2.2.1, is stronger in the private dense zone ($p > r/(s+1)$), whereas the second one, given in Proposition 2.2.2, dominates in the private sparse zone where $p \leq r/(s+1)$. An essential tool for both proofs is a strong information theoretical inequality (our Lemma 2.7.1) proved in [30], which states a bound for the Kullback-Leibler divergence between any distributions that have been processed through an arbitrary channel guaranteeing local α-differential privacy. We begin with the lower bound that is dominating in the dense zone.

Proposition 2.2.1. *Let $\alpha \in (0,\infty)$ and let $L, T > 0$. Then,*

$$\inf_{\substack{\widetilde{f} \\ Q\in\mathcal{Q}_\alpha}} \sup_{f\in\mathcal{D}^s_{pq}(L,T)} \mathbb{E}_{f,Q}\|\widetilde{f} - f\|_r^r \gtrsim (n(e^\alpha-1)^2)^{-\frac{rs}{2s+2}},$$

where the infimum is taken over all estimators $\widetilde{f}$ based on the private views $Z_1,\dots,Z_n$ and all Markov kernels $Q \in \mathcal{Q}_\alpha$ guaranteeing local α-differential privacy.

The proof of Proposition 2.2.1 is based on a reduction of the class $\mathcal{D}^s_{pq}$ to a finite number of hypotheses indexed by the vertices of a hypercube of suitable dimension. It is given in Section 2.7.1 in the appendix.

The following proposition complements Proposition 2.2.1 in stating a lower bound that is stronger in the private sparse zone.

Proposition 2.2.2. *Let $\alpha \in (0,\infty)$. Let $p \geq 1$, $s \geq 1/p$ and let $L, T > 0$. Then,*

$$\inf_{\substack{\widetilde{f} \\ Q\in\mathcal{Q}_\alpha}} \sup_{f\in\mathcal{D}^s_{pq}(L,T)} \mathbb{E}_{f,Q}\|\widetilde{f} - f\|_r^r \gtrsim \left(\frac{\log(n(e^\alpha-1)^2)}{n(e^\alpha-1)^2}\right)^{r\cdot\frac{s-1/p+1/r}{2(s-1/p)+2}},$$

where the infimum is taken over all estimators $\widetilde{f}$ based on the private views $Z_1,\dots,Z_n$ and all channels $Q \in \mathcal{Q}_\alpha$ providing local α-differential privacy.

The proof of Proposition 2.2.2 is given in Section 2.7.2 in the appendix.

Taking the maximum of the lower bounds obtained in Propositions 2.2.1 and 2.2.2 yields (2.6). In addition to our novel lower bounds, the known bounds (2.5) from the

non-private framework still hold true under local α-differential privacy since processing the original data $X_1, \dots, X_n$ through a privacy mechanism can be interpreted equivalently as imposing a restriction on the set of admissible estimators in (2.2). More precisely, the constraint of local α-differential privacy confines the set of potential estimators to those of the form $\widetilde{f} = f \circ Q$ where $Q \in \mathcal{Q}_\alpha$ and f is any measurable function. Thus,

$$\mathcal{R}^*_{n,\alpha} \geq \mathcal{R}_n \vee \mathfrak{r}^*_{n,\alpha} \geq \mathfrak{r}_n \vee \mathfrak{r}^*_{n,\alpha},$$

where the quantity $\mathfrak{r}_n$ is defined in (2.5). Hence, the following corollary holds.

Corollary 2.2.3. *Let the assumptions of Propositions 2.2.1 and 2.2.2 hold true. Then,*

$$\mathcal{R}^*_{n,\alpha}(\|\cdot\|_r^r, \mathcal{D}^s_{pq}) \gtrsim \begin{cases} n^{-\frac{rs}{2s+1}} \vee (n(e^\alpha-1)^2)^{-\frac{rs}{2s+2}}, & \text{if } p > \frac{r}{s+1}, \\ n^{-\frac{rs}{2s+1}} \vee \left(\frac{n(e^\alpha-1)^2}{\log(n(e^\alpha-1)^2)}\right)^{-\frac{r(s-1/p+1/r)}{2(s-1/p)+2}}, & \text{if } \frac{r}{2s+1} < p \leq \frac{r}{s+1}, \\ \left(\frac{n}{\log n}\right)^{-\frac{r(s-1/p+1/r)}{2(s-1/p)+1}} \vee \left(\frac{n(e^\alpha-1)^2}{\log(n(e^\alpha-1)^2)}\right)^{-\frac{r(s-1/p+1/r)}{2(s-1/p)+2}}, & \text{if } p \leq \frac{r}{2s+1}. \end{cases}$$

Note that the frontier between the dense and the sparse zone in the private framework is different from the one in the non-private framework leading to a partition into three regimes for the lower bound and a twofold elbow effect. Note that these lower bounds match the upper bounds derived in Section 2.4 and 2.5 at most up to logarithmic factors whenever α stays bounded as n increases. In addition, the bounds from the non-private setup dominate provided that α increases sufficiently fast in terms of n.

2.3 Privacy mechanisms

Let us denote with $X_1, \dots, X_n$ the real-valued random variables that represent the non-private observations held by the different data holders. We assume that $X_1, \dots, X_n \sim f$ for $f \in \mathcal{D}^s_{pq}$. In particular, the support of the density f is contained in the interval $[-T, T]$. In this section, we introduce a non-interactive privacy mechanism creating a private release $Z_1, \dots, Z_n$ based on the non-private sample that satisfies the defining property of α-differential privacy. For this purpose, we consider a wavelet basis as in (2.3). We assume in the sequel that the following condition on the parent wavelets is satisfied:

$$\varphi \text{ and } \psi \text{ are compactly supported on an interval } [-A, A]. \tag{W1}$$

The idea of the proposed anonymisation technique is to mask the empirical wavelet coefficients α'_{j_0k} and β'_{jk} for certain values of j. A consequence of (W1) and the compact support of f is that for any $j_0 \in \mathbb{Z}$ and any fixed resolution level $j \in \mathbb{Z}$, the corresponding α_{j_0k} and β_{jk} can *a priori* be non-zero for a finite number of k only. We denote the set of k with potentially non-zero α_{j_0k} by $\mathcal{N}_{j_0-1}$. Analogously, for $j \geq j_0$, the set of k with potentially non-zero β_{jk} is denoted with $\mathcal{N}_j$.

Let us now define two privacy mechanisms that will turn out to be convenient for the purposes of this paper. It will be sufficient to consider j_0, $j_1 \in \mathbb{N}$ from now on. Note that since the wavelets coefficients α'_{j_0k} and β'_{jk} are in any case zero for $k \notin \mathcal{N}_{j_0-1}$ and $k \notin \mathcal{N}_j$, respectively, we do not have to consider any privatisation of these quantities.

First privacy mechanism

For $i \in [\![1, n]\!]$, $j \in [\![j_0 - 1, j_1]\!]$, define

$$Z_{ijk} = \begin{cases} \varphi_{j_0k}(X_i) + \sigma_{j_0-1} W_{i,j_0-1,k}, & \text{if } j = j_0 - 1, k \in \mathcal{N}_{j_0-1}, \\ \psi_{jk}(X_i) + \tilde{\sigma}_j W_{ijk}, & \text{if } j \in [\![j_0, j_1]\!], k \in \mathcal{N}_j, \end{cases} \tag{2.7}$$

where W_{ijk} are independent Laplace distributed random variables with parameter 1,

$$\sigma_{j_0-1} = \frac{4c_A\|\varphi\|_\infty}{\alpha} \cdot 2^{j_0/2} \text{ and } \tilde{\sigma}_j = \frac{4c_A\|\psi\|_\infty}{\alpha} \cdot \frac{\sqrt{2}}{\sqrt{2}-1} \cdot 2^{j_1/2},$$

for $j \in [\![j_0, j_1]\!]$ with $c_A = 2\lceil A \rceil + 1$.

Second privacy mechanism

For $i \in [\![1, n]\!]$, $j \in [\![j_0 - 1, j_1]\!]$, define

$$Z_{ijk} = \begin{cases} \varphi_{j_0k}(X_i) + \sigma_{j_0-1} W_{i,j_0-1,k}, & \text{if } j = j_0 - 1, k \in \mathcal{N}_{j_0-1}, \\ \psi_{jk}(X_i) + \sigma_j W_{ijk}, & \text{if } j \in [\![j_0, j_1]\!], k \in \mathcal{N}_j, \end{cases} \tag{2.8}$$

where W_{ijk} are independent Laplace distributed random variables with parameter 1,

$$\sigma_{j_0-1} = \frac{4c_A\|\varphi\|_\infty}{\alpha} \cdot 2^{j_0/2} \text{ and } \sigma_j = \frac{4c_A\|\psi\|_\infty}{\alpha} \cdot \frac{2\nu-1}{\nu-1} \cdot (j \vee 1)^\nu \cdot 2^{j/2},$$

for $j \in [\![j_0, j_1]\!]$ with $c_A = 2\lceil A \rceil + 1$ and some $\nu > 1$.

Note that both privacy mechanisms in (2.7) and (2.8) are non-interactive because Z_{ijk} does only depend on X_i and not on $Z_{i'jk}$ for $i' \neq i$. The use of the Laplace distribution is convenient to provide α-differential privacy whereas the Gaussian distribution is suitable for weaker notions of privacy like approximate differential privacy and KL-divergence differential privacy [26]. The following proposition shows that both privacy mechanisms, $Z_i = (Z_{ijk})_{j\in[\![j_0-1,j_1]\!],k\in\mathcal{N}_j}$ satisfy the condition of α-differential privacy.

Proposition 2.3.1. *The privacy mechanisms given in (2.7) and (2.8) are local α-differential private.*

Proof. By definition of the privacy mechanism in (2.7), the conditional density of Z_i given $X_i = x_i$ can be written as

$$\begin{aligned} q^{Z_i|X_i=x_i}(z_i) &= \prod_{k\in\mathcal{N}_{j_0-1}} \frac{1}{2\sigma_{j_0-1}} \exp\left(-\frac{|z_{i,j_0-1,k} - \varphi_{j_0k}(x_i)|}{\sigma_{j_0-1}}\right) \\ &\quad \cdot \prod_{j=j_0}^{j_1} \prod_{k\in\mathcal{N}_j} \frac{1}{2\widetilde{\sigma}_j} \exp\left(-\frac{|z_{ijk} - \psi_{jk}(x_i)|}{\widetilde{\sigma}_j}\right). \end{aligned}$$

Thus, by the reverse and the ordinary triangle inequality,

$$\begin{aligned} \frac{q^{Z_i|X_i=x_i}(z_i)}{q^{Z_i|X_i=x_i'}(z_i)} &= \prod_{k\in\mathcal{N}_{j_0-1}} \exp\left(\frac{|z_{i,j_0-1,k} - \varphi_{j_0k}(x_i')| - |z_{i,j_0-1,k} - \varphi_{j_0k}(x_i)|}{\sigma_{j_0-1}}\right) \\ &\quad \cdot \prod_{j=j_0}^{j_1} \prod_{k\in\mathcal{N}_j} \exp\left(\frac{|z_{ijk} - \psi_{jk}(x_i')| - |z_{ijk} - \psi_{jk}(x_i)|}{\widetilde{\sigma}_j}\right) \\ &\leq \exp\left(\sum_{k\in\mathcal{N}_{j_0-1}} \frac{|\varphi_{j_0k}(x_i)| + |\varphi_{j_0k}(x_i')|}{\sigma_{j_0-1}}\right) \cdot \exp\left(\sum_{j=j_0}^{j_1} \sum_{k\in\mathcal{N}_j} \frac{|\psi_{jk}(x_i)| + |\psi_{jk}(x_i')|}{\widetilde{\sigma}_j}\right). \end{aligned}$$

Note that for any fixed x_i and arbitrary j, $\psi_{jk}(x_i) \neq 0$ holds only for at most $c_A = 2\lceil A\rceil + 1$ different k, and the same argument is valid for $\varphi_{j_0k}(x_i)$. Thus,

$$\begin{aligned} \frac{q^{Z_i|X_i=x_i}(z_i)}{q^{Z_i|X_i=x_i'}(z_i)} &\leq \exp\left(\frac{2\cdot 2^{j_0/2} c_A \|\varphi\|_\infty}{\sigma_{j_0-1}}\right) \cdot \exp\left(2\|\psi\|_\infty c_A \cdot \sum_{j=j_0}^{j_1} \frac{2^{j/2}}{\widetilde{\sigma}_j}\right) \\ &\leq \exp\left(\frac{\alpha}{2} + \frac{\alpha(\sqrt{2}-1)}{2\sqrt{2}} \sum_{j=j_0}^{j_1} \frac{2^{j/2}}{2^{j_1/2}}\right) \leq \exp(\alpha). \end{aligned}$$

For the privacy mechanism (2.8), analogous calculations yield for the conditional density

of Z_i given $X_i = x_i$ that

$$\frac{q^{Z_i|X_i=x_i}(z_i)}{q^{Z_i|X_i=x_i'}(z_i)} \leq \exp\left(\frac{2\cdot 2^{j_0/2}c_A\|\varphi\|_\infty}{\sigma_{j_0-1}}\right)\cdot\exp\left(2\|\psi\|_\infty c_A\cdot\sum_{j=j_0}^{j_1}\frac{2^{j/2}}{\sigma_j}\right)$$
$$\leq \exp\left(\frac{\alpha}{2}+\frac{\alpha}{2}\cdot\frac{\nu-1}{2\nu-1}(2+\sum_{j=2}^{\infty}j^{-\nu})\right)\leq\exp(\alpha),$$

where we used that $\sum_{j=j_0}^{j_1}(j\vee 1)^{-\nu}\leq\sum_{j=0}^{\infty}(j\vee 1)^{-\nu}$ and $\sum_{j=2}^{\infty}j^{-\nu}\leq(\nu-1)^{-1}$. □

2.4 Upper bound for linear wavelet estimators

The expansion (2.4) suggests to consider estimators of the form

$$\widehat{f}(x)=\sum_{k\in\mathcal{N}_{j_0-1}}\widehat{\alpha}_{j_0k}\varphi_{j_0k}(x)+\sum_{j=j_0}^{j_1}\sum_{k\in\mathcal{N}_j}\widehat{\beta}_{jk}\psi_{jk}(x)$$

with appropriate estimators $\widehat{\alpha}_{j_0k}$ and $\widehat{\beta}_{jk}$ of α_{j_0k} and β_{jk}, respectively. Note that in the local private framework, estimators of the wavelet coefficients are allowed to depend on the private views Z_{ijk} only but not on the hidden X_i. For the results concerning the linear estimator in this section, it suffices to consider the case $j_0 = 0$. In this case we put $\psi_{-1,k}=\varphi_{0,k}$, $\widehat{\beta}_{-1,k}=\widehat{\alpha}_{0k}$ and define a linear wavelet estimator through

$$\widehat{f}_{\text{lin}}(x)=\sum_{j=-1}^{j_1}\sum_{k\in\mathcal{N}_j}\widehat{\beta}_{jk}\psi_{jk}(x)\quad\text{with}\quad\widehat{\beta}_{jk}=\frac{1}{n}\sum_{i=1}^{n}Z_{ijk}.$$

Since $\mathbb{E}W_{ijk}=0$, the definition of $\widehat{\beta}_{jk}$ is natural and provides an unbiased estimate of the true wavelet coefficient β_{jk}.

Note that in the global differential privacy setting, a curator has access to the ensemble of original data and can release a privatised version of the estimator $\widehat{f}_{\text{lin}}$ where $\widehat{\alpha}_{j_0k}$ and $\widehat{\beta}_{jk}$ are allowed to depend on the whole non-masked sample $X_1,\dots,X_n$. However, in the local setting, privatisation of data must precede estimation. Therefore, in this later setup, we may only release for any $i=1,\dots,n$ the vector containing Z_{ijk} for all $j\in[\![j_0,j_1]\!]$ and k in $\mathcal{N}_j$. These vectors may be calculated by n distinct entities and neither the corresponding averages $\widehat{\alpha}_{j_0k},\widehat{\beta}_{jk}$ nor the final private estimator $\widehat{f}_{\text{lin}}$ can be directly released by any of these entities alone. We also underline the fact that the statistician needs to know the

wavelet basis used during privatisation and that (s)he can only reconstruct the wavelet estimator by using the given privatised sample. However, this additional information does not diminish the privacy as defined in this context.

The following proposition provides an upper bound for the estimator $\widehat{f}_{\text{lin}}$ in the so-called *matched case* when $r = p$. Its proof is given in Appendix 2.8.

Proposition 2.4.1. *Assume that the father wavelet φ satifies Assumption (2.1.2). Let $1 \leq p < \infty$ and Z_{ijk} defined as in (2.7). Then*

$$\sup_{f \in \mathcal{D}_{pq}^s} \mathbb{E}\|\widehat{f}_{\text{lin}} - f\|_p^p \lesssim 2^{-j_1 ps} + \left(\frac{2^{2j_1}}{n\alpha^2}\right)^{p/2} + \left(\frac{2^{j_1}}{n}\right)^{p/2}. \tag{2.9}$$

In particular, choosing $j_1 = j_1(n, \alpha)$ such that

$$2^{j_1} \asymp (n\alpha^2)^{\frac{1}{2s+2}} \wedge n^{\frac{1}{2s+1}}, \tag{2.10}$$

we obtain

$$\sup_{f \in \mathcal{D}_{pq}^s} \mathbb{E}\|\widehat{f}_{\text{lin}} - f\|_p^p \lesssim (n\alpha^2)^{-\frac{ps}{2s+2}} \vee n^{-\frac{ps}{2s+1}}. \tag{2.11}$$

The upper bound (2.11) suggests the following interpretation: As long as $\alpha^2 \geq n^{1/(2s+1)}$, the estimator $\widehat{f}_{\text{lin}}$ attains the rate $n^{-ps/(2s+1)}$ known to be optimal when the sample $X_1, \ldots, X_n$ is available. However, as soon as $\alpha^2 < n^{1/(2s+1)}$, this standard rate is deteriorated and the slower rate $(n\alpha^2)^{-ps/(2s+2)}$ is attained. As in [30], the alteration of the rate in comparison to the non-private framework concerns both the effective sample size (that changes from n to $n\alpha^2$) and the exponent appearing in the rate. We emphasize that the privacy mechanism (2.7) consists in a mere additive perturbation of the values $\varphi_{j_0k}(X_i)$ and $\psi_{jk}(X_i)$ by Laplace noise. This procedure is in notable contrast to the privacy mechanism suggested in [30] where a more complicated two-step procedure is used to release privatised coefficients in a Fourier series framework. In this Fourier series framework, the authors of [30] show that rate optimal estimation can be achieved by their two-step procedure whereas an additive perturbation of the Fourier coefficients by Laplace noise necessarily leads to non-optimal rates (see [30], Section 5.2.2). In our case, however, Proposition 2.4.1 together with Proposition 2.2.1 shows that rate optimal estimation can be achieved by means of additive Laplace perturbation only.

Although the risk bound of Proposition 2.4.1 is valid only in the matched case, it can

be extended to the case $r \neq p$ by means of the following proposition. Its proof is given in Appendix 2.8.

Corollary 2.4.2. *Assume that the father wavelet φ satisfies Assumption (2.1.2). Let $1 \leq p, r < \infty$ and Z_{ijk} defined as in (2.7), and put by $s' = s - (1/p - 1/r)_+$. Then, choosing j_1 as in (2.10) yields*

$$\sup_{f \in \mathcal{D}_{pq}^s} \mathbb{E}\|\widehat{f}_{\text{lin}} - f\|_r^r \lesssim (n\alpha^2)^{-\frac{rs'}{2s'+2}} \vee n^{-\frac{rs'}{2s'+1}}.$$

Corollary 2.4.2 together with Proposition 2.2.1 shows that the estimator $\widehat{f}_{\text{lin}}$ is of optimal order in the dense homogeneous zone where $p \geq r$ (which is equivalent to $s = s'$) and for α bounded from above. In analogy to [24], it would be possible to suggest a non-linear estimation procedure depending on s that is optimal (up to logarithmic factors in some cases) in the non-homogeneous dense case and in the sparse case as well. However, in Section 2.5, we directly propose a non-linear estimator that is adaptive to the smoothness s of the underlying density (as well as to the other parameters p and q of the Besov space).

2.5 Upper bounds for the non-linear adaptive estimator

In this section, the privacy mechanism is given by (2.8) in Section 2.3. We study the theoretical properties of the *non-linear* wavelet estimators of the form

$$\widetilde{f}_n(x) = \sum_k \widehat{\alpha}_{j_0 k} \varphi_{j_0 k}(x) + \sum_{j=j_0}^{j_1} \sum_k \widetilde{\beta}_{jk} \psi_{jk}(x) \tag{2.12}$$

where

$$\widehat{\alpha}_{j_0 k} = \frac{1}{n} \sum_{i=1}^n Z_{i, j_0 - 1, k} \quad \text{and} \quad \widetilde{\beta}_{jk} = \widehat{\beta}_{jk} \cdot \mathbb{1}_{\{|\widehat{\beta}_{jk}| \geq Kt\}},$$

and $\widehat{\beta}_{jk} = \frac{1}{n} \sum_{i=1}^n Z_{ijk}$ as in Section 2.4 (the choice of t and the value of the numerical constant K are specified in Theorem 2.5.1 and its proof below). Thus, non-linearity enters only with respect to the estimation of the detail coefficients β_{jk}.

Theorem 2.5.1. *Let the father wavelet φ satisfy Assumption 2.1.2 for some integer $N > 0$. Let the private views $Z_1, \ldots, Z_n$ of the sample $X_1, \ldots, X_n$ be generated with the*

privacy mechanism in (2.8). *Consider the estimator* $\widetilde{f}_n$ *defined in* (2.12) *with*

- $j_0 \in \mathbb{N}$ *such that* $2^{j_0} \asymp (n\alpha^2)^{\frac{1}{2(N+1)+2}} \wedge n^{\frac{1}{2(N+1)+1}}$,
- $j_1 = j_1' \wedge j_1''$ *where* j_1', $j_1'' \in \mathbb{N}$ *are such that*

$$2^{j_1'} \asymp \frac{n}{\log n}, \qquad \text{and} \qquad 2^{2j_1''} \asymp \frac{n\alpha^2}{\log(n\alpha^2)},$$

- $K = 4(\overline{L} + \sigma)$ *for some* $\overline{L} > 0$ *and* $\sigma = 4c_A\|\psi\|_\infty \cdot \frac{2\nu-1}{\nu-1}$ *with* ν *introduced in the definition of the second privacy mechanism,*
- $t = t_{j,n,\alpha} = \gamma \cdot \frac{j^{\nu+1/2}}{\sqrt{n}} \cdot (1 \vee \frac{2^{j/2}}{\alpha})$ *for* $j \in [\![j_0, j_1]\!]$ *and some sufficiently large constant* γ *(for instance,* $\gamma \geq r(N+1)$ *works).*

Then, the risk bound

$$\sup_{(s,p,q,L)\in\Theta} \sup_{f\in\mathcal{D}_{pq}^s(L,T)} \mathbb{E}\|\widetilde{f}_n - f\|_r^r \lesssim (\log n)^C \cdot \mathfrak{R}_{n,\alpha}^\star$$

where

$$\mathfrak{R}_{n,\alpha}^\star = \begin{cases} n^{-\frac{rs}{2s+1}} \vee (n\alpha^2)^{-\frac{rs}{2s+2}}, & \text{if } p > \frac{r}{s+1}, \\ n^{-\frac{rs}{2s+1}} \vee \left(\frac{n\alpha^2}{\log(n\alpha^2)}\right)^{-\frac{r(s-1/p+1/r)}{2(s-1/p)+2}}, & \text{if } \frac{r}{2s+1} < p \leq \frac{r}{s+1}, \\ \left(\frac{n}{\log n}\right)^{-\frac{r(s-1/p+1/r)}{2(s-1/p)+1}} \vee \left(\frac{n\alpha^2}{\log(n\alpha^2)}\right)^{-\frac{r(s-1/p+1/r)}{2(s-1/p)+2}}, & \text{if } p \leq \frac{r}{2s+1}, \end{cases}$$

and where

$$\Theta = (1/p, N+1) \times [1,\infty) \times [1,\infty) \times [\underline{L}, \overline{L}]$$

for some $0 < \underline{L} \leq \overline{L} < \infty$.

The proof of the Theorem is given in Appendix 2.9. Note that both the privacy mechanism and the estimator in Theorem 2.5.1 are independent of the quantities s, p, q, and L (only an upper bound $\overline{L}$ on L and an arbitrary value of $\nu > 1$ that should be chosen close to 1 are needed in order to specify the value of the constant K). Hence, the proposed procedure is adaptive over the collection of Besov spaces parametrized by the set Θ. Proposition 2.9.2 and Remark 2.9.3 show that the value $\overline{L}$ in the definition of K can be replaced with an upper bound on $\|f\|_\infty$. If such an a priori bound of $\|f\|_\infty$ is not

available, it might be replaced by some estimator of this quantity. The proposal of an appropriate estimator and its detailed analysis are outside the scope of our presentation and might be investigated in future work. The actual choice of the parameter ν is of secondary importance for our analysis: it should be larger than 1 in order to ensure convergence of the series $\sum_{j=2}^{\infty} j^{-\nu}$ in the proof of Proposition 2.3.1; however, it should not be too large since it appears in the final rates in the exponents of the additional logarithmic factors. We emphasize that neither the necessity nor the optimal expression of these logarithmic factors is not yet known in the framework of differential privacy.

2.6 Discussion

In this article, we have suggested refined methods for density estimation under the constraint of local α-differential privacy. By the use of estimators based on wavelet expansions, we have been able to obtain adaptive procedures that obtain the minimax rate of convergence up to an additional logarithmic factor only. To the best of our knowledge, adaptation to smoothness has not been considered in the framework of private estimation so far. Moreover, in allowing for general $\mathbb{L}^r$-risk and Besov ellipsoids we have widened the range of results in the privacy framework that has merely focused on $\mathbb{L}^2$-risk and Sobolev ellipsoids until now. We emphasize that in our minimax approach a careful coupling of a privacy mechanism associated with a corresponding estimator is provided. In the same spirit, one may produce alternative couplings and we think it would be useful to further compare the various privacy mechanisms from different perspectives.

A significant difference between our approach and the one suggested in Section 5.2.2 of [30] concerns the privacy mechanism: Whereas the procedure in [30] is built on a rather sophisticated sampling strategy aiming at the perturbation of empirical Fourier coefficients, our privacy mechanism consists in a simple Laplace perturbation of empirical wavelet coefficients. In [30] it has been observed (see the last paragraph of Section 5.2.2 in that paper) that such an approach is not feasible for the Fourier basis since it would lead to a suboptimal rate (under $\mathbb{L}^2$-risk) of order $(n\alpha^2)^{-2s/(2s+3)}$ over Sobolev ellipsoids of smoothness s instead of the optimal rate $(n\alpha^2)^{-s/(s+1)}$. A heuristic explanation for the easier accessibility of the problem by means of wavelet bases is given by their well-known *localisation* properties in contrast to the *global* Fourier basis.

Note that wavelet methods in the non-private framework do not necessarily suffer from a logarithmic loss in the rate (see, for instance, [24] where an additional logarithmic loss

only appears in the dense zone). The fact that we encounter this type of loss in our private scenario is caused by the term j^ν in the definition of the privacy mechanism (2.8). The problem whether and if so, how such logarithmic losses might be circumvented remains open and provides an interesting direction for future research.

Finally, let us sketch the connection between local private estimation in the non-interactive setup and statistical inverse problems, in particular, density deconvolution: On the one hand, in density deconvolution, the statistician is given a noisy sample $Z_1, \dots, Z_n$ where $Z_i = X_i + \varepsilon_i$ for $X_i \sim f$ and $\varepsilon_i \sim q$. Here, the density f is the quantity of interest and q an error density which is (at least in the overwhelming part of the literature) supposed to be known. In this setup, the Z_i are distributed according to the density g where

$$g(\cdot) = (K_q f)(\cdot) := \int q(\cdot - x) f(x) \mathrm{d}x \tag{2.13}$$

is the convolution of f with the error density q. It is well-known that the difficulty of reconstructing f from the sample $Z_1, \dots, Z_n$ is linked with the *degree of ill-posedness* of the inverse problem $g = K_q f$. The latter can be described either in terms of the sequence (λ_k^2) of eigenvalues of $K_q^* K_q$ (K_q^* denotes the adjoint operator of the linear operator K_q) or in terms of the decay of the Fourier transform of the error density q. General inverse problems of the form $Kf = g$ have been thoroughly investigated in [48] in the framework of a Gaussian white noise model. For Besov smooth signals f and $|\lambda_k| \asymp k^{-\rho}$ for some $\rho > 0$, [48] derived adaptive rates of estimation of f proportional to

$$\begin{cases} (\log n)^C n^{-\frac{rs}{2(s+\rho)+1}}, & \text{if } s > (\rho + \frac{1}{2})(\frac{r}{p} - 1), \\ (\log n)^C n^{-\frac{r(s-1/p+1/r)}{2(s-1/p+\rho)+1}}, & \text{if } s \le (\rho + \frac{1}{2})(\frac{r}{p} - 1) \text{ and } s \ge \frac{1}{p}. \end{cases}$$

On the other hand, the statistician who is given the non-interactive privatised sample $Z_1, \dots, Z_n$ is confronted with the problem of recovering f from a sample from the mixture density

$$g(\cdot) = (Kf)(\cdot) := \int q^{Z|X=x}(\cdot) f(x) \mathrm{d}x,$$

which is a special instance of an inverse problem and strongly resembles (2.13). In contrast to (2.13), however, the operator K is now not *a priori* given as a component of the problem but constitutes rather a part of its solution. In the local differential privacy framework, the statistician should select the operator K, corresponding to the choice of a privacy mechanism, subject to the two following constraints. First, the condition (2.1) concerning α-differential privacy must hold. Second, the least possible amount of information should

be smoothed out by the operator K. More precisely, denoting with ρ the degree of ill-posedness as above, the proofs of the lower bounds suggest that the least admissible value for ρ is $1/2$. Our privacy mechanisms, that is, our choices of K satisfy both constraints by leading to an overall estimation procedure that is nearly minimax.

We emphasize that the above interpretation of the locally differential private estimation problem does not rule out privacy mechanisms that add noise directly to the random variables $X_1, \ldots, X_n$ in principle. In this case, the probability density function q in (2.13) should satisfy the local α-differential privacy condition and have smoothness equal to $1/2$. An explicit density q satisfying (2.1) and having smoothness $\rho = 1/2$ does not seem trivial to find. As already mentioned, [30] have noted that adding Laplace noise directly to the observations cannot lead to an optimal procedure. Indeed, the convolution operator in this case has degree of ill-posedness corresponding to $\rho = 2$ which yields a suboptimal rate.

2.7 Appendix : Proofs of Section 2.2

We distinguish in the sequel the dense case and the sparse case that require different explicit constructions. However, for both proofs of the lower bounds we need the existence of a function f_0 with the following properties (see [41]):

- f_0 is a probability density,
- $J_{spq}(f_0) \leq L/2$,
- $\mathrm{supp}(f_0) \subseteq [-T, T]$,
- $f_0 \equiv c_0 > 0$ on some interval $[a, b]$.

In particular, $f_0 \in \mathcal{D}^s_{pq}(L/2, T)$.

The main tool in the proof of the lower bounds is adapted from [30]. It allows to reduce the problem to the study of the likelihoods of the non-privatised data and quantifies the loss of information in the process.

Suppose that we are given a finite indexed family of distributions $\{P_\nu, \nu \in \mathcal{V}\}$. Let V denote a random variable that is uniformly distributed over $\mathcal{V}$. Conditionally on $V = \nu$, suppose we sample a random vector $(X_1, \ldots, X_n)$ according to the product measure $P_\nu^{\otimes n} = P_\nu \otimes \ldots \otimes P_\nu$. Suppose that we draw an α-locally private sample $Z_1, \ldots, Z_n$ according to

a channel Q. Conditioned on $V = \nu$, $(Z_1, \dots, Z_n)$ is distributed according to the measure M_ν^n given by

$$M_\nu^n(S) := \int Q^n(S \mid x_1, \dots, x_n) \mathrm{d}P_\nu^{\otimes n}(x_1, \dots, x_n) \quad \text{for } S \in \sigma(\mathcal{Z}^n),$$

where $Q^n(\cdot \mid x_1, \dots, x_n)$ denotes the joint distribution on $\mathcal{Z}^n$ of the private sample $Z_{1:n}$ conditioned on $X_{1:n} = x_{1:n}$. In this setup, we have the following inequality.

Lemma 2.7.1. *[Based on [30], Theorem 1] Let $\alpha \geq 0$. For any α-locally differentially private conditional distribution Q and any $\nu, \nu' \in \mathcal{V}$, $\nu \neq \nu'$, we have in the above setting*

$$\mathrm{KL}(M_\nu^n, M_{\nu'}^n) + \mathrm{KL}(M_{\nu'}^n, M_\nu^n) \leq 4n(e^\alpha - 1)^2 \mathrm{TV}^2(P_\nu, P_{\nu'}).$$

Lemma 2.7.1 quantifies the property that α-differential privacy acts as a contraction on the space of probability measures.

2.7.1 Proof of Proposition 2.2.1

It is sufficient to prove the lower bound for n sufficiently large (the remaining finitely many n might merely further reduce the value of the numerical constant C). Let f_0 be the function introduced above. For fixed j (the choice of which will be specified later) define $\mathcal{I}_j$ as a maximal subset of $\mathbb{Z}$ such that $\mathrm{supp}(\psi_{jk}) \subset [a, b]$ and $\mathrm{supp}(\psi_{jk}) \cap \mathrm{supp}(\psi_{jk'}) = \emptyset$ if $k, k' \in \mathcal{I}_j$ with $k \neq k'$. Note that $N_j := |\mathcal{I}_j| \asymp 2^j$. Define

$$\mathcal{F} = \{f_\theta \colon f_\theta = f_0 + \gamma \sum_{k \in \mathcal{I}_j} \theta_k \psi_{jk} \text{ and } \theta = (\theta_k) \in \Theta := \{0, 1\}^{N_j}\}$$

where $\gamma = c(n(e^\alpha - 1)^2)^{-\frac{2s+1}{2(2s+2)}}$ for c sufficiently small and $2^j \asymp (n(e^\alpha - 1)^2)^{\frac{1}{2s+2}}$. For c sufficiently small, it holds $\gamma 2^{j/2} \|\psi\|_\infty \leqslant c_0$, which ensures that f_θ is non-negative for all $\theta \in \Theta$. One can easily check that $\int f_\theta = 1$ and $\mathrm{supp}(f_\theta) \subseteq [-T, T]$ for all $\theta \in \Theta$. Moreover, by the definition of γ, the choice of j and the equivalence of norms, we have

$$\begin{aligned} \|f_\theta\|_{spq} &\leq \|f_0\|_{spq} + c_1 \gamma 2^{j(s+1/2-1/p)} \Big(\sum_{k \in \mathcal{I}_j} |\theta_k|^p \Big)^{1/p} \\ &\leq \frac{L}{2} + c_1 \gamma 2^{j(s+1/2)} \leq \frac{L}{2} + C c c_1 \leq L, \end{aligned}$$

where the last inequality holds for c sufficiently small. Hence, $\mathcal{F} \subset \mathcal{D}^s_{pq}(L,T)$ and

$$\sup_{f\in\mathcal{D}^s_{pq}(L,T)} \mathbb{E}_f\|\widetilde{f}-f\|_r^r \geq \sup_{f\in\mathcal{F}} \mathbb{E}_f\|\widetilde{f}-f\|_r^r = \max_{\theta\in\Theta} \mathbb{E}_\theta\|\widetilde{f}-f_\theta\|_r^r.$$

Denoting by Δ_{jk} the support of ψ_{jk}, it holds for any estimator $\widetilde{f}$ of f that

$$\begin{aligned}
\mathbb{E}_\theta\|\widetilde{f}-f_\theta\|_r^r &= \mathbb{E}_\theta \int |\widetilde{f}(x)-f_\theta(x)|^r \mathrm{d}x \\
&\geq \sum_{k\in\mathcal{I}_j} \mathbb{E}_\theta \int_{\Delta_{jk}} |\widetilde{f}(x)-f_\theta(x)|^r \mathrm{d}x \\
&= \sum_{k\in\mathcal{I}_j} \mathbb{E}_\theta \int_{\Delta_{jk}} |\widetilde{f}(x)-f_0(x)-\gamma\theta_k\psi_{jk}(x)|^r \mathrm{d}x
\end{aligned}$$

since $f_\theta \equiv g_{\theta_k} := f_0 + \gamma\theta_k\psi_{jk}$ on Δ_{jk}. Set

$$\|\widetilde{f}-g_{\theta_k}\|^r_{r,\Delta_{jk}} = \int_{\Delta_{jk}} |\widetilde{f}(x)-g_{\theta_k}(x)|^r \mathrm{d}x = \int_{\Delta_{jk}} |\widetilde{f}(x)-f_0(x)-\gamma\theta_k\psi_{jk}(x)|^r \mathrm{d}x,$$

and $\check{\theta}_k = \mathrm{argmin}_{\theta\in\{0,1\}} \|\widetilde{f}-g_\theta\|_{r,\Delta_{jk}}$. It follows from the triangle inequality that

$$\begin{aligned}
2\|\widetilde{f}-g_{\theta_k}\|_{r,\Delta_{jk}} &\geq \|\widetilde{f}-g_{\theta_k}\|_{r,\Delta_{jk}} + \|\widetilde{f}-g_{\check{\theta}_k}\|_{r,\Delta_{jk}} \\
&\geq \|g_{\theta_k}-g_{\check{\theta}_k}\|_{r,\Delta_{jk}} \\
&= \gamma|\theta_k-\check{\theta}_k|\|\psi_{jk}\|_r.
\end{aligned}$$

Thus,

$$\begin{aligned}
\mathbb{E}_\theta\|\widetilde{f}-f_\theta\|_r^r &\geq \frac{\gamma^r}{2^r} \sum_{k\in\mathcal{I}_j} \mathbb{E}_\theta[|\check{\theta}_k-\theta_k|^r]\|\psi_{jk}\|_r^r \\
&= \frac{\gamma^r}{2^r}\|\psi_{j1}\|_r^r \cdot \mathbb{E}_\theta[d_H(\check{\theta},\theta)],
\end{aligned}$$

where d_H denotes the Hamming distance. Therefore,

$$\sup_{f\in\mathcal{D}^s_{pq}(L,T)} \mathbb{E}_f\|\widetilde{f}-f\|_r^r \geq \max_{\theta\in\Theta} \mathbb{E}_\theta\|\widetilde{f}-f_\theta\|_r^r \geq \frac{\gamma^r}{2^r}\|\psi_{j1}\|_r^r \cdot \inf_{\widetilde{\theta}} \max_{\theta\in\Theta} \mathbb{E}_\theta[d_H(\widetilde{\theta},\theta)].$$

In order to apply Lemma 2.7.2, we need to bound the Kullback-Leibler divergence between two different distributions M^n_θ and $M^n_{\theta'}$ of the private sample $(Z_1,\dots,Z_n)$ resulting from the sample $X_1,\dots,X_n$ if, for all $i \in [\![1,n]\!]$, X_i is distributed according to f_θ, $f_{\theta'}$ with

$d_H(\theta,\theta')=1$. We write $X_i\sim\mathbb{P}_\theta$ if X_i has density f_θ. Using Lemma 2.7.1 we obtain for any channel providing local α-differential privacy that

$$\mathrm{KL}(M_\theta^n,M_{\theta'}^n)\le 4(e^\alpha-1)^2 n\mathrm{TV}^2(\mathbb{P}_\theta,\mathbb{P}_{\theta'}).$$

Now, since $d_H(\theta,\theta')=1$ and $\theta,\theta'\in\Theta$, there exists $k_0\in\mathcal{I}_j$ such that

$$\begin{aligned}\mathrm{TV}(\mathbb{P}_\theta,\mathbb{P}_{\theta'})&=\frac{1}{2}\int|f_\theta(x)-f_{\theta'}(x)|\mathrm{d}x=\frac{1}{2}\int|\gamma\sum_{k\in\mathcal{I}_j}(\theta_k-\theta_k')\psi_{jk}(x)|\mathrm{d}x\\&=\frac{\gamma}{2}\int|\psi_{jk_0}(x)|\mathrm{d}x=\frac{1}{2}2^{-j/2}\gamma\|\psi\|_1,\end{aligned}$$

which implies that

$$\mathrm{KL}(M_\theta^n,M_{\theta'}^n)\le(e^\alpha-1)^2\|\psi\|_1^2 n2^{-j}\gamma^2\le c^2\|\psi\|_1^2C<\infty.$$

Applying Lemma 2.7.2 from the appendix with $N=N_j\gtrsim 2^j$ implies

$$\begin{aligned}\sup_{f\in\mathcal{D}_{pq}^s(L,T)}\mathbb{E}_f\|\widetilde{f}-f\|_r^r&\gtrsim\frac{\gamma^r}{2^r}2^{j(r/2-1)}\|\psi\|_r^r\cdot 2^j\\&\gtrsim(n(e^\alpha-1)^2)^{-\frac{rs}{2s+2}}.\end{aligned}$$

This implies the statement of the proposition since $\widetilde{f}$ and the channel distribution were arbitrary.

2.7.2 Proof of Proposition 2.2.2

We consider $f_0,\psi,\mathcal{I}_j$ and N_j as in the proof of Proposition 2.2.1, but consider now the set

$$\mathcal{F}=\{f_k=f_0+\gamma\cdot\psi_{jk},k\in\mathcal{I}_j\}\cup\{f_0\},$$

where j is chosen such that $2^j\simeq\left(\frac{n(e^\alpha-1)^2}{\log(n(e^\alpha-1)^2)}\right)^{\frac{1}{2(s+1-1/p)}}$ and $\gamma=c2^{-j(s+1/2-1/p)}$ for c sufficiently small. Let us first check that this choice of j and γ guarantees that $\mathcal{F}\subset\mathcal{D}_{pq}^s(L,T)$. First, we have $f_0\in\mathcal{D}_{pq}^s(L,T)$ and one can easily check that $\int f_k=1$ and $\mathrm{supp}(f_k)\subseteq[-T,T]$ for all $k\in\mathcal{I}_j$. Then, for any $k\in\mathcal{I}_j$, we have on $[a,b]$ that

$$f_k\ge c_0-\gamma\|\psi_{jk}\|_\infty\ge c_0-c2^{-j(s+1/2-1/p)}2^{j/2}\|\psi\|_\infty\ge c_0-c\|\psi\|_\infty\ge 0$$

for c sufficiently small, and outside of $[a,b]$ it holds $f_k = f_0 \geq 0$. Furthermore, for any $k \in \mathcal{I}_j$,

$$\|f_k\|_{spq} \leq \|f_0\|_{spq} + \gamma\|\psi_{jk}\|_{spq} \leq L/2 + c2^{-j(s+1/2-1/p)}\|\psi_{jk}\|_{spq} \leq L/2 + cc_1 \leq L$$

for c sufficiently small. Hence, $\mathcal{F} \subset \mathcal{D}^s_{pq}(L,T)$ and

$$\sup_{f\in\mathcal{D}^s_{pq}(L,T)} \mathbb{E}_f\|\widetilde{f} - f\|_r^r \geq \sup_{f\in\mathcal{F}} \mathbb{E}_f\|\widetilde{f} - f\|_r^r.$$

Now, we show that for $k, k' \in \mathcal{I}_j$, $k \neq k'$, the hypotheses f_k and $f_{k'}$, as well as the hypotheses f_k and f_0, are sufficiently separated in the sense of Lemma 2.7.3. For such k, k' we have:

$$\begin{aligned}\|f_k - f_{k'}\|_r^r \geq \|f_k - f_0\|_r^r &= \gamma^r 2^{rj(1/2-1/r)} \cdot \|\psi\|_r^r = c^r 2^{-rj(s+1/2-1/p)} 2^{rj(1/2-1/r)} \cdot \|\psi\|_r^r \\ &= c^r \|\psi\|_r^r 2^{-jr(s-1/p+1/r)} \\ &\geq C\left(\frac{\log(n(e^\alpha-1)^2)}{n(e^\alpha-1)^2}\right)^{r\cdot\frac{s-1/p+1/r}{2(s+1-1/p)}}.\end{aligned}$$

For $k \in \{0\} \cup \mathcal{I}_j$, let M_k^n be the distribution of the private sample $(Z_1, \ldots, Z_n)$ resulting from the sample $X_1, \ldots, X_n$ if for all $i \in [\![1,n]\!]$ X_i is distributed according to f_k. For all $k \in \mathcal{I}_j$ we have $M_k^n \ll M_0^n$. It remains to bound the quantity $\frac{1}{N_j}\sum_{k\in\mathcal{I}_j} \mathrm{KL}(M_k^n, M_0^n)$. We write $X_i \sim \mathbb{P}_k$ if X_i has density f_k, $k \in \{0\}\cup\mathcal{I}_j$. First consider the total variation distance between $\mathbb{P}_k$ and $\mathbb{P}_0$ for $k \in \mathcal{I}_j$:

$$\begin{aligned}\mathrm{TV}(\mathbb{P}_k, \mathbb{P}_0) &= \frac{1}{2}\int |f_k - f_0| = \frac{\gamma}{2}\int |\psi_{jk}| = \frac{\gamma}{2} 2^{-j/2}\|\psi\|_1 \\ &= \frac{c}{2}\|\psi\|_1 2^{-j(s-1/p+1)},\end{aligned}$$

and thus

$$\mathrm{TV}^2(\mathbb{P}_k, \mathbb{P}_0) \leq \frac{c^2}{4}\|\psi\|_1^2 C \cdot \frac{\log(n(e^\alpha-1)^2)}{n(e^\alpha-1)^2}.$$

Applying Lemma 2.7.1 gives

$$\frac{1}{N_j}\sum_{k\in\mathcal{I}_j} \mathrm{KL}(M_k^n, M_0^n) \leq c^2\|\psi\|_1^2 C \cdot \log(n(e^\alpha-1)^2). \tag{2.14}$$

Now, $\log(N_j) \geq \log(C2^j)$ and

$$\log(C2^j) > \frac{\log(n(e^\alpha-1)^2)}{2(s-1/p+1)}(1+o(1)) \geq \frac{1}{2}\frac{\log(n(e^\alpha-1)^2)}{2(s-1/p+1)}$$

for n sufficiently large, say $n \geq n_0$. Putting this estimate into (2.14) yields

$$\frac{1}{N_j}\sum_{k\in\mathcal{I}_j} \mathrm{KL}(M_k^n, M_0^n) \leq C\log(N_j)$$

for $n \geq n_0$ and $C < 1/8$ for c sufficiently small. We can then apply Lemma 2.7.3, which yields for $n \geq n_0$ that

$$\sup_{f\in\mathcal{D}_{pq}^s} \mathbb{E}_f\|\widetilde{f}-f\|_r^r \geq C\left(\frac{\log(n(e^\alpha-1)^2)}{n(e^\alpha-1)^2}\right)^{r\cdot\frac{s-1/p+1/r}{2(s-1/p)+2}}.$$

The statement of the proposition follows since both the estimator $\widetilde{f}$ and the privacy mechanism considered were arbitrary.

2.7.3 Further auxiliary results for the lower bound proofs

The following lemma is a Kullback-Leibler version of Assouad's lemma. As above, we denote by d_H the Hamming distance, that is, $d_H(\theta,\theta') = \sum_{i=1}^d \mathbb{1}_{\{\theta_i\neq\theta_i'\}}$ for $\theta,\theta' \in \mathbb{R}^d$.

Lemma 2.7.2 ([72], p. 118, Theorem 2.12)**.** *Denote with $\Theta = \{0,1\}^N$ the set of all binary sequences of length N. Let $\{\mathbb{P}_\theta : \theta \in \Theta\}$ be a set of 2^N probability measures on some measurable space $(\mathcal{X},\mathscr{A})$ and let the corresponding expectations be denoted by $\mathbb{E}_\theta$. Then*

$$\inf_{\widetilde{\theta}}\max_{\theta\in\Theta}\mathbb{E}_\theta[d_H(\theta,\widetilde{\theta})] \geq \frac{N}{2}\max\{\exp(-\beta)/2, 1-\sqrt{\beta/2}\}$$

provided that $\mathrm{KL}(\mathbb{P}_\theta,\mathbb{P}_{\theta'}) \leq \beta < \infty$ for all $\theta,\theta' \in \Theta$ with $d_H(\theta,\theta') = 1$.

For the lower bound in the sparse case we need the following lemma taken from [72].

Lemma 2.7.3 ([72], p. 101, Theorem 2.7)**.** *Assume that $M \geq 1$ and suppose that Θ contains elements $\theta_0,\theta_1,\ldots,\theta_M$ such that:*

(i) $d(\theta_j,\theta_k) \geq 2\Psi > 0$, for all $0 \leq j < k \leq M$,

(ii) $\mathbb{P}_j \ll \mathbb{P}_0$, *for all* $j = 1, \dots, M$, *and*

$$\frac{1}{M}\sum_{j=1}^{M} \mathrm{KL}(\mathbb{P}_j, \mathbb{P}_0) \leq \beta \log M$$

with $0 < \beta < 1/8$ *and* $\mathbb{P}_j = \mathbb{P}_{\theta_j}$, $j = 0, 1, \dots, M$. *Then*

$$\inf_{\widetilde{\theta}} \sup_{\theta \in \Theta} \mathbb{E}_\theta(d^r(\widetilde{\theta}, \theta)) \geq c(\beta)\Psi^r.$$

2.8 Appendix : Proofs of Section 2.4

2.8.1 Proof of Proposition 2.4.1

We give the proof for $p > 2$ only, which is based on Statement (ii) from Lemma 2.8.1. The proof for $1 \leq p \leq 2$ follows similarly using (i) instead. We decompose the risk of the estimator $\widehat{f}_{\mathrm{lin}}$ into approximation and stochastic error:

$$\mathbb{E}\|\widehat{f}_{\mathrm{lin}} - f\|_p^p \leq 2^{p-1}\{\mathbb{E}\|\widehat{f}_{\mathrm{lin}} - \mathbb{E}[\widehat{f}_{\mathrm{lin}}]\|_p^p + \|\mathbb{E}[\widehat{f}_{\mathrm{lin}}] - f\|_p^p\}.$$

The approximation term can be dealt with exactly as in the case of non-private data (see [41], p. 130),

$$\|\mathbb{E}[\widehat{f}_{\mathrm{lin}}] - f\|_p^p \leq C 2^{-spj_1},$$

and it remains to consider the stochastic term. Putting $\beta'_{-1,k} = \frac{1}{n}\sum_{i=1}^n \varphi(X_i - k)$ and $\beta'_{jk} = \frac{1}{n}\sum_{i=1}^n \psi_{jk}(X_i)$, we have

$$\begin{aligned}\widehat{f}_{\mathrm{lin}} - \mathbb{E}[\widehat{f}_{\mathrm{lin}}] = &\sum_{j=-1}^{j_1}\sum_{k\in\mathcal{N}_j} \beta'_{jk}\psi_{jk}(x) - \sum_{j=-1}^{j_1}\sum_{k\in\mathcal{N}_j} \beta_{jk}\psi_{jk}(x) \\ &+ \sum_{k\in\mathcal{N}_{-1}} \left(\frac{1}{n}\sum_{i=1}^n \sigma_{-1} W_{i,-1,k}\right)\psi_{-1,k}(x) + \sum_{j=0}^{j_1}\sum_{k\in\mathcal{N}_j}\left(\frac{1}{n}\sum_{i=1}^n \widetilde{\sigma}_j W_{ijk}\right)\psi_{jk}(x),\end{aligned}$$

which can be rewritten as

$$\begin{aligned}\widehat{f}_{\mathrm{lin}} - \mathbb{E}[\widehat{f}_{\mathrm{lin}}] = &\frac{1}{n}\sum_{i=1}^n K_{j_1+1}(x, X_i) - \mathbb{E}[K_{j_1+1}(x, X_1)] \\ &+ \sum_{k\in\mathcal{N}_{-1}} \left(\frac{1}{n}\sum_{i=1}^n \sigma_{-1} W_{i,-1,k}\right)\psi_{-1,k}(x) + \sum_{j=0}^{j_1}\sum_{k\in\mathcal{N}_j}\left(\frac{1}{n}\sum_{i=1}^n \widetilde{\sigma}_j W_{ijk}\right)\psi_{jk}(x),\end{aligned}$$

where $K_j(x,y) = 2^j \sum_k \varphi(2^j x - k)\bar{\varphi}(2^j y - k)$. We further decompose

$$\mathbb{E}\|\widehat{f}_{\text{lin}} - \mathbb{E}[\widehat{f}_{\text{lin}}]\|_p^p \le 2^{p-1}\mathbb{E}\left\|\frac{1}{n}\sum_{i=1}^n K_{j_1+1}(\cdot, X_i) - \mathbb{E}(K_{j_1+1}(\cdot, X_1))\right\|_p^p + 2^{p-1}\mathbb{E}\left\|\sum_{k\in\mathcal{N}_{-1}}\left(\frac{1}{n}\sum_{i=1}^n \sigma_{-1}W_{i,-1,k}\right)\psi_{-1,k} + \sum_{j=0}^{j_1}\sum_{k\in\mathcal{N}_j}\left(\frac{1}{n}\sum_{i=1}^n \sigma_j W_{ijk}\right)\psi_{jk}\right\|_p^p.$$

The first term on the right-hand side is analysed as in the non-private setup (see [41], p. 130) leading to the bound

$$\mathbb{E}\left\|\frac{1}{n}\sum_{i=1}^n K_{j_1+1}(\cdot, X_i) - \mathbb{E}[K_{j_1+1}(\cdot, X_1)]\right\|_p^p \le C\left(\frac{2^{j_1}}{n}\right)^{p/2}. \tag{2.15}$$

For the remaining term, we have by Tonelli's theorem

$$\mathbb{E}\int\left|\sum_{k\in\mathcal{N}_{-1}}\left(\frac{1}{n}\sum_{i=1}^n \sigma_{-1}W_{i,-1,k}\right)\psi_{-1,k}(x) + \sum_{j=0}^{j_1}\sum_{k\in\mathcal{N}_j}\left(\frac{1}{n}\sum_{i=1}^n \widetilde{\sigma}_j W_{ijk}\right)\psi_{jk}(x)\right|^p \mathrm{d}x = \frac{1}{n^p}\int_\Delta \mathbb{E}\left|\sum_{k\in\mathcal{N}_{-1}}\left(\sum_{i=1}^n \sigma_{-1}W_{i,-1,k}\right)\psi_{-1,k}(x) + \sum_{j=0}^{j_1}\sum_{k\in\mathcal{N}_j}\left(\sum_{i=1}^n \widetilde{\sigma}_j W_{ijk}\right)\psi_{jk}(x)\right|^p \mathrm{d}x$$

where Δ is some compact set the length of which depends on A and T only. The expectation inside the integral is bounded from above by Rosenthal's inequality (Statement (ii)

of Lemma 2.8.1):

$$
\begin{aligned}
&\mathbb{E}\left|\sum_{k\in\mathcal{N}_{-1}}\left(\sum_{i=1}^{n}\sigma_{-1}W_{i,-1,k}\right)\psi_{-1,k}(x)+\sum_{j=0}^{j_1}\sum_{k\in\mathcal{N}_j}\left(\sum_{i=1}^{n}\widetilde{\sigma}_j W_{ijk}\right)\psi_{jk}(x)\right|^p\\
&\lesssim \sum_{k\in\mathcal{N}_{-1}}\sum_{i=1}^{n}\mathbb{E}\left|\sigma_{-1}W_{i,-1,k}\psi_{-1,k}(x)\right|^p+\sum_{j=0}^{j_1}\sum_{k\in\mathcal{N}_j}\sum_{i=1}^{n}\mathbb{E}\left|\widetilde{\sigma}_j W_{ijk}\psi_{jk}(x)\right|^p\\
&\quad+\left(\sum_{k\in\mathcal{N}_{-1}}\sum_{i=1}^{n}\mathbb{E}|\sigma_{-1}W_{i,-1,k}\psi_{-1,k}(x)|^2+\sum_{j=0}^{j_1}\sum_{k\in\mathcal{N}_j}\sum_{i=1}^{n}\mathbb{E}|\widetilde{\sigma}_j W_{ijk}\psi_{jk}(x)|^2\right)^{p/2}\\
&= n\sum_{k\in\mathcal{N}_{-1}}\sigma_{-1}^p|\psi_{-1,k}(x)|^p\mathbb{E}|W_{1,-1,k}|^p+n\sum_{j=0}^{j_1}\sum_{k\in\mathcal{N}_j}\widetilde{\sigma}_j^p|\psi_{jk}(x)|^p\mathbb{E}|W_{1jk}|^p\\
&\quad+n^{p/2}\left(\sum_{k\in\mathcal{N}_{-1}}\sigma_{-1}^2|\psi_{-1,k}(x)|^2\mathbb{E}|W_{1,-1,k}|^2+\sum_{j=0}^{j_1}\widetilde{\sigma}_j^2\sum_{k\in\mathcal{N}_j}|\psi_{jk}(x)|^2\mathbb{E}|W_{1jk}|^2\right)^{p/2}\\
&\asymp n\sum_{k\in\mathcal{N}_{-1}}\sigma_{-1}^p|\psi_{-1,k}(x)|^p+n\sum_{j=0}^{j_1}\sum_{k\in\mathcal{N}_j}\widetilde{\sigma}_j^p|\psi_{jk}(x)|^p\\
&\quad+n^{p/2}\left(\sum_{k\in\mathcal{N}_{-1}}\sigma_{-1}^2|\psi_{-1,k}(x)|^2+\sum_{j=0}^{j_1}\widetilde{\sigma}_j^2\sum_{k\in\mathcal{N}_j}|\psi_{jk}(x)|^2\right)^{p/2}\\
&\asymp n\sum_{k\in\mathcal{N}_{-1}}|\psi_{-1,k}(x)|^p\frac{1}{\alpha^p}+n\sum_{j=0}^{j_1}\sum_{k\in\mathcal{N}_j}2^{j_1p/2}|\psi_{jk}(x)|^p\frac{1}{\alpha^p}\\
&\quad+n^{p/2}\left(\sum_{k\in\mathcal{N}_{-1}}|\psi_{-1,k}(x)|^2\frac{1}{\alpha^2}+\sum_{j=0}^{j_1}2^{j_1}\sum_{k\in\mathcal{N}_j}|\psi_{jk}(x)|^2\frac{1}{\alpha^2}\right)^{p/2}.
\end{aligned}
$$

Recall the definition of ψ_{jk} and noting that due to the boundedness of the support of the wavelet parents φ and ψ we have for any x and fixed j that $\psi_{jk}(x)\neq 0$ only for a finite number of k that is independent of j. Thus, using the last expression we bound from above as follows

$$
\begin{aligned}
&\int_\Delta\mathbb{E}\left|\sum_{k\in\mathcal{N}_{-1}}\left(\sum_{i=1}^{n}\sigma_{-1}W_{i,-1,k}\right)\psi_{-1,k}(x)+\sum_{j=0}^{j_1}\sum_{k\in\mathcal{N}_j}\left(\sum_{i=1}^{n}\widetilde{\sigma}_j W_{ijk}\right)\psi_{jk}(x)\right|^p\mathrm{d}x\\
&\leq C\left(\frac{n}{\alpha^p}+n2^{j_1p/2}\sum_{j=0}^{j_1}\frac{2^{jp/2}}{\alpha^p}+n^{p/2}\left(\frac{1}{\alpha^2}+2^{j_1}\sum_{j=0}^{j_1}\frac{2^j}{\alpha^2}\right)^{p/2}\right)\\
&\simeq \frac{n}{\alpha^p}+n\cdot\frac{2^{pj_1}}{\alpha^p}+\frac{n^{p/2}}{\alpha^p}+n^{p/2}\cdot\frac{2^{pj_1}}{\alpha^p}.
\end{aligned}
$$

Thus,

$$\mathbb{E}\int_\Delta \left| \sum_{k\in\mathcal{N}_{-1}} \left(\frac{1}{n}\sum_{i=1}^n \sigma_{-1} W_{i,-1,k}\right)\psi_{-1,k}(x) + \sum_{j=0}^{j_1}\sum_{k\in\mathcal{N}_j}\left(\frac{1}{n}\sum_{i=1}^n \tilde{\sigma}_j W_{ijk}\right)\psi_{jk}(x)\right|^p \mathrm{d}x$$
$$\lesssim \frac{2^{pj_1}}{\alpha^p n^{p-1}} + \left(\frac{2^{2j_1}}{n\alpha^2}\right)^{p/2}. \tag{2.16}$$

Combining (2.15) and (2.16) yields

$$\mathbb{E}\|\widehat{f}_{\mathrm{lin}} - \mathbb{E}[\widehat{f}_{\mathrm{lin}}]\|_p^p \lesssim \left(\frac{2^{2j_1}}{n\alpha^2}\right)^{p/2} + \left(\frac{2^{j_1}}{n}\right)^{p/2},$$

which proves (2.9). Choosing $j_1 = j_1(n,\alpha)$ as in (2.10) immediately implies (2.11).

2.8.2 Proof of Corollary 2.4.2

We distinguish between the cases $p \geq r$ and $p < r$.

2.8.2.0.1 ***1. Case*: $p > r$** In this case, $s' = s$. Let us consider the estimator $\widehat{f}_{\mathrm{lin}}$ with j_1 chosen as in Proposition 2.4.1. First note that there exists a constant $\bar{C} > 0$ such that the Lebesgue measure of $\mathrm{supp}(\widehat{f}_{\mathrm{lin}} - f))$ is bounded from above by a constant $\bar{C} > 0$. Then, applying Hölder's inequality and Proposition 2.4.1 yields

$$\mathbb{E}\|\widehat{f}_{\mathrm{lin}} - f\|_r^r \leq \bar{C}^{1-r/p}\Big(\mathbb{E}\|\widehat{f}_{\mathrm{lin}} - f\|_p^p\Big)^{r/p} \lesssim (n\alpha^2)^{-\frac{rs}{2s+2}} \vee n^{-\frac{rs}{2s+1}}.$$

2.8.2.0.2 ***2. Case*: $p \leq r$** In this case, $s' = s - 1/p + 1/r$. Thanks to the Besov embedding it holds $\mathcal{B}^s_{pq} \subset \mathcal{B}^{s'}_{rq}$, which implies $\mathcal{D}^s_{pq} \subset \mathcal{D}^{s'}_{rq}$. Thus, again using the upper bound for the matched case from Proposition 2.4.1,

$$\sup_{f\in\mathcal{D}^s_{pq}} \mathbb{E}\|\widehat{f}_{\mathrm{lin}} - f\|_r^r \leq \sup_{f\in\mathcal{D}^{s'}_{rq}} \mathbb{E}\|\widehat{f}_{\mathrm{lin}} - f\|_r^r$$
$$\lesssim (n\alpha^2)^{-\frac{rs'}{2s'+2}} \vee n^{-\frac{rs'}{2s'+2}},$$

which is the desired bound for the case $p \leq r$.

2.8.3 Inequalities for moments of sums of independent random variables

Lemma 2.8.1. *Let $X_1, \dots, X_n$ be independent centred random variables with $\mathbb{E}[|X_i|^r] < \infty$.*

(i) If $0 < r \leq 2$, then

$$\mathbb{E}\left(\left|\sum_{i=1}^{n} X_i\right|^r\right) \leq \left(\sum_{i=1}^{n} \mathbb{E}(X_i^2)\right)^{r/2}.$$

(ii) If $r > 2$, then there exists a constant $C = C(r)$ such that

$$\mathbb{E}\left(\left|\sum_{i=1}^{n} X_i\right|^r\right) \leq C\left\{\sum_{i=1}^{n} \mathbb{E}(|X_i|^r) + \left(\sum_{i=1}^{n} \mathbb{E}(X_i^2)\right)^{r/2}\right\}.$$

Inequality (i) follows directly from Jensen's inequality and concavity of $x \mapsto x^{r/2}$ for $0 < r \leq 2$. For a proof of inequality (ii) we refer to [61], p. 59, Theorem 2.9.

2.9 Appendix : Proof of Theorem 2.5.1

This section is devoted to the proof of Theorem 2.5.1. The main reasoning is given in Section 2.9.1 but some tedious calculations for this proof are deferred to Section 2.9.2. Sections 2.9.3 and 2.9.4 contain auxiliary results used in Section 2.9.2.

2.9.1 Proof of Theorem 2.5.1

As in the proof of the Corollary 2.4.2, we note that it is sufficient to prove the result for $p \leq r$ and one can deduce the result for $p > r$ as in the proof of this corollary.

We consider the upper bound $\mathbb{E}\|\widetilde{f}_n - f\|_r^r \leq 3^{r-1}(\mathbb{E}\|A\|_r^r + \mathbb{E}\|B\|_r^r + \|C\|_r^r)$ where

$$A = \sum_{k\in\mathbb{Z}} (\widehat{\alpha}_{j_0k} - \alpha_{j_0k})\varphi_{j_0k}, \quad B = \sum_{j=j_0}^{j_1} \sum_{k\in\mathbb{Z}} (\widetilde{\beta}_{jk} - \beta_{jk})\psi_{jk}, \quad \text{and}$$
$$C = \sum_{k\in\mathbb{Z}} \alpha_{j_1k}\varphi_{j_1k} - f.$$

We consider the risk bounds for $\mathbb{E}\|A\|_r^r$, $\mathbb{E}\|B\|_r^r$, and $\|C\|_r^r$ separately.

2.9.1.0.1 Upper bound for the term $\mathbb{E}\|A\|_r^r$: Putting $\alpha'_{j_0k} = \frac{1}{n}\sum_{i=1}^n \varphi_{j_0k}(X_i)$ it holds

$$\mathbb{E}\|A\|_r^r \le 2^{r-1}\mathbb{E}\Big\|\sum_{k\in\mathbb{Z}}(\alpha'_{j_0k}-\alpha_{j_0k})\varphi_{j_0k}\Big\|_r^r + 2^{r-1}\mathbb{E}\Big\|\sum_k\left(\frac{\sigma_{j_0-1}}{n}\sum_{i=1}^n W_{i,j_0-1,k}\right)\varphi_{j_0k}\Big\|_r^r.$$

The first term on the right-hand side is bounded by the compact support assumption on φ and using Lemma 1 from [24] as in the non-private case (see [24], p. 522):

$$2^{r-1}\mathbb{E}\Big\|\sum_{k\in\mathbb{Z}}(\alpha'_{j_0k}-\alpha_{j_0k})\varphi_{j_0k}\Big\|_r^r \le C(r)2^{j_0(r/2-1)}\sum_k\mathbb{E}|\alpha'_{j_0k}-\alpha_{j_0k}|^r \le C(r)\left(\frac{2^{j_0}}{n}\right)^{r/2}.$$

Concerning the second term, first, by Fubini's theorem

$$\mathbb{E}\Big\|\sum_k\left(\frac{\sigma_{j_0-1}}{n}\sum_{i=1}^n W_{i,j_0-1,k}\right)\varphi_{j_0k}\Big\|_r^r = \int\mathbb{E}|\sum_k\left(\frac{\sigma_{j_0-1}}{n}\sum_{i=1}^n W_{i,j_0-1,k}\right)\varphi_{j_0k}(x)|^r\mathrm{d}x,$$

and the integrand on the right-hand side can be bounded as follows: for $r>2$,

$$\begin{aligned}
\mathbb{E}|\sum_k\left(\frac{\sigma_{j_0-1}}{n}\sum_{i=1}^n W_{i,j_0-1,k}\right)\varphi_{j_0k}(x)|^r &\le \frac{C(r)}{n^r}\Bigg[\sigma_{j_0-1}^r\sum_k|\varphi_{j_0k}(x)|^r\sum_{i=1}^n\mathbb{E}|W_{i,j_0-1,k}|^r \\
&\qquad + \left(\sigma_{j_0-1}^2\sum_k|\varphi_{j_0k}(x)|^2\sum_{i=1}^n\mathbb{E}|W_{i,j_0-1,k}|^2\right)^{r/2}\Bigg] \\
&= \frac{C(r)}{n^r}\left[\sigma_{j_0-1}^r\sum_k|\varphi_{j_0k}(x)|^r nr! + \left(2n\sigma_{j_0-1}^2\sum_k|\varphi_{j_0k}(x)|^2\right)^{r/2}\right] \\
&\lesssim \frac{1}{n^r}\left[2^{rj_0}\cdot\frac{n}{\alpha^r} + \left(2^{2j_0}n\alpha^{-2}\right)^{r/2}\right] \\
&= \frac{2^{rj_0}}{n^{r-1}\alpha^r} + \left(\frac{2^{2j_0}}{n\alpha^2}\right)^{r/2},
\end{aligned}$$

whereas for $r\le 2$,

$$\mathbb{E}|\sum_k\left(\frac{\sigma_{j_0-1}}{n}\sum_{i=1}^n W_{i,j_0-1,k}\right)\varphi_{j_0k}(x)|^r \lesssim \left(\frac{2^{2j_0}}{n\alpha^2}\right)^{r/2}.$$

Thus, altogether,

$$\mathbb{E}\|A\|_r^r \lesssim \left(\frac{2^{j_0}}{n}\right)^{r/2} + \left(\frac{2^{2j_0}}{n\alpha^2}\right)^{r/2}.$$

Hence, for our choice of j_0 and grant to $s < N+1$ from Assumption 2.1.2, we obtain

$$\begin{aligned}
\mathbb{E}\|A\|_r^r &\lesssim \left(\frac{n^{\frac{1}{2(N+1)+1}}}{n}\right)^{r/2} + \left(\frac{(n\alpha^2)^{\frac{2}{2(N+1)+2}}}{n\alpha^2}\right)^{r/2} \\
&= n^{-\frac{r(N+1)}{2(N+1)+1}} + (n\alpha^2)^{-\frac{r(N+1)}{2(N+1)+2}} \\
&\leq n^{-\frac{rs}{2s+1}} + (n\alpha^2)^{-\frac{rs}{2s+2}} \\
&\lesssim n^{-\frac{rs}{2s+1}} \vee (n\alpha^2)^{-\frac{rs}{2s+2}} \vee \left(\frac{n}{\log n}\right)^{-\frac{r(s-1/p+1/r)}{2(s-1/p)+1}} \vee \left(\frac{n\alpha^2}{\log(n\alpha^2)}\right)^{-\frac{r(s-1/p+1/r)}{2(s-1/p)+2}},
\end{aligned}$$

and the bound on the right-hand side is the claimed rate.

2.9.1.0.2 Upper bound for the term $\mathbb{E}\|B\|_r^r$:

We consider the sets

$$\begin{aligned}
\widehat{B}_j &= \{k : |\widehat{\beta}_{jk}| > Kt_{j,n,\alpha}\}, & \widehat{S}_j &= \widehat{B}_j^{\complement}, \\
B_j &= \{k : |\beta_{jk}| > (K/2)t_{j,n,\alpha}\}, & S_j &= B_j^{\complement}, \\
B'_j &= \{k : |\beta_{jk}| > 2Kt_{j,n,\alpha}\}, & S'_j &= (B'_j)^{\complement},
\end{aligned}$$

and the decomposition

$$\begin{aligned}
B &= \sum_{j=j_0}^{j_1}\sum_k (\widehat{\beta}_{jk} - \beta_{jk})\psi_{jk}\left[\mathbb{1}_{\widehat{B}_j \cap S_j}(k) + \mathbb{1}_{\widehat{B}_j \cap B_j}(k)\right] \\
&\quad - \sum_{j=j_0}^{j_1}\sum_k \beta_{jk}\psi_{jk}\left[\mathbb{1}_{\widehat{S}_j \cap B'_j}(k) + \mathbb{1}_{\widehat{S}_j \cap S'_j}(k)\right] \\
&=: (e_{bs} + e_{bb}) - (e_{sb} + e_{ss}).
\end{aligned}$$

Appropriate bounds for the four terms $e_{bs}, e_{bb}, e_{sb}, e_{ss}$ are derived in Appendix 2.9.2.

2.9.1.0.3 Upper bound for the term $\|C\|_r^r$:

In the case we consider, $p \leq r$, we use the embedding $\mathcal{B}^s_{pq} \subset \mathcal{B}^{s'}_{r\infty}$, where we recall that $s' = s - \frac{1}{p} + \frac{1}{r}$. Then, it holds

$$\|\sum_{k\in\mathbb{Z}} \alpha_{j_1 k}\varphi_{j_1 k} - f\|_r^r \leq C\|f\|_{spq}^r \cdot 2^{-j_1 s' r}.$$

Moreover, with our choice of j_1,

$$\begin{aligned} 2^{-j_1 s' r} &\leq 2^{-j_1' s' r} + 2^{-j_1'' s' r} \\ &\lesssim \left(\frac{n}{\log n}\right)^{-\frac{rs'}{2(s-1/p)+1}} + \left(\frac{n\alpha^2}{\log(n\alpha^2)}\right)^{-\frac{rs'}{2(s-1/p)+2}}, \end{aligned}$$

and the sum on the right-hand side is bounded from above by the claimed rate.

2.9.2 Bounds for the terms e_{bs}, e_{bb}, e_{sb}, and e_{ss}

Consider the event A_{jk} defined via $A_{jk} = \{|\widehat{\beta}_{jk} - \beta_{jk}| > K/2 \cdot t_{j,n,\alpha}\}$. The concentration inequality (2.21) for this event as well as the bound (2.22) will be used frequently in the sequel without further reference. In the following, we bound the terms $\mathbb{E}\|e_{bs}\|_r^r$, $\mathbb{E}\|e_{bb}\|_r^r$, $\mathbb{E}\|e_{sb}\|_r^r$, and $\mathbb{E}\|e_{ss}\|_r^r$ separately.

2.9.2.1 Bound for e_{bs}

By the Cauchy-Schwarz inequality and the fact that $\widehat{B}_j \cap S_j \subset A_{jk}$,

$$\begin{aligned} \mathbb{E}\|e_{bs}\|_r^r &\lesssim \sum_{j=j_0}^{j_1} 2^{j(r/2-1)} \sum_{k \in \mathcal{N}_j} \mathbb{E}[|\widehat{\beta}_{jk} - \beta_{jk}|^r \mathbb{1}_{\widehat{B}_j \cap S_j}(k)] \\ &\leq \sum_{j=j_0}^{j_1} 2^{j(r/2-1)} \sum_{k \in \mathcal{N}_j} \left(\mathbb{E}[|\widehat{\beta}_{jk} - \beta_{jk}|^{2r}]\right)^{1/2} \cdot \mathbb{P}(|\widehat{\beta}_{jk} - \beta_{jk}| \geq K/2 \cdot t_{j,n,\alpha})^{1/2} \\ &\leq \sum_{j=j_0}^{j_1} 2^{j(r/2-1)} \sum_{k \in \mathcal{N}_j} (n^{-r/2} \vee j^{\nu r/2} 2^{jr/2} (n\alpha^2)^{-r/2}) \cdot 2^{-\gamma j/2} \\ &\leq \sum_{j=j_0}^{j_1} 2^{jr/2} 2^{-\gamma j/2} (n^{-r/2} \vee j^{\nu r/2} 2^{jr/2} (n\alpha^2)^{-r/2}) \\ &\leq n^{-r/2} \sum_{j=j_0}^{j_1} 2^{jr/2} 2^{-\gamma j/2} + (n\alpha^2)^{-r/2} j_1^{\nu r/2} \sum_{j=j_0}^{j_1} 2^{jr} 2^{-\gamma j/2} \end{aligned}$$

and this term is bounded from above by the claimed rate provided that $\gamma \geq 2r$.

2.9.2.2 Bound for e_{sb}

Using the relation $\widehat{S}_j \cap B'_j \subset A_{jk}$, we obtain

$$\begin{aligned}\mathbb{E}\|e_{sb}\|_r^r &\lesssim \sum_{j=j_0}^{j_1} 2^{j(r/2-1)} \sum_k |\beta_{jk}|^r \cdot \mathbb{E}[\mathbb{1}_{\widehat{S}_j \cap B'_j}(k)] \\ &\lesssim \sum_{j=j_0}^{j_1} 2^{j(r/2-1)} \sum_{k \in \mathcal{N}_j} |\beta_{jk}|^r \cdot \mathbb{P}(|\widehat{\beta}_{jk} - \beta_{jk}| \geq K \cdot t_{j,n,\alpha}) \\ &\lesssim \sum_{j=j_0}^{j_1} 2^{j(\frac{r}{2}-1-\gamma)} \|\beta_{j\cdot}\|_r^r.\end{aligned}$$

In the considered case $p \leq r$, we exploit the embedding $\mathcal{B}^s_{pq} \subseteq \mathcal{B}^{s'}_{rq}$ with $s' = s - \frac{1}{p} + \frac{1}{r}$ to get the bound

$$\|\beta_{j\cdot}\|_r \lesssim 2^{-j(s'+\frac{1}{2}-\frac{1}{r})}.$$

Hence,

$$\mathbb{E}\|e_{sb}\|_r^r \lesssim \sum_{j=j_0}^{j_1} 2^{j(\frac{r}{2}-1-\gamma)} 2^{-jr(s'+\frac{1}{2}-\frac{1}{r})} = \sum_{j=j_0}^{j_1} 2^{-j(\gamma+rs')} \lesssim 2^{-j_0(\gamma+rs')}$$

by the definition of j_0. Noting that

$$\begin{aligned}2^{-j_0(\gamma+rs')} &\lesssim (n\alpha^2)^{-\frac{\gamma+rs'}{2(N+1)+2}} \vee n^{-\frac{\gamma+rs'}{2(N+1)+1}} \\ &\leq (n\alpha^2)^{-\frac{rs}{2s+2}} \vee n^{-\frac{rs}{2s+1}}\end{aligned}$$

provided that γ is large enough ($\gamma \geq r(N+1)$ is sufficient), shows that $\mathbb{E}\|e_{sb}\|_r^r$ is at most of the same order as the claimed rate.

2.9.2.3 Bound for e_{bb}

Put $t'_{j,n,\alpha} = \gamma j^{\nu+1/2} n^{-1/2}$ and $t''_{j,n,\alpha} = \gamma j^{\nu+1/2}(n\alpha^2)^{-1/2}2^{j/2}$. Note that $t_{j,n,\alpha} = t'_{j,n,\alpha} \vee t''_{j,n,\alpha}$. For any $\rho \geq 0$, it holds

$$
\begin{aligned}
\mathbb{E}\|e_{bb}\|_r^r &\lesssim \sum_{j=j_0}^{j_1} 2^{j(r/2-1)} \sum_k \mathbb{E}[|\widehat{\beta}_{jk} - \beta_{jk}|^r \mathbb{1}_{\widehat{B}_j \cap B_j}(k)] \\
&\lesssim \sum_{j=j_0}^{j_1} 2^{j(r/2-1)} \sum_k (n^{-r/2} \vee j^{\nu r/2} 2^{jr/2} (n\alpha^2)^{-r/2}) \mathbb{1}_{B_j}(k) \\
&\lesssim \sum_{j=j_0}^{j_1} 2^{j(r/2-1)} \sum_k n^{-r/2} \mathbb{1}_{B_j}(k) \\
&\quad + \sum_{j=j_0}^{j_1} 2^{j(r/2-1)} \sum_k j^{\nu r/2} 2^{jr/2} \cdot (n\alpha^2)^{-r/2} \mathbb{1}_{B_j}(k) \\
&\lesssim \sum_{j=j_0}^{j_1} 2^{j(r/2-1)} (t'_{j,n,\alpha})^r \cdot \sum_k |\beta_{jk}|^\rho (t'_{j,n,\alpha})^{-\rho} \\
&\quad + \sum_{j=j_0}^{j_1} 2^{j(r/2-1)} (t''_{j,n,\alpha})^r \sum_k |\beta_{jk}|^\rho (t''_{j,n,\alpha})^{-\rho} \\
&\lesssim \underbrace{\sum_{j=j_0}^{j_1} 2^{j(r/2-1)} (t'_{j,n,\alpha})^{r-\rho} \sum_k |\beta_{jk}|^\rho}_{=:S_1} + \underbrace{\sum_{j=j_0}^{j_1} 2^{j(r/2-1)} (t''_{j,n,\alpha})^{r-\rho} \cdot \sum_k |\beta_{jk}|^\rho}_{=:S_2}. \qquad (2.17)
\end{aligned}
$$

As this argument shows, one can even choose distinct values of ρ for different j, which will be used in the following calculations. Note that

$$\sum_k |\beta_{jk}|^p \lesssim 2^{-jp(s+1/2-1/p)},$$

and, if $\rho \leq p$, by Hölder's inequality

$$\sum_k |\beta_{jk}|^\rho \leq 2^{j(1-\rho/p)} \Big(\sum_k |\beta_{jk}|^p \Big)^{\rho/p} \leq 2^{j(1-\rho/p)} 2^{-j\rho(s+1/2-1/p)} = 2^{-j\rho(s+1/2-1/\rho)}.$$

In the sequel, we consider three different cases corresponding to the three regimes in the statement of Theorem 2.5.1.

2.9.2.3.1 *1. Case*: $p > r/(s+1)$

- Bound for S_1: Set $q_1 = r/(2s+1)$ and define $\kappa_1 \in \mathbb{N}$ such that

$$2^{\kappa_1(r/2-p/2-sp)} \asymp n^{-\frac{p-q_1}{2}}.$$

Choosing $\rho < q_1 \leq p$ for the indices $j \in [\![j_0, \kappa]\!]$, we obtain (note that $s+1/2 = r/(2q_1)$)

$$\begin{aligned}
\sum_{j=j_0}^{\kappa_1} 2^{j(r/2-1)}(t'_{j,n,\alpha})^{r-\rho} \sum_k |\beta_{jk}|^\rho &\lesssim j_1^{(r-\rho)(\nu+1/2)} n^{-(r-\rho)/2} \sum_{j=j_0}^{\kappa_1} 2^{j(r/2-1)} \sum_k |\beta_{jk}|^\rho \\
&\leq j_1^{(r-\rho)/2} n^{-(r-\rho)/2} \sum_{j=j_0}^{\kappa_1} 2^{j(r/2-1)} 2^{j(1-\rho/p)} 2^{-j\rho(s+1/2-1/p)} \\
&\lesssim j_1^{(r-\rho)(\nu+1/2)} n^{-(r-\rho)/2} \sum_{j=j_0}^{\kappa_1} 2^{j(r/2-\rho(s+1/2))} \\
&\lesssim (\log n)^C n^{-(r-\rho)/2} 2^{\kappa_1(r/2-\frac{r\rho}{2q_1})} \\
&\asymp (\log n)^C n^{(q_1-r)/2} \\
&= (\log n)^C n^{-\frac{rs}{2s+1}}.
\end{aligned}$$

Choosing $\rho = p$ for indices $j \in [\![\kappa_1 + 1, j_1]\!]$, we obtain

$$\begin{aligned}
\sum_{j=\kappa_1+1}^{j_1} 2^{j(r/2-1)}(t'_{j,n,\alpha})^{r-\rho} \sum_k |\beta_{jk}|^\rho &\lesssim j_1^{(r-p)(\nu+1/2)} n^{-(r-p)/2} \sum_{j=\kappa_1+1}^{j_1} 2^{j(r/2-sp-p/2)} \\
&\lesssim j_1^{(r-p)(\nu+1/2)} n^{-(r-p)/2} 2^{\kappa_1(r/2-sp-p/2)} \\
&\lesssim j_1^{(r-p)(\nu+1/2)} n^{-(r-q_1)/2} \\
&\asymp (\log n)^C \cdot n^{-\frac{rs}{2s+1}}.
\end{aligned}$$

- Bound for S_2: Set $q_2 = r/(s+1)$ and define $\kappa_2 \in \mathbb{N}$ such that

$$2^{\kappa_2(r-p-sp)} \asymp (n\alpha^2)^{-\frac{p-q_2}{2}}.$$

Choosing $\rho < q_2 \leq p$ for the indices $j \in [\![j_0, \kappa_2]\!]$, we obtain (note that $s+1 = r/q_2$)

$$\begin{aligned}\sum_{j=j_0}^{\kappa_2} 2^{j(r/2-1)}(t''_{j,n,\alpha})^{r-\rho} \cdot \sum_k |\beta_{jk}|^\rho &\lesssim j_1^{(r-\rho)(\nu+1/2)}(n\alpha^2)^{-(r-\rho)/2} \sum_{j=j_0}^{\kappa_2} 2^{j(r-\rho(s+1))} \\ &\lesssim (\log n)^C (n\alpha^2)^{-(r-\rho)/2} 2^{\kappa_2(r-\frac{r\rho}{q_2})} \\ &\asymp (\log n)^C (n\alpha^2)^{(q_2-r)/2} \\ &= (\log n)^C (n\alpha^2)^{-\frac{rs}{2s+2}}.\end{aligned}$$

Choosing $\rho = p$ for indices $j \in [\![\kappa_2 + 1, j_1]\!]$, we obtain

$$\begin{aligned}\sum_{j=\kappa_2+1}^{j_1} 2^{j(r/2-1)}(t''_{j,n,\alpha})^{r-\rho} \sum_k |\beta_{jk}|^\rho &\lesssim j_1^{(r-p)(\nu+1/2)}(n\alpha^2)^{-(r-p)/2} \sum_{j=\kappa_2+1}^{j_1} 2^{j(r-sp-p)} \\ &\lesssim j_1^{(r-p)(\nu+1/2)}(n\alpha^2)^{-(r-p)/2} 2^{\kappa_2(r-sp-p)} \\ &\lesssim (\log n)^C \cdot (n\alpha^2)^{(q_2-r)/2} \\ &= (\log n)^C \cdot (n\alpha^2)^{-\frac{rs}{2s+2}}.\end{aligned}$$

2.9.2.3.2 *2. Case*: $p \in (r/(2s+1), r/(s+1)]$

- Bound for S_1: The sum S_1 can be dealt with as in the first case, since the choices of q_1 and κ_1 from that case are still legitimated for $p \in (r/(2s+1), r/(s+1)]$.

- Bound for S_2: In order to bound S_2 in the second case, define q_2 and κ_2 via the relations

$$q_2 = r \cdot \frac{1 - 1/r}{s - 1/p + 1} \qquad \text{and} \qquad 2^{\kappa_2} \asymp (n\alpha^2)^{\frac{q_2}{2(r-1)}}.$$

To deal with the sum over $j \in [\![j_0, \kappa_2]\!]$, we take $\rho = p$ and obtain

$$\begin{aligned}\sum_{j=j_0}^{\kappa_2} 2^{j(r/2-1)}(t''_{j,n,\alpha})^{r-\rho} \sum_k |\beta_{jk}|^\rho &\lesssim j_1^{(\nu+1/2)(r-p)}(n\alpha^2)^{(r-p)/2} \sum_{j=j_0}^{\kappa_2} 2^{j(r-sp-p)} \\ &\lesssim (\log n)^C (n\alpha^2)^{-(r-p)/2} \sum_{j=j_0}^{\kappa_2} 2^{j(r-1)(1-p/q_2)} \\ &\lesssim (\log n)^C (n\alpha^2)^{-(r-p)/2} 2^{\kappa_2(r-1)(1-p/q_2)} \\ &\asymp (\log n)^C (n\alpha^2)^{(q_2-r)/2} \\ &= (\log n)^C (n\alpha^2)^{-\frac{rs'}{2(s-1/p)+2}}\end{aligned}$$

For the sum over indices $j \in [\![\kappa_2+1, j_1]\!]$, we choose $\rho > q_2 > p$, and obtain by monotony of ℓ^ω-norms in ω, and putting $s'' = s + 1/2 - 1/p$ that

$$\begin{aligned}
\sum_{j=\kappa_2+1}^{j_1} 2^{j(r/2-1)} (t''_{j,n,\alpha})^{r-\rho} \sum_k |\beta_{jk}|^\rho &\lesssim j_1^{(\nu+1/2)(r-\rho)} (n\alpha^2)^{-\frac{r-\rho}{2}} \sum_{j=\kappa_2+1}^{j_1} 2^{j(r-\rho/2-1-\rho s'')} \\
&\lesssim (\log n)^C (n\alpha^2)^{-\frac{r-\rho}{2}} \sum_{j=\kappa_2+1}^{j_1} 2^{j(r-1-\rho/2-\rho s'')} \\
&= (\log n)^C (n\alpha^2)^{-\frac{r-\rho}{2}} \sum_{j=\kappa_2+1}^{j_1} 2^{j(r-1)(1-\rho/q_2)} \\
&\lesssim (\log n)^C (n\alpha^2)^{-\frac{r-\rho}{2}} 2^{\kappa_2(r-1)(1-\rho/q_2)} \\
&\asymp (\log n)^C (n\alpha^2)^{\frac{q_2-r}{2}} \\
&= (\log n)^C (n\alpha^2)^{-\frac{rs'}{2(s-1/p)+2}}.
\end{aligned}$$

2.9.2.3.3 *3. Case*: $p \le r/(2s+1)$

- Bound for S_1: Put

$$q_1 = r \cdot \frac{1/2 - 1/r}{s + 1/2 - 1/p},$$

and choose $\kappa_1 \in \mathbb{N}$ such that

$$2^{\kappa_1} \asymp n^{\frac{1}{2}\frac{q_1}{r/2-1}}.$$

Then, taking $\rho = p$ for the indices $j \in [\![j_0, \kappa_1]\!]$ in the first sum in (2.17), we obtain

$$\begin{aligned}
\sum_{j=j_0}^{\kappa_1} 2^{j(r/2-1)} (t'_{j,n,\alpha})^{r-\rho} \sum_k |\beta_{jk}|^\rho &\le j_1^{(\nu+1/2)(r-p)} n^{-(r-p)/2} \sum_{j=j_0}^{\kappa_1} 2^{j(r/2-sp-p/2)} \\
&\lesssim (\log n)^C n^{-(r-p)/2} \sum_{j=j_0}^{\kappa_1} 2^{j(r/2-1)(1-p/q_1)} \\
&\lesssim (\log n)^C n^{-(r-p)/2} 2^{\kappa_1(r/2-1)(1-p/q_1)} \\
&= (\log n)^C n^{\frac{q_1-r}{2}} \\
&= (\log n)^C n^{-\frac{rs'}{2(s-1/p)+1}}.
\end{aligned}$$

For the sum over indices $j \in [\![\kappa_1+1, j_1]\!]$, we choose $\rho > q_1 > p$, and obtain by monotony

of ℓ^ω-norms in ω and putting $s'' = s + 1/2 - 1/p$ that

$$\begin{aligned}
\sum_{j=\kappa_1+1}^{j_1} 2^{j(r/2-1)}(t'_{j,n,\alpha})^{r-\rho}\sum_k|\beta_{jk}|^\rho &\lesssim j_1^{(\nu+1/2)(r-\rho)}n^{-\frac{r-\rho}{2}}\sum_{j=\kappa_1+1}^{j_1}2^{j(r/2-1-\rho s'')}\\
&\lesssim (\log n)^C n^{-\frac{r-\rho}{2}}\sum_{j=\kappa_1+1}^{j_1}2^{j(r/2-1-\rho s'')}\\
&= (\log n)^C n^{-\frac{r-\rho}{2}}\sum_{j=\kappa_1+1}^{j_1}2^{j(r/2-1)(1-\rho/q_1)}\\
&\lesssim (\log n)^C n^{-\frac{r-\rho}{2}}2^{\kappa_1(r/2-1)(1-\rho/q_1)}\\
&\asymp (\log n)^C n^{\frac{q_1-r}{2}}\\
&= (\log n)^C n^{-\frac{rs'}{2(s-1/p)+1}}.
\end{aligned}$$

- Bound for S_2: S_2 can be dealt with exactly as in the second case.

2.9.2.4 Bound for e_{ss}

For any $0 \le \rho \le r$

$$\begin{aligned}
\mathbb{E}\|e_{ss}\|_r^r &\lesssim \sum_{j=j_0}^{j_1}2^{j(\frac{r}{2}-1)}\sum_k|\beta_{jk}|^r\mathbb{E}[\mathbb{1}_{\widehat{S}_j\cap S'_j}(k)]\\
&\lesssim \sum_{j=j_0}^{j_1}2^{j(\frac{r}{2}-1)}((t'_{j,n,\alpha})^{r-\rho}\vee(t''_{j,n,\alpha})^{r-\rho})\sum_k|\beta_{jk}|^\rho.
\end{aligned}$$

This term can be bounded from above by the right-hand side of (2.17), and we conclude in the same way as for the term e_{bb}.

2.9.3 A concentration inequality for the $\widehat{\beta}_{jk}$

For our proof, we need concentration inequalities for the events

$$A_{jk} := \left\{|\widehat{\beta}_{jk}-\beta_{jk}| \ge (K/2)\frac{j^{\nu+1/2}}{\sqrt{n}}\left(1\vee\frac{2^{j/2}}{\alpha}\right)\right\}$$

for $K > 0$, where $j \in [\![j_0, j_1]\!]$ and $k \in \mathcal{N}_j$. Let recall the two-sided Bernstein's inequality (cf. [11] Theorem 2.10).

Theorem 2.9.1. *Let $Y_1, \dots, Y_n$ be independent real valued random variables. Assume that there exist some positive numbers v and c such that*

$$\sum_{i=1}^{n} \mathbb{E}[Y_i^2] \leqslant v, \tag{2.18}$$

and for all integers $m \geqslant 3$

$$\sum_{i=1}^{n} \mathbb{E}[|Y_i|^m] \leqslant \frac{m!}{2} v c^{m-2}. \tag{2.19}$$

Let $S = \sum_{i=1}^{n}(Y_i - \mathbb{E}[Y_i])$, then for every positive x

$$\mathbb{P}\left[|S| \geqslant \sqrt{2vx} + cx\right] \leqslant 2\exp(-x). \tag{2.20}$$

Using this inequality, we can prove the following result.

Proposition 2.9.2. *For all $j \in [\![j_0, j_1]\!]$ satisfying $j \leq n$, for all $k \in \mathcal{N}_j$, and for all $\gamma \geqslant 1$ we have*

$$\mathbb{P}\left(|\widehat{\beta}_{jk} - \beta_{jk}| \geq 4(\bar{c} + \sigma)\gamma \frac{j^{\nu+1/2}}{\sqrt{n}} \left(1 \vee \frac{2^{j/2}}{\alpha}\right)\right) \leqslant 2^{-\gamma j}, \tag{2.21}$$

where $\bar{c}$ is an upper bound for $\sup_{f \in \mathcal{D}^s_{pq}(L,T)} \|f\|_\infty$ and $\sigma = 4c_A\|\psi\|_\infty(2\nu - 1)/(\nu - 1)$ appears in the privacy mechanism (2.8).

Remark 2.9.3. By Equation (15) in [24], the choice $\bar{c} = L$ is admissible for $f \in \mathcal{D}^s_{pq}(L, T)$.

Proof. We will apply Bernstein's inequality to the random variables $\{Z_{ijk}\}_{i=1,\dots,n}$. Using that $\psi_{jk}(X_i)$ and W_{ijk} are independent and that $\mathbb{E}[W_{ijk}] = 0$, we get for all $i \in [\![1, n]\!]$

$$\begin{aligned}
\mathbb{E}[Z_{ijk}^2] &= \mathbb{E}[\psi_{jk}(X_i)^2] + \sigma_j^2\mathbb{E}[W_{ijk}^2] + 2\sigma_j\mathbb{E}[\psi_{jk}(X_i)W_{ijk}] \\
&= \mathbb{E}[\psi_{jk}(X_i)^2] + \sigma_j^2\mathbb{E}[W_{ijk}^2] + 2\sigma_j\mathbb{E}[\psi_{jk}(X_i)]\mathbb{E}[W_{ijk}] \\
&= \mathbb{E}[\psi_{jk}(X_i)^2] + \sigma_j^2\mathbb{E}[W_{ijk}^2] \\
&\leqslant \bar{c} + 2\sigma_j^2 \\
&\leqslant 2(\bar{c} + \sigma_j)^2,
\end{aligned}$$

where $\bar{c} > 0$ depends on L is such that $\|f\|_\infty \leq \bar{c}$ for all f in $\mathcal{B}^s_{pq}(L)$ with $s > \frac{1}{p}$. Let $m \geqslant 3$ be an integer. Using again that $\psi_{jk}(X_i)$ and W_{ijk} are independent we get for all

$i \in [\![1, n]\!]$

$$\begin{aligned}
\mathbb{E}[|Z_{ijk}|^m] &\leqslant \mathbb{E}[(|\psi_{jk}(X_i)| + \sigma_j |W_{ijk}|)^m] \\
&= \mathbb{E}\left[\sum_{l=0}^{m} \binom{m}{l} \sigma_j^l |W_{ijk}|^l |\psi_{jk}(X_i)|^{m-l}\right] \\
&= \sum_{l=0}^{m} \binom{m}{l} \sigma_j^l \mathbb{E}\left[|W_{ijk}|^l\right] \mathbb{E}\left[|\psi_{jk}(X_i)|^{m-l}\right] \\
&= \sum_{l=0}^{m} \binom{m}{l} \sigma_j^l \mathbb{E}\left[|\psi_{jk}(X_i)|^{m-l}\right] l! \\
&\leqslant m! \sum_{l=0}^{m} \binom{m}{l} \sigma_j^l (\bar{c})^{m-l} \\
&= m! (\bar{c} + \sigma_j)^m.
\end{aligned}$$

Conditions (2.18) and (2.19) are thus satisfied with $v = 2n(\bar{c} + \sigma_j)^2$ and $c = \bar{c} + \sigma_j$, and according to Bernstein's inequality (2.20) we have for all $x > 0$

$$\mathbb{P}\left(|\widehat{\beta}_{jk} - \beta_{jk}| \geqslant (\bar{c} + \sigma_j)\left(2\sqrt{\frac{x}{n}} + \frac{x}{n}\right)\right) \leqslant 2\exp(-x).$$

Note that we have for all $j \in [\![j_0, j_1]\!]$,

$$\bar{c} + \sigma_j = \bar{c} + \sigma j^\nu \frac{2^{j/2}}{\alpha} \leqslant (\bar{c} + \sigma) j^\nu \left(1 \vee \frac{2^{j/2}}{\alpha}\right),$$

where $\sigma = 4c_A \|\psi\|_\infty (2\nu - 1)/(\nu - 1)$ appears in the definition of σ_j in (2.8). Take $x = Cj$, $C > 0$ and note that $2\sqrt{Cj/n} + Cj/n \leqslant (2\sqrt{C} + C)\sqrt{j/n}$ if $j \leqslant n$. Consequently, we get for all $C > 0$, for all $j \in [\![j_0, j_1]\!]$ satisfying $j \leqslant n$ and for all $k \in \mathcal{N}_j$,

$$\mathbb{P}\left(|\widehat{\beta}_{jk} - \beta_{jk}| \geqslant (\bar{c} + \sigma)(C + 2\sqrt{C})\frac{j^{\nu+1/2}}{\sqrt{n}}\left(1 \vee \frac{2^{j/2}}{\alpha}\right)\right) \leqslant 2\exp(-Cj).$$

Then, it suffices to take $C = 2\ln(2)\gamma$ to obtain (2.21). □

2.9.4 Moment bounds and norm inequalities

Consider an arbitrary random function

$$\widehat{g} = \sum_{j=j_0}^{j_1} \sum_k \widehat{g}_{jk} \psi_{jk}.$$

Putting

$$S(\iota) = \sum_{j=j_0}^{j_1} 2^{j\iota} \leq \begin{cases} c_\gamma 2^{\max(j_1\iota, j_0\iota)} & \text{if } \iota \neq 0, \\ j_1 - j_0, & \text{if } \iota = 0, \end{cases}$$

it has been shown in [24] that for arbitrary $v \in \mathbb{R}$ and $u = r/(r-2)$ it holds

$$\mathbb{E}\|\widehat{g}\|_r^r \leq \begin{cases} C^r \sum_{j=j_0}^{j_1} 2^{j(r/2-1)} \sum_k \mathbb{E}|\widehat{g}_{jk}|^r, & \text{if } 1 \leq r \leq 2, \\ C^r S(uv)^{(r/2-1)_+} \sum_{j=j_0}^{j_1} 2^{j(r/2-1-vr/2)} \sum_{k\in\mathbb{Z}} \mathbb{E}|\widehat{g}_{jk}|^r, & \text{if } r > 2. \end{cases}$$

As in [24], adopting the formal convention $S^0 = 1$, it suffices to consider the second inequality for all $r \geq 1$ (setting $v = 0$ for the case $r \leq 2$). Thus, for any $r \geq 1$,

$$\mathbb{E}\|\widehat{g}\|_r^r \lesssim \sum_{j=j_0}^{j_1} 2^{j(r/2-1)} \sum_k \mathbb{E}|\widehat{g}_{jk}|^r. \tag{2.22}$$

Consider again the decomposition $\widehat{\beta}_{jk} = \beta'_{jk} + \frac{\sigma_j}{n} \sum_{i=1}^n W_{ijk}$. We have, for any $m \geq 1$,

$$\mathbb{E}|\widehat{\beta}_{jk} - \beta_{jk}|^m \leq 2^{m-1}\mathbb{E}|\beta'_{jk} - \beta_{jk}|^m + 2^{m-1}\mathbb{E}\left|\frac{\sigma_j}{n}\sum_{i=1}^n W_{ijk}\right|^m.$$

In [24], p. 520, Equation (16) it is shown that

$$\mathbb{E}|\beta'_{jk} - \beta_{jk}|^m \leq cn^{-m/2} \tag{2.23}$$

provided that $2^j \leq n$ with a constant c depending only on s, p, q, L, $\|\psi\|_m$ and m. In addition, by Rosenthal's inequality, it can be shown for any $m \geq 1$ that

$$\mathbb{E}\left|\frac{\sigma_j}{n}\sum_{i=1}^n W_{ijk}\right|^m \lesssim j^{\nu m/2} 2^{jm/2} (n\alpha^2)^{-m/2}. \tag{2.24}$$

Combining (2.23) and (2.24) yields

$$\mathbb{E}|\widehat{\beta}_{jk} - \beta_{jk}|^m \lesssim n^{-m/2} \vee j^{\nu m/2} 2^{jm/2} (n\alpha^2)^{-m/2}. \tag{2.25}$$

Chapter 3

Sharp phase transitions for exact support recovery under local differential privacy

Abstract: *We address the problem of variable selection in the Gaussian mean model in $\mathbb{R}^d$ under the additional constraint that only privatised data are available for inference. For this purpose, we adopt a recent generalisation of classical minimax theory to the framework of local $\alpha-$differential privacy. We provide lower and upper bounds on the rate of convergence for the expected Hamming loss over classes of at most s-sparse vectors whose non-zero coordinates are separated from 0 by a constant $a > 0$. As corollaries, we derive necessary and sufficient conditions (up to log factors) for exact recovery and for almost full recovery. When we restrict our attention to non-interactive mechanisms that act independently on each coordinate our lower bound shows that, contrary to the non-private setting, both exact and almost full recovery are impossible whatever the value of a in the high-dimensional regime such that $n\alpha^2/d^2 \lesssim 1$. However, in the regime $n\alpha^2/d^2 \gg \log(n\alpha^2/d^2)\log(d)$ we can exhibit a sharp critical value a^* (up to a logarithmic factor) such that exact and almost full recovery are possible for all $a \gg a^*$ and impossible for $a \leq a^*$. We show that these results can be improved when allowing for all non-interactive (that act globally on all coordinates) locally $\alpha-$differentially private mechanisms in the sense that phase transitions occur at lower levels.*

Based on [14].

3.1 Introduction

Problem statement

Nowadays, a large amount of data, such as internet browsing history, social media activity, location information from smartphones, or medical records, are collected and stored. On the one hand, the analysis of these data can benefit to individuals, companies, or communities such as the scientific one. For instance, companies can use data to improve their products and services, or health data can be used for medical research. On the other hand, people are more and more concerned with the protection of their privacy and may be reluctant to share their sensitive data. In this context, it seems essential to be able to understand the tradeoffs between the statistical utility of the collected data and the privacy of individuals from whom these data are obtained. This requires a formal definition of privacy and differential privacy has been adopted by researchers in the computer science, machine learning, and statistics communities as a natural one.

Two kinds of differential privacy are discussed in the literature: central differential privacy which has been introduced by Dwork et al. in [33], and local differential privacy. We will focus in this paper on the second setting but we briefly discuss the difference between central and local privacy. In both settings, n individuals want their privacy to be preserved while their data, which will be denoted $X_1, \dots, X_n$, are used for statistical analyses. In the central setting, the n data-holders share confidence in a common curator who has access to the original data $X_1, \dots, X_n$ and use them to generate a private release Z. In a nutshell, central differential privacy ensures that the probability of observing an output does not change much when a single data point of the original database is modified. We refer to [80] for the formal definition of differential privacy in the central setting. In the local setting, data is privatized before it is shared with a data collector : for all $i \in [\![1, n]\!]$, X_i is transformed into a private data Z_i directly on the ith individual's machine and the data collector or the statistician only have access to the private sample $Z_1, \dots, Z_n$. However, some interaction between the different data-holders is allowed. Formally, the privatized data $Z_1, \dots, Z_n$ are obtained by successively applying suitable Markov kernels : given $X_i = x_i$ and $Z_1 = z_1, \dots, Z_{i-1} = z_{i-1}$, the i-th dataholder draws

$$Z_i \sim Q_i(\cdot \mid X_i = x_i, Z_1 = z_1, \dots, Z_{i-1} = z_{i-1})$$

for some Markov kernel $Q_i : \mathscr{Z} \times \mathcal{X} \times \mathcal{Z}^{i-1} \to [0, 1]$ where the measure spaces of the non-

private and private data are denoted with $(\mathcal{X}, \mathscr{X})$ and $(\mathcal{Z}, \mathscr{Z})$, respectively. Such randomizations are known as sequentially interactive. We say that the sequence of Markov kernels $(Q_i)_{i=1,\dots,n}$ provides α-local differential privacy or that $Z_1, \dots, Z_n$ are α-local differentially private views of $X_1, \dots, X_n$ if

$$\sup_{A \in \mathscr{Z}} \frac{Q_i(A \mid X_i = x, Z_1 = z_1, \dots, Z_{i-1} = z_{i-1})}{Q_i(A \mid X_i = x', Z_1 = z_1, \dots, Z_{i-1} = z_{i-1})} \leq \exp(\alpha) \quad \forall i \in [\![1, n]\!], \forall x, x' \in \mathcal{X}. \quad (3.1)$$

In this paper, we will focus on the special case of non-interactive local differential privacy where Z_i depends only on X_i but not on Z_k for $k < i$. In this scenario, we have

$$Z_i \sim Q_i(\cdot \mid X_i = x_i),$$

and condition (3.1) becomes

$$\sup_{A \in \mathscr{Z}} \frac{Q_i(A \mid X_i = x)}{Q_i(A \mid X_i = x')} \leq \exp(\alpha) \quad \forall i \in [\![1, n]\!], \forall x, x' \in \mathcal{X}.$$

We consider the problem of support recovery with separation assumptions under local differential privacy as a special instance of the general problem described above. Precisely, for $i = 1, \dots, n$, the ith data holder observes a random vector $X^i = (X^i_j)_{j=1,\dots,d} \in \mathbb{R}^d$ distributed according to the normal distribution $\mathcal{N}(\theta, \sigma^2 I_d)$, where the mean vector θ is assumed to be (s, a)-sparse in the sense that θ belongs to one of the following sets:

$$\Theta^+_d(s, a) = \{\theta \in \mathbb{R}^d : \text{there exists a set } S \subseteq \{1, \dots, d\} \text{ with at most } s \text{ elements such that } \theta_j \geq a \text{ for all } j \in S, \text{ and } \theta_j = 0 \text{ for all } j \notin S\},$$

or

$$\Theta_d(s, a) = \{\theta \in \mathbb{R}^d : \text{there exists a set } S \subseteq \{1, \dots, d\} \text{ with at most } s \text{ elements such that } |\theta_j| \geq a \text{ for all } j \in S, \text{ and } \theta_j = 0 \text{ for all } j \notin S\}.$$

The aim is that every data holder releases a private view Z^i of X^i such that the notion of local differential privacy is satisfied and that the support of θ can be estimated from the data $Z^1, \dots, Z^n$ in an optimal way.

Notation. For two sequences $\{a_d\}_d$ and $\{b_d\}_d$ of non-negative real numbers, we write $a_d \lesssim b_d$ if there exists some constant $C > 0$ such that $a_d \leq C b_d$. If $b_d > 0$ we write $a_d \sim b_d$

if $a_d/b_d \to 1$ as $d \to \infty$ and we write $a_d \gg b_d$ if $a_d/b_d \to \infty$ as $d \to \infty$. We recall that a centred Laplace distribution with parameter $\lambda > 0$ has the probability density function defined by $f_\lambda(x) = \frac{1}{2\lambda} \exp\left(-\frac{|x|}{\lambda}\right)$ on $\mathbb{R}$.

Motivation

The problem of high-dimensional sparse vectors estimation has recently been studied in the framework of local differential privacy in [30]. For the 1-sparse means problem, the authors proved that the private minimax risk for non-interactive α-locally differentially private mechanisms over the set of distributions P supported on $\mathbb{B}_\infty(r) \subset \mathbb{R}^d$ with $\|\mathbb{E}_P[X]\|_0 \leq 1$ is bounded from below by

$$\min\left\{r^2, \frac{r^2 d \log(2d)}{n(e^\alpha - 1)^2}\right\},$$

proving that high-dimensional 1-sparse mean estimation is impossible in this setting when both $r^2 \gtrsim 1$ and $r^2 d \log(2d) \gtrsim n(e^\alpha - 1)^2$.

Obvious applications of variable selection are the estimation of the set that supports the non-null coefficients in the mean vector, or the estimation of its size. We may use our procedure to build a private mean estimator of $s-$sparse vectors in two steps: use one part of the sample to recover the support and the other part to estimate the mean values of the selected variables, that is a vector of reduced size. Moreover these results are a benchmark for working on more realistic models such as high-dimensional linear regression and clustering of high-dimensional vectors, see [58] and [57].

Minimax framework

Let X^i, $i = 1, \ldots, n$ be i.i.d $\mathcal{N}(\theta, \sigma^2 I_d)$ random vectors of $\mathbb{R}^d$. We assume that the vectors $X^i = (X^i_j)_{j=1,\ldots,d}$ for $i = 1, \ldots, n$ are observed by n distinct data holders who refuse to share their respective observations. The statistician does not have access to these data but only to α-locally differentially private views $Z^1, \ldots Z^n$. We assume that θ belongs to one of the sets $\Theta_d^+(s, a)$ or $\Theta_d(s, a)$ introduced in Section 3.1 and we study the problem of selecting the relevant components of θ, that is, of estimating the vector

$$\eta = \eta(P_\theta) = (I(\theta_j \neq 0))_{j=1,\ldots,d},$$

where $I(\cdot)$ is the indicator function. Our goal is to estimate the vector η by a *selector* $\hat{\eta}$, that is a measurable function $\hat{\eta} = \hat{\eta}(Z^1, \dots, Z^n)$ taking values in $\{0,1\}^d$, where $Z^1, \dots, Z^n$ are α-locally differentially private views of $X^1, \dots, X^n$. We judge the quality of a selector $\hat{\eta}$ as an estimator of η by the Hamming loss between $\hat{\eta}$ and η which counts the number of positions at which $\hat{\eta}$ and η differ :

$$|\hat{\eta} - \eta| := \sum_{j=1}^{d} |\hat{\eta}_j - \eta_j| = \sum_{j=1}^{d} I(\hat{\eta}_j \neq \eta_j).$$

For the support recovery problem, we consider only α-locally differentially private mechanisms which transform each $X^i \in \mathbb{R}^d$ into a private release Z^i taking also values in $\mathbb{R}^d$, that are known as non-interactive privacy mechanisms. However, we distinguish between privacy mechanisms that act on each coordinate of X^i either separately, locally or globally. More specifically, we will consider the two following scenarios:

- **Coordinate Local (CL) Privacy Mechanisms** : there is a sequence $Q = (Q^i)_{i=1,\dots,n}$ of Markov kernels providing α-local differential privacy such that $Z^i \sim Q^i(\cdot \mid X^i = x^i)$ for all $i \in [\![1, n]\!]$, and Q^i is obtained as product of coordinate-wise kernels as follows:

  $$\text{for all } i \in [\![1, n]\!] \text{ and all } j \in [\![1, d]\!], Z^i_j \sim Q^i_j(\cdot \mid X^i_j = x)$$

  for some (α/d)-differentially private mechanism Q^i_j. We denote by $\mathcal{Q}^{CL}_\alpha$ the set of all privacy mechanisms $Q = (Q^1, \dots, Q^n)$ satisfying these assumptions.

- **Coordinate Global (CG) Privacy Mechanisms** : there is a sequence $Q = (Q^i)_{i=1,\dots,n}$ of Markov kernels providing α-local differential privacy such that $Z^i \sim Q^i(\cdot \mid X^i = x^i)$ for all $i \in [\![1, n]\!]$. We denote by $\mathcal{Q}_\alpha$ the set of all privacy mechanisms $Q = (Q^1, \dots, Q^n)$ satisfying this assumption.

In other words, in the Coordinate Local case, we consider only non-interactive α-locally differentially private mechanisms that act coordinates by coordinates. This scenario is easier to study than the second one for which any non-interactive α-locally differentially private mechanism is allowed to be used.

For both scenarios, if P_θ denotes the distribution of X^i then we denote by $Q^i P_\theta$ the distribution of Z^i. Since the distribution of $(X^1, \dots, X^n)$ is $P_\theta^{\otimes n}$, the distribution of $(Z^1, \dots, Z^n)$ will be denoted by $Q(P_\theta^{\otimes n})$. In the Coordinate Local case, we denote by P_{θ_j} the distribution of X^i_j and by $Q^i_j P_{\theta_j}$ the distribution of Z^i_j.

We say that a selector $\hat{\eta} = (\hat{\eta}_1, \dots, \hat{\eta}_d)$ is *separable* if for all $j = 1, \dots, d$ its jth component $\hat{\eta}_j$ depends only on $(Z_j^i)_{i=1,\dots,n}$. We denote by $\mathcal{T}$ the set of all separable selectors. We are interested in the study of the following private minimax risks

$$\mathcal{R}_n^{CL}(\alpha, \Theta) = \inf_{Q \in \mathcal{Q}_\alpha^{CL}} \inf_{\hat{\eta} = \hat{\eta}(Z^1, \dots, Z^n) \in \mathcal{T}} \sup_{\theta \in \Theta} \frac{1}{s} \mathbb{E}_{Q(P_\theta^{\otimes n})} |\hat{\eta}(Z^1, \dots, Z^n) - \eta|, \tag{3.2}$$

in the coordinate local case, and

$$\mathcal{R}_n(\alpha, \Theta) = \inf_{Q \in \mathcal{Q}_\alpha} \inf_{\hat{\eta} = \hat{\eta}(Z^1, \dots, Z^n) \in \mathcal{T}} \sup_{\theta \in \Theta} \frac{1}{s} \mathbb{E}_{Q(P_\theta^{\otimes n})} |\hat{\eta}(Z^1, \dots, Z^n) - \eta|, \tag{3.3}$$

in the coordinate global case, for $\Theta = \Theta_d^+(s, a)$ and $\Theta = \Theta_d(s, a)$.

We are interested in the study of two asymptotic properties : *almost full recovery* and *exact recovery*, that we define here. Let $(\Theta_d^+(s_d, a_d))_{d \geq 1}$ be a sequence of classes of sparse vectors. We will say that *almost full recovery is possible* for $(\Theta_d^+(s_d, a_d))_{d \geq 1}$ in the Coordinate Local case if there exists $Q \in \mathcal{Q}_\alpha^{CL}$ and a selector $\hat{\eta}$ such that

$$\lim_{d \to \infty} \sup_{\theta \in \Theta_d^+(s_d, a_d)} \frac{1}{s_d} \mathbb{E}_{Q(P_\theta^{\otimes n})} |\hat{\eta} - \eta| = 0.$$

We will say that *almost full recovery is impossible* for $(\Theta_d^+(s_d, a_d))_{d \geq 1}$ in the Coordinate Local case if

$$\liminf_{d \to +\infty} \inf_{Q \in \mathcal{Q}_\alpha^{CL}} \inf_{\hat{\eta} = \hat{\eta}(Z^1, \dots, Z^n) \in \mathcal{T}} \sup_{\theta \in \Theta_d^+(s,a)} \frac{1}{s_d} \mathbb{E}_{Q(P_\theta^{\otimes n})} |\hat{\eta} - \eta| > 0.$$

We will say that *exact recovery is possible* for $(\Theta_d^+(s_d, a_d))_{d \geq 1}$ in the Coordinate Local case if there exists $Q \in \mathcal{Q}_\alpha^{CL}$ and a selector $\hat{\eta}$ such that

$$\lim_{d \to \infty} \sup_{\theta \in \Theta_d^+(s_d, a_d)} \mathbb{E}_{Q(P_\theta^{\otimes n})} |\hat{\eta} - \eta| = 0.$$

We will say that *exact recovery is impossible* for $(\Theta_d^+(s_d, a_d))_{d \geq 1}$ in the Coordinate Local case if

$$\liminf_{d \to +\infty} \inf_{Q \in \mathcal{Q}_\alpha^{CL}} \inf_{\hat{\eta} = \hat{\eta}(Z^1, \dots, Z^n) \in \mathcal{T}} \sup_{\theta \in \Theta_d^+(s,a)} \mathbb{E}_{Q(P_\theta^{\otimes n})} |\hat{\eta} - \eta| > 0.$$

We use similar definitions in the Coordinate Global case with $\mathcal{Q}_\alpha^{CL}$ replaced by $\mathcal{Q}_\alpha$.

3.1.1 Related work

Variable selection with Hamming loss in the Gaussian mean model in $\mathbb{R}^d$ has been studied in the non-private setting in [12]. The authors provide non-asymptotic lower and upper bounds on the non-private version of minimax risk (3.2). As corollaries, they derive necessary and sufficient conditions for almost full recovery and exact recovery to be possible. They highlight a critical value $a^* = (\sigma/\sqrt{n})\sqrt{2\log(d/s-1)}(1+o(1))$ such that almost full recovery is possible for $a \geq a^*$ and impossible for $a < a^*$. Similar results have been obtained for exact recovery with the greater critical value $a^* = (\sigma/\sqrt{n})(\sqrt{2\log(d-s)}+\sqrt{2\log s})$. In the present paper, we will see how these results are affected by the privacy constraints.

A few papers tackle selection problems under privacy constraints. In [70], the authors study top-k selection under a relaxation of central differential privacy called (ε,δ)-approximate differential privacy (see for instance [32]). However, they use a weighted Hamming loss as described below. Precisely, if $X_1,\dots,X_n$ are drawn i.i.d. from some distribution P on $\{0,1\}^d$, they want to find the k greatest coordinates of the mean vector $\theta = \mathbb{E}_P[X_1]$ while respecting (ε,δ)-differential privacy constraints. They prove that the existence of a $(1,1/(nd))$-differentially private mechanism that outputs $Z \in \{0,1\}^d$ with k non zero coordinates such that

$$\mathbb{E}\left[\sum_{j=1}^{d}\theta_j \mathbb{1}(Z_j=1)\right] \geq \max_{\eta\in\{0,1\}^d:\|\eta\|_1=k}\sum_{j=1}^{d}\theta_j\mathbb{1}(\eta_j=1)-\beta$$

requires $n \gtrsim \sqrt{k}\log d$ samples in the low accuracy regime where $\beta = k/10$. Moreover, repeated use of the classical exponential mechanism solves this problem with $n = O(\sqrt{k}\log d)$ samples. In [6], the authors study an empirical version of the problem studied in [70] : they want to find the top-k coordinates of the vector $q \in \mathbb{R}^d$ defined by $q_j = (1/n)\sum_{i=1}^n X_{i,j}$, $j=1,\dots,d$ while respecting (ε,δ)-differential privacy constraints. Let τ be the k-th largest value among the coordinates $\{q_1,\dots,q_k\}$. They prove that the existence of a (ε,δ)-differentially private mechanism that outputs a set $S \subset [\![1,d]\!]$ of k elements such that $q_j \geq \tau-\beta$ for all $j \in S$ requires $n \gtrsim k\log(d)$ samples in the high-accuracy regime where $\beta \asymp \sqrt{\log d/n}$. In [74], Ullman studies the same problem as [70] for $k=1$ under non-interactive α-local differential privacy constraints. If we consider the low-accuracy regime considered by [70], the result by Ullman shows that solving the problem under non-interactive α-local differential privacy requires $n \gtrsim d\log d/\alpha^2$ samples,

	$a \lesssim \frac{\sigma}{\sqrt{N}}$	$\frac{\sigma}{\sqrt{N}} \ll a \leq 2\sigma$	$a \geq 2\sigma$
$N := \frac{n\alpha^2}{d^2} \lesssim 1$	impossible	impossible	impossible
$N := \frac{n\alpha^2}{d^2} \gg 1$	impossible	possible, as soon as $a \gg \frac{\sigma}{\sqrt{N}}\sqrt{\log(N)\log(d)}$, possible, if $N \gg \log(d)$ if moreover $N \gg \log(N)\log(d)$	

Table 3.1: Exact recovery in the Coordinate Local case. Similar results hold for almost full recovery with $\log(d)$ replaced by $\log(d/s)$.

highlighting an exponentially worse dependence on the dimension compared to the result obtained in the central model of (ε, δ)-approximate differential privacy.

Organisation of the paper

In Section 3.2, we study the minimax risk (3.2). We first provide a lower bound which enables us to obtain necessary conditions for almost full recovery and exact recovery to be possible in the case where only coordinate local privacy mechanisms are used. In particular, we prove that almost full recovery is impossible in this case as soon as the quantity $n\alpha^2/d^2$ is bounded from above. We then provide non-asymptotic upper bounds on the minimax risks in propositions and state more explicit asymptotic sufficient conditions for almost full recovery and exact recovery to be possible in our corollaries. These conditions and associated results are summarised in Table 3.1. In Section 3.3, we study the minimax risk (3.3) and prove that the results of Section 3.2 can be improved when any non-interactive (coordinate global) α-locally differentially private mechanism is allowed. See Table 3.2 for a summary of these results. Detailed proofs can be found in the Appendix.

3.2 Minimax risk using coordinate local non-interactive privacy mechanisms

In this section, we provide a lower bound on the private minimax risk (3.2). This enables us to obtain necessary conditions for almost full recovery and exact recovery to be possible

	$a \lesssim \sigma\sqrt{\frac{\log d}{Nd}}$	$\sigma\sqrt{\frac{\log d}{Nd}} \ll a \leq 2\sigma$	$a \geq 2\sigma$
$\frac{Nd}{\log d} \lesssim 1$	impossible	impossible	impossible if $a \leq \sigma\sqrt{\log\left(1+\frac{\log d}{16Nd}\right)}$
$\frac{Nd}{\log d} \gg 1$	impossible	possible, as soon as $a \gg \sigma\sqrt{\frac{\log d}{Nd}}\sqrt{\log(Nd)}$, if moreover $Nd \gg \log(Nd)\log(d)$	possible

Table 3.2: Exact recovery in the Coordinate Global case. We have set $N = n\alpha^2/d^2$ for a better comparison with the Coordinate Local case.

in the Coordinate Local scenario. In particular, we prove that almost full recovery is impossible in the private setting of the Coordinate Local case if the quantity $N := n\alpha^2/d^2$ is bounded from above. We then provide upper bounds on the minimax risk that entail sufficient conditions for almost full recovery and exact recovery to be possible.

3.2.1 Lower bound

We first state our lower bound.

Theorem 3.2.1. *For any $a > 0$, $\alpha > 0$, $1 \leq s \leq d$, $n \geq 1$, we have*

$$\mathcal{R}_n^{CL}(\alpha, \Theta_d^+(s,a)) \geq \left(1 - \frac{s}{d}\right) \exp\left(-4n(e^{\alpha/d}-1)^2 \min\left\{\frac{a^2}{4\sigma^2}, 1\right\}\right). \tag{3.4}$$

The proof of Theorem 3.2.1 can be found in Appendix 3.5.2. Some auxiliary results used for the proof of Theorem 3.2.1 can be found in Appendix 3.5.1. Note that since $\Theta_d^+(s,a) \subset \Theta_d(s,a)$ we have $\mathcal{R}_n^{CL}(\alpha, \Theta_d^+(s,a)) \leq \mathcal{R}_n^{CL}(\alpha, \Theta_d(s,a))$, thus the right hand side of (3.4) is also a lower bound for $\mathcal{R}_n^{CL}(\alpha, \Theta_d(s,a))$.

For better confidentiality in practice, the parameter α must not be too large. In particular, we assume that $\alpha/d \to 0$ when $d \to +\infty$. We thus have $n(e^{\alpha/d}-1)^2 \sim n\alpha^2/d^2$ and Theorem 3.2.1 immediately shows the following.

Corollary 3.2.2. *Let $\alpha > 0$, $1 \leq s \leq d$, $n \geq 1$ be such that $s/d \leq C_0$ for some constant $C_0 \in (0,1)$, and $\alpha/d \to 0$ when $d \to \infty$. Then, if $n\alpha^2/d^2 \leq C_1$ for some constant $C_1 > 0$*

or if $n\alpha^2/d^2 \to \infty$ *as* $d \to \infty$ *and* $a^2 \leq C_2\sigma^2 d^2/(n\alpha^2)$*, it holds*

$$\mathcal{R}_n^{CL}(\alpha, \Theta) \geq C$$

for some constant $C > 0$*, where* $\Theta = \Theta_d^+(s, a)$ *or* $\Theta = \Theta_d(s, a)$*.*

Corollary 3.2.2 shows that almost full recovery is impossible under local differential privacy constraints if the quantity $n\alpha^2/d^2$ is bounded from above. In particular, almost full recovery is impossible under local differential privacy constraints in the high-dimensional setting, that is when $n \leq d$, whatever the value of a. Corollary 3.2.2 also proves that if $n\alpha^2/d^2 \to +\infty$ then almost full recovery is impossible if $a \lesssim (\sigma d)/(\sqrt{n}\alpha)$.

This underlines a strong difference between the private setting and the classical setting, since [12] proved that in the non-private setting almost full recovery is possible for a large enough even if $n = 1$. Transposed to this setting, variable selection is possible for $a \gg \sigma/\sqrt{n}$ and any $n \geq 1$ without privacy constraints, whereas it is impossible for any signal value a when the effective size $N = n\alpha^2/d^2 \lesssim 1$ under privacy constraints.

3.2.2 Privacy mechanism

In this section, we introduce a non-interactive privacy mechanism creating private views $Z^1, \ldots, Z^n$ of the original data $X^1, \ldots, X^n$ that satisfy the local differential privacy constraint of level α. These privatized data will then be used to define a private selector whose risk will be studied in Section 3.2.3.

To obtain the privatized data, we first censor the unbounded random variables X_j^i, for $i = 1, \ldots, n$, $j = 1, \ldots, d$, and then make use of an appropriately scaled version of the classical Laplace mechanism. For all $i \in [\![1, n]\!]$ and $j \in [\![1, d]\!]$ define

$$Z_j^i = [X_j^i]_T + \frac{2Td}{\alpha} W_j^i, \tag{3.5}$$

where $[\cdot]_T = \max\{-T, \min\{\cdot, T\}\}$ denotes the censoring operator at level T, the W_j^i's are i.i.d Laplace(1) random variables, and W_j^i is independent from X_j^i. The censoring level T needs to be properly chosen and will be specified later.

Note that the privacy mechanism defining $(Z^i)_{i=1,\ldots,n}$ is non-interactive since Z^i does only depend on X^i and not on Z^k for $k \neq i$. This is also a coordinate local mechanism since Z_j^i depends on X_j^i but not on the X_l^i for $l \neq j$. The following Proposition shows that it satisfies the condition of α-local differential privacy.

Proposition 3.2.3. *For all $i \in [\![1,n]\!]$ and $j \in [\![1,d]\!]$, Z_j^i is an α/d-differentially private view of X_j^i. Consequently, for all $i \in [\![1,n]\!]$ $Z^i = (Z_j^i)_{j=1,\dots,d}$ is an α-differentially private view of X^i.*

Proof. Set $r = 2Td/\alpha$. By definition of the privacy mechanism (3.5), the conditional density of Z_j^i given $X_j^i = x$ can be written as

$$q^{Z_j^i|X_j^i=x}(z) = \frac{1}{2r} \exp\left(-\frac{|z-[x]_T|}{r}\right).$$

Thus, by the reverse and the ordinary triangle inequality it holds for all $i \in [\![1,n]\!]$, $j \in [\![1,d]\!]$ and all $x, x', z \in \mathbb{R}$,

$$\begin{aligned}\frac{q^{Z_j^i|X_j^i=x}(z)}{q^{Z_j^i|X_j^i=x'}(z)} &= \exp\left(\frac{|z-[x']_T|}{r} - \frac{|z-[x]_T|}{r}\right)\\ &\le \exp\left(\frac{|[x']_T-[x]_T|}{r}\right)\\ &\le \exp\left(\frac{2T}{r}\right) \le \exp\left(\frac{\alpha}{d}\right).\end{aligned}$$

This proves that Z_j^i is an α/d-differentially private view of X_j^i. Let us check that Z^i is an α-differentially private view of X^i. Denote by $q^{Z^i|X^i=x}$ the conditional density of Z^i given $X^i = x$ and note that for all $x, x', z \in \mathbb{R}^d$ it holds

$$\frac{q^{Z^i|X^i=x}(z)}{q^{Z^i|X^i=x'}(z)} = \prod_{j=1}^{d} \frac{q^{Z_j^i|X_j^i=x_j}(z_j)}{q^{Z_j^i|X_j^i=x_j'}(z_j)} \le e^{\alpha},$$

using the independence of the coordinates $X_1^i, ..., X_d^i$ and the conditional independence of $Z_1^i, ..., Z_d^i$ given X^i. □

3.2.3 Upper bounds

Using these privatized data, we define two selectors that will provide upper bounds on the minimax risk (3.2). For the class $\Theta_d^+(s,a)$, we will use the selector $\hat{\eta}^+$ with the components

$$\hat{\eta}_j^+ = I\left(\frac{1}{n}\sum_{i=1}^{n} Z_j^i \ge \tau\right), \quad j = 1, \dots, d, \tag{3.6}$$

where the threshold τ has to be properly chosen, later on. For the class $\Theta_d(s,a)$, we will use the selector $\hat{\eta}$ with the components

$$\hat{\eta}_j = I\left(\left|\frac{1}{n}\sum_{i=1}^{n} Z_j^i\right| \geq \tau\right), \quad j = 1,\dots,d, \tag{3.7}$$

where τ to be defined later on. Note that $\hat{\eta}^+$ and $\hat{\eta}$ are separable selectors since $\hat{\eta}_j^+$ and $\hat{\eta}_j$ depend only on $(Z_j^i)_{i=1,\dots,n}$ and not on the Z_k^i for $k \neq j$. We now study the performances of these selectors. Recall that Φ denotes the standard Gaussian cumulative distribution function.

Proposition 3.2.4. *Assume that $a > b\sigma$ for some constant $b > 0$. Set $C_1 := 1 - 2\Phi(-b)$. If τ, T are chosen such that*

$$T \leq a - \sigma b,\ C_1 T - \tau \geq 0,\ \tau\alpha/(8Td) \leq 1 \text{ and } \alpha(C_1 T - \tau)/(8Td) \leq 1,$$

then it holds for all $\theta \in \Theta_d^+(s,a)$,

$$\begin{aligned}\mathbb{E}\left[\frac{1}{s}|\hat{\eta}^+ - \eta|\right] \leq \frac{d-|S|}{s}&\left[\exp\left(-\frac{n\tau^2}{2^3\min\{T^2,\sigma^2\}}\right) + \exp\left(-\frac{\tau^2 n\alpha^2}{2^7 T^2 d^2}\right)\right] \\ &+ \frac{|S|}{s}\left[\exp\left(-\frac{n(C_1T-\tau)^2}{2^3\min\{T^2,\sigma^2\}}\right) + \exp\left(-\frac{(C_1T-\tau)^2 n\alpha^2}{2^7 T^2 d^2}\right)\right],\end{aligned} \tag{3.8}$$

and for all $\theta \in \Theta_d(s,a)$ it holds

$$\begin{aligned}\mathbb{E}\left[\frac{1}{s}|\hat{\eta} - \eta|\right] \leq 2\Bigg\{\frac{d-|S|}{s}&\left[\exp\left(-\frac{n\tau^2}{2^3\min\{T^2,\sigma^2\}}\right) + \exp\left(-\frac{\tau^2 n\alpha^2}{2^7 T^2 d^2}\right)\right] \\ &+ \frac{|S|}{s}\left[\exp\left(-\frac{n(C_1T-\tau)^2}{2^3\min\{T^2,\sigma^2\}}\right) + \exp\left(-\frac{(C_1T-\tau)^2 n\alpha^2}{2^7 T^2 d^2}\right)\right]\Bigg\},\end{aligned} \tag{3.9}$$

where S denotes the support of θ.

The proof of Proposition 3.2.4 is given in section 3.5.4 in the Appendix. Some auxiliary results used in the proof of Proposition 3.2.4 can be found in Appendix 3.5.3. The following Corollary gives sufficient conditions so that almost full recovery and exact recovery are possible under local differential privacy in the Coordinate Local case when $a \geq 2\sigma$.

Corollary 3.2.5. *Set* $C_1 = 1 - 2\Phi(-1)$. *Assume that*

$$\alpha/d \to 0, n\alpha^2/d^2 \to +\infty \text{ and } \limsup \frac{\log(d/s)}{n\alpha^2/d^2} < \frac{C_1^2}{2^9}.$$

Then the selector $\hat{\eta}^+$ *defined by* (3.6) *with* $T = \sigma$ *and* $\tau = C_1 T/2$ *satisfies*

$$\sup_{\theta \in \Theta} \frac{1}{s} \mathbb{E}_{Q(P_\theta^{\otimes n})} |\hat{\eta}^+(Z^1, \ldots, Z^d) - \eta| \to 0, \tag{3.10}$$

for all $a \geq 2\sigma$, *where* $\Theta = \Theta_d^+(s,a)$ *or* $\Theta = \Theta_d(s,a)$. *If, in addition,* $\limsup \frac{\log(d)}{n\alpha^2/d^2} < \frac{C_1^2}{2^9}$, *then*

$$\sup_{\theta \in \Theta} \mathbb{E}_{Q(P_\theta^{\otimes n})} |\hat{\eta}^+(Z^1, \ldots, Z^d) - \eta| \to 0, \tag{3.11}$$

for all $a \geq 2\sigma$.

The proof of Corollary 3.2.5 is given in section 3.5.5 in the Appendix. Since we have seen that almost full recovery is impossible when $n\alpha^2/d^2$ is bounded from above or when $n\alpha^2/d^2 \to +\infty$ and $a \lesssim (\sigma d)/(\sqrt{n}\alpha)$, it remains to study the case where $n\alpha^2/d^2 \to +\infty$ and $\sigma d/(\sqrt{n}\alpha) \ll a \leq 2\sigma$. This is done below.

Proposition 3.2.6. *Let* $a > 0$. *If* T *and* τ *are chosen such that* $T \geq a + \sigma\sqrt{2\log\left(\max\left\{e, \frac{4\sigma}{a\sqrt{2\pi}}\right\}\right)}$, $\tau \leq a/2$, $\tau\alpha/(8Td) < 1$ *and* $\alpha(a/2-\tau)/(8Td) \leq 1$ *then it holds for all* $\theta \in \Theta_d^+(s,a)$,

$$\mathbb{E}\left[\frac{1}{s}|\hat{\eta}^+ - \eta|\right] \leq \frac{d-|S|}{s}\left[\exp\left(-\frac{n\tau^2}{2^3\min\{T^2,\sigma^2\}}\right) + \exp\left(-\frac{\tau^2 n\alpha^2}{2^7 T^2 d^2}\right)\right] + \frac{|S|}{s}\left[\exp\left(-\frac{n(a/2-\tau)^2}{2^3\min\{T^2,\sigma^2\}}\right) + \exp\left(-\frac{(a/2-\tau)^2 n\alpha^2}{2^7 T^2 d^2}\right)\right],$$

where S *denotes the support of* θ.

The proof of Proposition 3.2.6 can be found in section 3.5.6 in the Appendix. Note that as for the case $a \geq b\sigma$, if $\theta \in \Theta_d(s,a)$ we use $\hat{\eta}$ instead of $\hat{\eta}^+$ and we can prove the same result with an extra multiplicative factor 2. The next corollary gives new sufficient conditions so that almost full recovery and exact recovery are possible.

Corollary 3.2.7. *Assume that* $\alpha/d \to 0$, $n\alpha^2/d^2 \to +\infty$ *and* $\sigma d/(\sqrt{n}\alpha) \ll a \leq 2\sigma$. *The selector* $\hat{\eta}^+$ *defined by* (3.6) *with* $T = a + \sigma\sqrt{2\log\left(\frac{\sqrt{n}\alpha}{d}\right)}$ *and* $\tau = a/4$ *satisfies for* d *large*

enough

$$\sup_{\theta\in\Theta_d^+(s,a)} \frac{1}{s}\mathbb{E}_{Q(P_\theta^{\otimes n})}|\hat{\eta}^+(Z^1,\dots,Z^d)-\eta| \le 2\exp\left(\log\left(\frac{d}{s}\right) - \frac{a^2 n\alpha^2}{2^{13}\sigma^2\log\left(\frac{n\alpha^2}{d^2}\right)d^2}\right).$$

In particular, if $a \gg \frac{\sigma d}{\alpha\sqrt{n}}\log^{1/2}\left(\frac{n\alpha^2}{d^2}\right)\log^{1/2}\left(\frac{d}{s}\right)$ *it holds*

$$\sup_{\theta\in\Theta_d^+(s,a)} \frac{1}{s}\mathbb{E}_{Q(P_\theta^{\otimes n})}|\hat{\eta}^+(Z^1,\dots,Z^d)-\eta| \to 0. \tag{3.12}$$

Moreover, if $a \gg \frac{\sigma d}{\alpha\sqrt{n}}\log^{1/2}\left(\frac{n\alpha^2}{d^2}\right)\log^{1/2}(d)$

$$\sup_{\theta\in\Theta_d^+(s,a)} \mathbb{E}_{Q(P_\theta^{\otimes n})}|\hat{\eta}^+(Z^1,\dots,Z^d))-\eta| \to 0. \tag{3.13}$$

If $n\alpha^2/d^2 \to \infty$ with $(n\alpha^2/d^2) \gg \log(n\alpha^2/d^2)\log(d/s)$, then Corollary 3.2.7 combined with Corollary 3.2.5 and with the lower bound (3.4) prove a phase transition result (up to log factors) at the value $a^* = a^*(n,\alpha,d,\sigma) = \sigma d/(\alpha\sqrt{n})$. Indeed, we get that almost full recovery is impossible in the Coordinate Local case for all $a \le Ca^*$ and is possible for all $a \gg a^*\log^{1/2}(n\alpha^2/d^2)\log^{1/2}(d/s)$.

3.3 Minimax risk using coordinate global non-interactive privacy mechanisms

In this section, we study the minimax risk (3.3). We prove that in the Coordinate Global case, almost full recovery and exact recovery are possible under weaker assumptions than the one we obtained for the Coordinate Local case.

3.3.1 Privacy mechanism

We describe in this section the privacy mechanism we use to obtain private data that will be used to design a private selector and to obtain upper bounds on the minimax risk (3.3) in the Coordinate Global case.

For all $i \in [\![1,n]\!]$, the private view Z^i of X^i is obtained using the following steps:

- Compute $f_T(X^i) = ([X_j^i]_T)_{j=1,\dots,d}$ where $[\cdot]_T = \max\{-T, \min\{\cdot, T\}\}$ denotes the

censoring operator of level T and T will be specified later.

- Define a random vector $\tilde{X}^i \in \mathbb{R}^d$ with coordinates

$$\tilde{X}^i_j \sim \begin{cases} T & \text{with probability } \frac{1}{2} + \frac{[X^i_j]_T}{2T} \\ -T & \text{with probability } \frac{1}{2} - \frac{[X^i_j]_T}{2T}. \end{cases}$$

- Sample $Y^i \sim \mathcal{B}(\pi_\alpha)$ where $\pi_\alpha = e^\alpha/(e^\alpha + 1)$ and generate

$$\tilde{Z}^i \sim \begin{cases} \mathcal{U}\left(\tilde{z} \in \{-B, B\}^d \mid \langle \tilde{z}, \tilde{X}^i \rangle > 0 \text{ or } (\langle \tilde{z}, \tilde{X}^i \rangle = 0 \text{ and } \tilde{z}_1 = (B/T)\tilde{X}^i_1)\right) & \text{if } Y^i = 1 \\ \mathcal{U}\left(\tilde{z} \in \{-B, B\}^d \mid \langle \tilde{z}, \tilde{X}^i \rangle < 0 \text{ or } (\langle \tilde{z}, \tilde{X}^i \rangle = 0 \text{ and } \tilde{z}_1 = -(B/T)\tilde{X}^i_1)\right) & \text{if } Y^i = 0. \end{cases}$$

with

$$B = T\frac{e^\alpha + 1}{e^\alpha - 1}K_d, \text{ where } \frac{1}{K_d} = \begin{cases} \frac{1}{2^{d-1}}\binom{d-1}{\frac{d-1}{2}} & \text{if } d \text{ is odd} \\ \frac{(d-2)!(d-2)}{2^{d-1}(\frac{d}{2}-1)!\frac{d}{2}!} & \text{if } d \text{ is even.} \end{cases} \tag{3.14}$$

- Define the vector Z^i by $Z^i = \tilde{Z}^i$ if d is odd, and by its components

$$Z^i_j = \begin{cases} \frac{d-2}{2(d-1)}\tilde{Z}^i_1 & \text{if } j = 1 \\ \tilde{Z}^i_j & \forall j \in [\![2, d]\!], \end{cases}$$

if d is even.

This mechanism is strongly inspired by the one proposed by Duchi et al. [30] for mean estimation on the set of distributions P supported on $\mathbb{B}_\infty(r) \subset \mathbb{R}^d$ with $\|\mathbb{E}[X]\|_0 \leq s$. In particular, if d is odd, the event $\{\langle \tilde{z}, \tilde{X}^i \rangle = 0\}$ has probability zero for all $\tilde{z} \in \{-B, B\}^d$ and our mechanism coincides in this case with the one proposed by Duchi et al. [30] at the exception that we added a censoring step. Since in our framework the X^i are not compactly supported, this censoring step is needed so that the probabilities appearing in the definition of $\tilde{X}^i$ are non-negative.

Proposition 3.3.1. *For all $i \in [\![1, n]\!]$, Z^i is an α-differentially private view of X^i.*

The following proposition will be useful in the analysis of the selector proposed in Section 3.3.2.

Proposition 3.3.2. *For all $i \in [\![1, n]\!]$, it holds*

$$\mathbb{E}[Z^i \mid X^i] = f_T(X^i).$$

The proofs of Proposition 3.3.1 and Proposition 3.3.2 can be found respectively in Section 3.6.1 and 3.6.2 of the Appendix. Note that it also holds $\mathbb{E}[Z^i \mid X^i] = f_T(X_i)$ when Z_i is produced via the Laplace mechanism described in Subsection 3.2.2. However the variance $\mathrm{Var}(Z_j^i \mid X^i)$ is slower by a multiplicative factor d when Z^i is produced with the Laplace mechanism than when it is obtained with the above coordinate global mechanism. Indeed, if Z^i is produced with the above mechanism, then we have $\mathrm{Var}(Z_j^i \mid X^i) \leq B^2$. Stirling's approximation yields $K_d^2 \lesssim d$ for d large enough, see Lemma 3.6.1 in Appendix 3.6.3 for details. Thus, if α is bounded, we obtain $\mathrm{Var}(Z_j^i \mid X^i) \leq T^2 d/\alpha^2$. Now, if Z^i is produced with the Laplace mechanism then it holds $\mathrm{Var}(Z_j^i \mid X^i) = 8T^2 d^2/\alpha^2$. This faster variance explains that we will obtain better results when allowing for coordinate global mechanisms.

3.3.2 Upper bounds

Using the privatized data of the previous subsection, we define two selectors that will enable us to obtain upper bounds on the minimax risk (3.3). As in the Coordinate Local case, for the class $\Theta_d^+(s,a)$, we will use the selector $\hat{\eta}^+$ with the components

$$\hat{\eta}_j^+ = I\left(\frac{1}{n}\sum_{i=1}^n Z_j^i \geq \tau\right), \quad j = 1, \dots, d, \tag{3.15}$$

where the threshold τ has to be chosen. For the class $\Theta_d(s,a)$, we will use the selector $\hat{\eta}$ with the components

$$\hat{\eta}_j = I\left(\left|\frac{1}{n}\sum_{i=1}^n Z_j^i\right| \geq \tau\right), \quad j = 1, \dots, d. \tag{3.16}$$

We now study the performances of these selectors.

The following result gives an upper bound on the risk of selector (3.15) when $a \geq C\sigma$ and will enable us to obtain sufficient conditions so that almost full recovery is possible when $a \geq 2\sigma$ in the Coordinate Global case.

Proposition 3.3.3. *Assume that $a > b\sigma$ for some constant $b > 0$. Set $C_1 := 1 - 2\Phi(-b)$. If τ, T are chosen such that*

$$T \leq a - \sigma b, \text{ and } C_1 T - \tau > 0,$$

then it holds for all $\theta \in \Theta_d^+(s,a)$,

$$\mathbb{E}\left[\frac{1}{s}|\hat{\eta}^+ - \eta|\right] \leq \frac{d-|S|}{s}\exp\left(-\frac{n\tau^2}{2B^2}\right) + \frac{|S|}{s}\exp\left(-\frac{n(C_1T-\tau)^2}{2B^2}\right),$$

where S *denotes the support of* θ. *In particular, choosing* $T = \sigma$ *and* $\tau = C_1T/2$ *with* $C_1 = 1 - 2\Phi(-1)$ *yields*

$$\sup_{\theta\in\Theta_d^+(s,a)} \mathbb{E}\left[\frac{1}{s}|\hat{\eta}^+ - \eta|\right] \leq \frac{d}{s}\exp\left(-\frac{C_1^2 n(e^\alpha-1)^2}{8(e^\alpha+1)^2K_d^2}\right)$$

for all $a \geq 2\sigma$.

The proof of Proposition 3.3.3 can be found in section 3.6.4 of the Appendix. Note that we can provide similar results on the class $\Theta_d(s,a)$ considering the selector $\hat{\eta}$. The upper bounds are the same than for the class $\Theta_d^+(s,a)$ up to a multiplicative factor 2 that comes from the use in the proof of the two-sided Hoeffding's inequality instead of the one-sided inequality. Since $K_d \leq C\sqrt{d}$ for d large enough, we obtain that a sufficient condition for almost full recovery to be possible when $a \geq 2\sigma$ is that $\frac{n(e^\alpha-1)^2}{(e^\alpha+1)^2 d} \gtrsim \log(d/s)$. Moreover, using that $(e^\alpha-1)^2/(e^\alpha+1)^2 \geq 0.2\alpha^2$ if $\alpha \leq 1$, we obtain that a sufficient condition for almost full recovery to be possible when $a \geq 2\sigma$ and $\alpha \leq 1$ is that $n\alpha^2/d \gtrsim \log(d/s)$. This improves the result we obtained when we considered only privacy mechanisms acting coordinates by coordinates for which we needed $n\alpha^2/d^2 \gtrsim \log(d/s)$. We now deal with the case $a << \sigma$.

Proposition 3.3.4. *Let* $a > 0$. *If* T *and* τ *are chosen such that*

$$T \geq a + \sigma\sqrt{2\log\left(\max\left\{e, \frac{4\sigma}{a\sqrt{2\pi}}\right\}\right)}, \text{ and } \tau < a/2,$$

then it holds for all $\theta \in \Theta_d^+(s,a)$,

$$\mathbb{E}\left[\frac{1}{s}|\hat{\eta}^+ - \eta|\right] \leq \frac{d-|S|}{s}\exp\left(-\frac{n\tau^2}{2B^2}\right) + \frac{|S|}{s}\exp\left(-\frac{n(a/2-\tau)^2}{2B^2}\right),$$

where S *denotes the support of* θ.

The proof of Proposition 3.3.4 can be found in Appendix 3.6.5.

Corollary 3.3.5. *Assume that* $\alpha/d \to 0$, $n\alpha^2/d \to +\infty$ *and* $\sigma\sqrt{d}/(\alpha\sqrt{n}) \ll a \leq 2\sigma$. *The selector* $\hat{\eta}^+$ *defined by* (3.15) *with* $T = a + \sigma\sqrt{2\log\left(\sqrt{\frac{n\alpha^2}{d}}\right)}$ *and* $\tau = a/4$ *satisfies for* n, d *large enough*

$$\sup_{\theta\in\Theta_d^+(s,a)} \frac{1}{s}\mathbb{E}_{Q(P_\theta^{\otimes n})}|\hat{\eta}^+(Z^1,\dots,Z^d)) - \eta| \leq \frac{d}{s}\exp\left(-\frac{n(e^\alpha-1)^2a^2}{2^7\sigma^2(e^\alpha+1)^2K_d^2\log(n\alpha^2/d)}\right).$$

In particular, if $\alpha \in (0,1]$, *if* $n\alpha^2/d \to +\infty$ *with* $(n\alpha^2/d)/\log(n\alpha^2/d) \gg \log(d)$ *then it holds*

$$\sup_{\theta\in\Theta_d^+(s,a)} \mathbb{E}_{Q(P_\theta^{\otimes n})}|\hat{\eta}^+(Z^1,\dots,Z^d)) - \eta| \to 0,$$

for all a *satisfying* $\sigma\sqrt{\frac{d}{n\alpha^2}}\sqrt{\log\left(\frac{n\alpha^2}{d}\right)\log(d)} \ll a \leq 2\sigma$.

The first statement in Corollary 3.3.5 is a direct consequence of Proposition 3.3.4. The second statement is a direct consequence of the first one where we have used $(e^\alpha-1)^2/(e^\alpha+1)^2 \geq 0.2\alpha^2$ for $\alpha \in (0,1]$ and $K_d \leq C\sqrt{d}$ for d large enough. In the next subsection, we complement these results with a lower bound. This will enable us to exhibit a value a^* such that exact recovery is impossible for all $a \leq a^*$ and possible for $a \gg a^*$ under the assumptions $\alpha \in (0,1]$ and $n\alpha^2/d \to \infty$ with $(n\alpha^2/d)/\log(n\alpha^2/d) \gg \log(d)$.

3.3.3 Lower bound

Proposition 3.3.6. *For any* $a > 0$, $\alpha > 0$, $d \geq 4$, $1 \leq s \leq d$, $n \geq 1$, *we have*

$$\inf_{Q\in\mathcal{Q}_\alpha}\inf_{\hat{\eta}\in\mathcal{T}}\sup_{\theta\in\Theta_d^+(s,a)} \mathbb{E}_{Q(P_\theta^{\otimes n})}|\hat{\eta}-\eta| \geq \frac{1}{4}\left(1 - \frac{2n(e^\alpha-1)^2}{d\log(d)}\left[\exp\left(\frac{a^2}{\sigma^2}\right)-1\right]\right).$$

The proof of Proposition 3.3.6 is based on a private version of Fano's method, see Proposition 2 in [30]. It can be found in Section 3.6.6 of the Appendix. Using that $(e^\alpha - 1)^2 \leq 4\alpha^2$ for $\alpha \in (0,1)$ and $\exp(x^2) - 1 \leq 14x^2$ for $0 \leq x \leq 2$, Proposition 3.3.6 immediatly shows the following.

Corollary 3.3.7. *Let* $\alpha \in (0,1)$. *If* $n\alpha^2/(d\log d) \leq C/448$ *for some constant* $C \in (0,1)$ *then it holds*

$$\inf_{Q\in\mathcal{Q}_\alpha}\inf_{\hat{\eta}\in\mathcal{T}}\sup_{\theta\in\Theta_d^+(s,a)} \mathbb{E}_{Q(P_\theta^{\otimes n})}|\hat{\eta}-\eta| \geq \frac{1}{4}(1-C) > 0,$$

for all $a \leq 2\sigma$.

This shows that exact recovery is impossible for all $a \leq 2\sigma$ if $n\alpha^2/(d\log d) \leq C/448$ for some constant $C \in (0,1)$. Proposition 3.3.6 also implies that exact recovery is impossible if $a \leq \sigma\sqrt{\log(1+Cd\log d/(8n\alpha^2))}$ for some constant $C \in (0,1)$. However, unlike the coordinate local case, the lower bound provided by Proposition 3.3.6 does not allow us to say that exact recovery is also impossible for $a \geq \max\{2\sigma, \sigma\sqrt{\log(1+Cd\log d/(8n\alpha^2))}\}$ when $n\alpha^2/(d\log d)$ is bounded from above. The following corollary is also a direct consequence of Proposition 3.3.6. It shows that when $n\alpha^2/(d\log d) \to \infty$, exact recovery is still impossible if a is too small.

Corollary 3.3.8. *If $\alpha \in (0,1)$, $n\alpha^2/d \to +\infty$ with $n\alpha^2/d \gg \log d$ and $a \leq (\sigma/224)\sqrt{d\log d/(n\alpha^2)}$ it holds*

$$\liminf_{d\to+\infty} \inf_{Q\in\mathcal{Q}_\alpha} \inf_{\hat{\eta}\in\mathcal{T}} \sup_{\theta\in\Theta_d^+(s,a)} \mathbb{E}_{Q(P_\theta^{\otimes n})}|\hat{\eta}-\eta| \geq \frac{1}{8}.$$

The lower bound of Proposition 3.3.6 combined with the upper bounds of Subsection 3.3.2 exhibit a phase transition at the value a^* (up to a logarithmic factor) such that exact recovery is impossible for all $a \leq a^*$ and possible for $a \gg a^*$ under the assumptions $\alpha \in (0,1]$ and $n\alpha^2/d \to \infty$ with $(n\alpha^2/d)/\log(n\alpha^2/d) \gg \log(d)$. Precisely, set

$$a^* = a^*(n,\alpha,d,\sigma) = \frac{\sigma}{224}\sqrt{\frac{d\log d}{n\alpha^2}}.$$

Proposition 3.3.6 combined with Corollary 3.3.5 and Proposition 3.3.3 give the following result.

Corollary 3.3.9. *Assume that $\alpha \in (0,1]$ and $n\alpha^2/d \to +\infty$ with $(n\alpha^2/d)/\log(n\alpha^2/d) \gg \log(d)$. Then, exact recovery is impossible for all $a \leq a^*$ and is possible for all $a \gg a^*\sqrt{\log(n\alpha^2/d)}$.*

Note that Proposition 3.3.6 does not allow us to obtain impossibility results for almost full recovery in the regime $n\alpha^2/(d\log d) \gg 1$. Its proof relies on a private Fano's method (Proposition 2 in [30]) applied with the family of distributions $\{\mathcal{N}(a\omega_i, \sigma^2 I_d), i = 1,\dots,d\}$ where $\omega_i \in \{0,1\}^d$ is defined by $\omega_{ij} = \delta_{ij}$ and δ is the Kronecker delta. The same proof with ω_i defined by $\omega_{ij} = 1$ if $j \in [\![(i-1)s+1, is]\!]$ and $\omega_{ij} = 0$ otherwise for $i = 1,\dots\lfloor d/s\rfloor$, provides the following lower bound.

Proposition 3.3.10. *For any $a > 0$, $\alpha > 0$, $n \geq 1$. If $d/s \leq 4$ then we have*

$$\inf_{Q\in\mathcal{Q}_\alpha} \inf_{\hat{\eta}\in\mathcal{T}} \sup_{\theta\in\Theta_d^+(s,a)} \frac{1}{s}\mathbb{E}_{Q(P_\theta^{\otimes n})}|\hat{\eta}-\eta| \geq \frac{1}{4}\left(1 - \frac{2n(e^\alpha-1)^2}{\lfloor d/s\rfloor\log(\lfloor d/s\rfloor)}\left[\exp\left(\frac{sa^2}{\sigma^2}\right)-1\right]\right).$$

However, this bound turns out to be suboptimal in the sense that when it holds $(n\alpha^2/d)/\log(n\alpha^2/d) \gg \log(d/s)$ the combination of this bound with upper bounds in Proposition 3.3.3 and Corollary 3.3.5 allows us to exhibit the critical value a^* for almost full recovery only up to a logarithmic factor times the sparsity s. Indeed, on the one hand Proposition 3.3.3 and Corollary 3.3.5 prove that almost full recovery is possible for all $a \gg \sigma\sqrt{d/(n\alpha^2)}\sqrt{\log\left(n\alpha^2/d\right)\log(d/s)}$ in the regime $(n\alpha^2/d)/\log(n\alpha^2/d) \gg \log(d/s)$. On the other hand Proposition 3.3.10 proves that, in the same regime, almost full recovery is impossible for $a \lesssim (\sigma/s)\sqrt{d/(n\alpha^2)}\sqrt{\log(d/s)}$ but does not allow us to say what happen for $(\sigma/s)\sqrt{d/(n\alpha^2)}\sqrt{\log(d/s)} \ll a \lesssim \sigma\sqrt{d/(n\alpha^2)}\sqrt{\log(n\alpha^2/d)\log(d/s)}$.

3.4 Discussion

We addressed the problem of variable selection in the Gaussian mean model in $\mathbb{R}^d$ under local differential privacy constraints. We have provided lower and upper bounds on the rate of convergence for the expected Hamming loss over classes of at most s-sparse vectors whose non-zero coordinates are separated from 0 by a constant $a > 0$. When we restrict our attention to non-interactive mechanisms that act independently on each coordinate (*coordinate local privacy mechanisms*) we have proved that, contrary to the non-private setting, almost full recovery and exact recovery are impossible whatever the value of a in the high-dimensional regime. This is due to the fact that the loss of information due to privacy may reduce the effective sample size $N := n\alpha^2/d^2$ under the value 1, and this does not allow support recovery neither exact nor almost full.
However, in the regime $n\alpha^2/d^2 \gg \log(n\alpha^2/d^2)\log(d)$ we have exhibited a critical value a^* (up to a logarithmic factor) such that exact recovery is possible for all $a \gg a^*$ and impossible for all $a \leq a^*$. We have also proved that these results can be improved when allowing for all non-interactive locally differentially private mechanisms, that we also call *coordinate global*. The effective sample size is Nd in this case and it is larger than N.
For many estimation problems allowing for sequentially interactive privacy mechanisms do not improve substantially over non-interactive minimax rates. This includes for instance density estimation [13], one-dimensional mean estimation [30], and estimation of a linear functional of the true distribution [63]. However, for some estimation problems (see for instance the estimation of the integrated square of a density, [15]) and some testing problems (see [10] and [15]) allowing for sequentially interaction between data-holders can substantially improve over non-interactive minimax rates of estimation or non-interactive

minimax rates of testing. The change of regime from coordinate local to coordinate global privacy mechanisms suggests that support recovery will be improved for interactive privacy mechanisms, but it is left for future work to study whether that is indeed the case.

3.5 Appendix : Proofs of Section 3.2

3.5.1 Some auxiliary results for the proof of the lower bound

The proof of Theorem 3.2.1 strongly relies on the following result known as the Bayesian version of the Neyman-Pearson lemma.

Theorem 3.5.1 ([52], Problem 3.10)**.** *Let P_0 and P_1 be probability distributions possessing densities p_0 and p_1 with respect to a measure μ. Consider the problem of testing $H_0 : P = P_0$ against $H_1 : P = P_1$, and suppose that known probabilities π and $1-\pi$ can be assigned to H_0 and H_1 prior to the experiment. Then the test T^* given by*

$$T^*(X) = I((1-\pi)p_1(X) > \pi p_0(X))$$

is a minimizer of the overall probability of error resulting from the use of a test T,

$$\pi \mathbb{E}_0[T(X)] + (1-\pi)\mathbb{E}_1[1-T(X)].$$

The following lemmas are also useful to prove the lower bound.

Lemma 3.5.2. *Let $b, c > 0$. Let P and Q be two probability measures having densities p and q with respect to some measure μ. It holds*

$$\int \min\{bp(x), cq(x)\} \mathrm{d}\mu(x) \geq \frac{bc}{b+c} \left(\int \sqrt{p(x)q(x)} \mathrm{d}\mu(x) \right)^2.$$

The case $b = c = 1$ can be found in [72] (lemma 2.3). We generalize the proof for any $b, c > 0$.

Proof. Cauchy-Schwarz inequality yields

$$\begin{aligned} bc\left(\int \sqrt{p(x)q(x)}\mathrm{d}\mu(x)\right)^2 &= \left(\int \sqrt{bp(x)\cdot cq(x)}\mathrm{d}\mu(x)\right)^2 \\ &= \left(\int \sqrt{\min\{bp(x),cq(x)\}}\sqrt{\max\{bp(x),cq(x)\}}\mathrm{d}\mu(x)\right)^2 \\ &\leq \int \min\{bp(x),cq(x)\}\mathrm{d}\mu(x)\int \max\{bp(x),cq(x)\}\mathrm{d}\mu(x). \end{aligned}$$

Set $A=\{x : bp(x)\geq cq(x)\}$ and note that

$$\int \min\{bp,cq\}\mathrm{d}\mu+\int \max\{bp,cq\}\mathrm{d}\mu=\int_A cq\mathrm{d}\mu+\int_{A^C} bp\mathrm{d}\mu+\int_A bp\mathrm{d}\mu+\int_{A^C} cq\mathrm{d}\mu=b+c.$$

Thus,

$$\begin{aligned} bc\left(\int \sqrt{p(x)q(x)}\mathrm{d}\mu(x)\right)^2 &\leq \int \min\{bp(x),cq(x)\}\mathrm{d}\mu(x)\left[b+c-\int \min\{bp(x),q(x)\}\mathrm{d}\mu(x)\right] \\ &\leq (b+c)\int \min\{bp(x),q(x)\}\mathrm{d}\mu(x). \end{aligned}$$

□

In the proof of the lower bound, Lemma 3.5.2 will be combined with the following result whose proof can be found in [72].

Lemma 3.5.3. *Let P and Q be two probability measures having densities p and q with respect to some measure μ. It holds*

$$\left(\int \sqrt{p(x)q(x)}\mathrm{d}\mu(x)\right)^2 \geq \exp(-\mathrm{KL}(P,Q)).$$

3.5.2 Proof of Theorem 3.2.1

Let $Q\in\mathcal{Q}_\alpha^{CL}$ and let $\hat{\eta}$ be a separable selector. Since $\hat{\eta}_j$ depends only on $(Z_j^i)_{i=1,\dots,n}$, it holds

$$\mathbb{E}_{Q(P_\theta^{\otimes n})}|\hat{\eta}(Z)-\eta| = \sum_{j=1}^d \mathbb{E}_{\otimes_{i=1}^n Q_j^i P_{\theta_j}}|\hat{\eta}_j(Z_j^1,\dots,Z_j^n)-\eta_j|.$$

Following the proof of Theorem 2.2 in [12], we denote by Θ' the set of all θ in $\Theta_d^+(s,a)$ such that exactly s components of θ are equal to a and the remaining $d-s$ components are equal to 0. Since Θ' is a subset of $\Theta_d^+(s,a)$, it holds

$$\begin{aligned}
\sup_{\theta\in\Theta_d^+(s,a)} \frac{1}{s}\mathbb{E}_{Q(P_\theta^{\otimes n})}|\hat{\eta}(Z)-\eta| &\geq \frac{1}{s|\Theta'|}\sum_{\theta\in\Theta'}\sum_{j=1}^{d}\mathbb{E}_{\otimes_{i=1}^n Q_j^i P_{\theta_j}}|\hat{\eta}_j(Z_j^1,\dots,Z_j^n)-\eta_j| \\
&= \frac{1}{s|\Theta'|}\sum_{j=1}^{d}\left(\sum_{\theta\in\Theta':\theta_j=0}\mathbb{E}_{\otimes_{i=1}^n Q_j^i P_0}(\hat{\eta}_j)+\sum_{\theta\in\Theta':\theta_j=a}\mathbb{E}_{\otimes_{i=1}^n Q_j^i P_a}(1-\hat{\eta}_j)\right) \\
&= \frac{1}{s}\sum_{j=1}^{d}\left(\left(1-\frac{s}{d}\right)\mathbb{E}_{\otimes_{i=1}^n Q_j^i P_0}(\hat{\eta}_j)+\frac{s}{d}\mathbb{E}_{\otimes_{i=1}^n Q_j^i P_a}(1-\hat{\eta}_j)\right) \\
&\geq \frac{1}{s}\sum_{j=1}^{d}\inf_{T\in[0,1]}\left(\left(1-\frac{s}{d}\right)\mathbb{E}_{\otimes_{i=1}^n Q_j^i P_0}(T)+\frac{s}{d}\mathbb{E}_{\otimes_{i=1}^n Q_j^i P_a}(1-T)\right).
\end{aligned}$$

Set

$$L_j^* = \inf_{T\in[0,1]}\left(\left(1-\frac{s}{d}\right)\mathbb{E}_{\otimes_{i=1}^n Q_j^i P_0}(T)+\frac{s}{d}\mathbb{E}_{\otimes_{i=1}^n Q_j^i P_a}(1-T)\right).$$

Since Q_j^i provides α_j-differential privacy, the channel probabilities $Q_j^i(\cdot \mid x)$ have densities $z \mapsto q_j^i(z \mid x)$ with respect to some measure μ_j^i. Therefore, $dQ_j^i P_0(z) = m_{j,0}^i(z)\mathrm{d}\mu_j^i(z)$, and $dQ_j^i P_a(z) = m_{j,a}^i(z)\mathrm{d}\mu_j^i(z)$, where $m_{j,b}^i(z) = \int_{\mathbb{R}} q_j^i(z \mid x)dP_b(x)$, $b \in \{0,a\}$. Thus, for $b \in \{0,a\}$, it holds

$$d(\otimes_{i=1}^n Q_j^i P_b)(y_1,\dots,y_n) = [\prod_{i=1}^n m_{j,b}^i(y_i)]\mathrm{d}\mu_j(y_1,\dots,y_n),$$

where $\mu_j = \mu_j^1 \otimes \cdots \otimes \mu_j^n$. According to Theorem 3.5.1, the infimum L_j^* is thus attained for $T = T_j^*$ given by

$$T_j^*(Y_1,\dots,Y_n) = I\left(\frac{s}{d}\prod_{i=1}^n m_{j,a}^i(Y_i) > \left(1-\frac{s}{d}\right)\prod_{i=1}^n m_{j,0}^i(Y_i)\right).$$

Set $A_j = \{(y_1, \dots, y_n) \in \mathbb{R}^n : \frac{s}{d} \prod_{i=1}^n m_{j,a}^i(y_i) > \left(1 - \frac{s}{d}\right) \prod_{i=1}^n m_{j,0}^i(y_i)\}$.

$$\begin{aligned}
\sup_{\theta \in \Theta_d^+(s,a)} \frac{1}{s} \mathbb{E}_{Q(P_\theta^{\otimes n})} |\hat{\eta}(Z) - \eta| &\geq \frac{1}{s} \sum_{j=1}^d \left[\left(1 - \frac{s}{d}\right) \int_{A_j} [\prod_{i=1}^n m_{j,0}^i(y_i)] \mathrm{d}\mu_j(y_1, \dots, y_n) \right. \\
&\qquad \left. + \frac{s}{d} \int_{A_j^C} [\prod_{i=1}^n m_{j,a}^i(y_i)] \mathrm{d}\mu_j(y_1, \dots, y_n) \right] \\
&= \frac{1}{s} \sum_{j=1}^d \int_{\mathbb{R}^n} \min \left\{ \left(1 - \frac{s}{d}\right) \prod_{i=1}^n m_{j,0}^i(y_i), \frac{s}{d} \prod_{i=1}^n m_{j,a}^i(y_i) \right\} \mathrm{d}\mu_j(y_1, \dots, y_n) \\
&\geq \left(1 - \frac{s}{d}\right) \cdot \frac{1}{d} \sum_{j=1}^d \left(\int_{\mathbb{R}^n} \sqrt{\left(\prod_{i=1}^n m_{j,0}^i(y_i) \right) \left(\prod_{i=1}^n m_{j,a}^i(y_i) \right)} \mathrm{d}\mu_j(y_1, \dots, y_n) \right)^2 \\
&\geq \left(1 - \frac{s}{d}\right) \cdot \frac{1}{d} \sum_{j=1}^d \exp\left(-\mathrm{KL}\left(\otimes_{i=1}^n Q_j^i P_0, \otimes_{i=1}^n Q_j^i P_a \right) \right),
\end{aligned}$$

where the two last inequalities follow from lemma 3.5.2 and lemma 3.5.3. Using successively a property of the Kullback-Leibler divergence and Theorem 1 of [30] on the contractive effects of privacy on pairs of distribution, we obtain

$$\begin{aligned}
\sup_{\theta \in \Theta_d^+(s,a)} \frac{1}{s} \mathbb{E}_{Q(P_\theta^{\otimes n})} |\hat{\eta}(Z) - \eta| &\geq \left(1 - \frac{s}{d}\right) \cdot \frac{1}{d} \sum_{j=1}^d \exp\left(-\sum_{i=1}^n \mathrm{KL}\left(Q_j^i P_0, Q_j^i P_a \right) \right) \\
&\geq \left(1 - \frac{s}{d}\right) \cdot \frac{1}{d} \sum_{j=1}^d \exp\left(-4n(e^{\alpha/d} - 1)^2 \mathrm{TV}(P_0, P_a)^2 \right) \\
&= \left(1 - \frac{s}{d}\right) \exp\left(-4n(e^{\alpha/d} - 1)^2 \mathrm{TV}(P_0, P_a)^2 \right).
\end{aligned}$$

Since this result holds for all $Q \in \mathcal{Q}_\alpha^{CL}$ and all separable selector $\hat{\eta}$, we obtain

$$\inf_{Q \in \mathcal{Q}_\alpha^{CL}} \inf_{\hat{\eta} \in \mathcal{T}} \sup_{\theta \in \Theta_d^+(s,a)} \frac{1}{s} \mathbb{E}_{Q(P_\theta^{\otimes n})} |\hat{\eta} - \eta| \geq \left(1 - \frac{s}{d}\right) \exp\left(-4n(e^{\alpha/d} - 1)^2 \mathrm{TV}(P_0, P_a)^2 \right).$$

The inequality $TV(P_0, P_a) \leq 1$ and Pinsker's inequality

$$TV(P_0, P_a) \leq \sqrt{\frac{\mathrm{KL}(P_0, P_a)}{2}} = \frac{a}{2\sigma},$$

then imply the statement of Theorem 3.2.1.

3.5.3 Some auxiliary results for the upper bounds

Lemma 3.5.4. *For all $a \geq 0$, $\frac{1}{n}\sum_{i=1}^n \left([a+\sigma\xi_j^i]_T - \mathbb{E}\left[[a+\sigma\xi_j^i]_T\right]\right)$ is a sub-gaussian random variable with parameter at most $\min\left\{\frac{T}{\sqrt{n}}, \frac{\sigma}{\sqrt{n}}\right\}$.*

Proof. First, observe that $[a+\sigma\xi_j^i]_T \in [-T,T]$ almost surely. Then, according to Exercise 2.4 in [76] the random variable $[a+\sigma\xi_j^i]_T - \mathbb{E}\left[[a+\sigma\xi_j^i]_T\right]$ is sub-gaussian with parameter at most T for all $i \in [\![1,n]\!]$. Since $(\xi_j^i)_{i=1,\dots,n}$ are independent, we obtain that $\frac{1}{n}\sum_{i=1}^n \left([a+\sigma\xi_j^i]_T - \mathbb{E}\left[[a+\sigma\xi_j^i]_T\right]\right)$ is sub-gaussian with parameter at most $T/\sqrt{n}$. We now prove that it is also subgaussian with parameter at most $\sigma/\sqrt{n}$. To this aim, define $g : x \in \mathbb{R}^n \mapsto \frac{1}{n}\sum_{i=1}^n [a+\sigma x_i]_T \in \mathbb{R}$. It holds

$$|g(x)-g(y)| \leq \frac{\sigma}{\sqrt{n}}\|x-y\|_2 \quad \forall x,y \in \mathbb{R}^n.$$

Set $Y = (\xi_j^1, \dots, \xi_j^n)$. According to Theorem 2.26 in [76], $g(Y) - \mathbb{E}[g(Y)]$ is sub-gaussian with parameter at most $\sigma/\sqrt{n}$. □

We now recall Bernstein's inequality (cf. [11] Corollary 2.11).

Theorem 3.5.5. *Let $Y_1, \dots, Y_n$ be independent real valued random variables. Assume that there exist some positive numbers v and c such that*

$$\sum_{i=1}^n \mathbb{E}[Y_i^2] \leqslant v, \tag{3.17}$$

and for all integers $m \geqslant 3$

$$\sum_{i=1}^n \mathbb{E}[|Y_i|^m] \leqslant \frac{m!}{2} v c^{m-2}. \tag{3.18}$$

Let $S = \sum_{i=1}^n (Y_i - \mathbb{E}[Y_i])$, then for every positive t

$$\mathbb{P}(S \geqslant t) \leqslant \exp\left(-\frac{t^2}{2(v+ct)}\right). \tag{3.19}$$

Note that if $v \leq ct$ then (3.19) yields $\mathbb{P}(S \geq t) \leq \exp(-t/4c)$. If $ct \leq v$ then (3.19) yields $\mathbb{P}(S \geq t) \leq \exp(-t^2/4v)$.

3.5.4 Proof of Proposition 3.2.4

It holds

$$\begin{aligned}|\hat{\eta}^+ - \eta| &= \sum_{j:\eta_j=0} \hat{\eta}_j^+ + \sum_{j:\eta_j=1} (1-\hat{\eta}_j^+) \\ &= \sum_{j:\eta_j=0} I\left(\frac{1}{n}\sum_{i=1}^n [\sigma\xi_j^i]_T + \frac{2Td}{n\alpha}\sum_{i=1}^n W_j^i \geq \tau\right) \\ &\qquad + \sum_{j:\eta_j=1} I\left(\frac{1}{n}\sum_{i=1}^n [\theta_j + \sigma\xi_j^i]_T + \frac{2Td}{n\alpha}\sum_{i=1}^n W_j^i < \tau\right).\end{aligned}$$

Thus,

$$\begin{aligned}\mathbb{E}\left[\frac{1}{s}|\hat{\eta}^+ - \eta|\right] &= \frac{1}{s}\sum_{j:\eta_j=0} \underbrace{\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^n [\sigma\xi_j^i]_T + \frac{2Td}{n\alpha}\sum_{i=1}^n W_j^i \geq \tau\right)}_{=T_{1,j}} \\ &\qquad + \frac{1}{s}\sum_{j:\eta_j=1} \underbrace{\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^n [\theta_j + \sigma\xi_j^i]_T + \frac{2Td}{n\alpha}\sum_{i=1}^n W_j^i < \tau\right)}_{=T_{2,j}}.\end{aligned}$$

We first study $T_{1,j}$. It holds

$$T_{1,j} \leq \mathbb{P}\left(\frac{1}{n}\sum_{i=1}^n [\sigma\xi_j^i]_T \geq \frac{\tau}{2}\right) + \mathbb{P}\left(\sum_{i=1}^n W_j^i \geq \frac{\tau n\alpha}{4Td}\right).$$

Note that $\mathbb{E}\left[[\sigma\xi_j^i]_T\right] = 0$. Using Lemma 3.5.4 to bound from above the first term and Bernstein's inequality (3.19) with $v = 2n$ and $c = 1$ to bound from above the second term, we obtain if $\tau\alpha/(8Td) < 1$

$$T_{1,j} \leq \exp\left(-\frac{n\tau^2}{2^3\min\{T^2,\sigma^2\}}\right) + \exp\left(-\frac{\tau^2 n\alpha^2}{2^7 T^2 d^2}\right).$$

Since $x \mapsto [x]_T$ is a non-decreasing function and since $\theta_j \geq a$ for all j such that $\eta_j = 1$, it holds

$$\begin{aligned}
T_{2,j} &\leq \mathbb{P}\left(\frac{1}{n}\sum_{i=1}^{n}[a+\sigma\xi_j^i]_T + \frac{2Td}{n\alpha}\sum_{i=1}^{n}W_j^i < \tau\right) \\
&= \mathbb{P}\left(\frac{1}{n}\sum_{i=1}^{n}\left([a+\sigma\xi_j^i]_T - \mathbb{E}\left[[a+\sigma\xi_j^i]_T\right]\right) + \mathbb{E}\left[[a+\sigma\xi_j^1]_T\right] + \frac{2Td}{n\alpha}\sum_{i=1}^{n}W_j^i < \tau\right) \\
&= \mathbb{P}\left(-\frac{1}{n}\sum_{i=1}^{n}\left([a+\sigma\xi_j^i]_T - \mathbb{E}\left[[a+\sigma\xi_j^i]_T\right]\right) - \frac{2Td}{n\alpha}\sum_{i=1}^{n}W_j^i > \mathbb{E}\left[[a+\sigma\xi_j^1]_T\right] - \tau\right).
\end{aligned}$$

Now, if $\xi \sim \mathcal{N}(0,1)$ then

$$\begin{aligned}
\mathbb{E}\left[[a+\sigma\xi]_T\right] &= T\mathbb{P}\left(\xi > \frac{T-a}{\sigma}\right) - T\mathbb{P}\left(\xi < \frac{-T-a}{\sigma}\right) + \mathbb{E}\left[(a+\sigma\xi)I(|a+\sigma\xi| \leq T)\right] \\
&= T\mathbb{P}\left(\xi > \frac{T-a}{\sigma}\right) - T\mathbb{P}\left(\xi < \frac{-T-a}{\sigma}\right) + \int_{\frac{-T-a}{\sigma}}^{\frac{T-a}{\sigma}}(a+\sigma x)\frac{1}{\sqrt{2\pi}}e^{-x^2/2}\mathrm{d}x \\
&\geq T\mathbb{P}\left(\xi > \frac{T-a}{\sigma}\right) - T\mathbb{P}\left(\xi < \frac{-T-a}{\sigma}\right) + a\mathbb{P}\left(\frac{-T-a}{\sigma} \leq \xi \leq \frac{T-a}{\sigma}\right) \\
&\qquad + \sigma\cdot\left(\frac{-T-a}{\sigma}\right)\cdot\mathbb{P}\left(\frac{-T-a}{\sigma} \leq \xi \leq \frac{T-a}{\sigma}\right) \\
&= T\left[\mathbb{P}\left(\xi > \frac{T-a}{\sigma}\right) - \mathbb{P}\left(\xi \leq \frac{T-a}{\sigma}\right)\right] \\
&= T\left[1 - 2\Phi\left(\frac{T-a}{\sigma}\right)\right],
\end{aligned}$$

where Φ denotes the standard Gaussian cumulative distribution function. Thus, if $a \geq T + \sigma b$ for some $b > 0$, it holds $\mathbb{E}\left[[a+\sigma\xi_j^1]_T\right] \geq C_1 T$ with $C_1 = 1 - 2\Phi(-b)$, and

$$\begin{aligned}
T_{2,j} &\leq \mathbb{P}\left(-\frac{1}{n}\sum_{i=1}^{n}\left([a+\sigma\xi_j^i]_T - \mathbb{E}\left[[a+\sigma\xi_j^i]_T\right]\right) - \frac{2Td}{n\alpha}\sum_{i=1}^{n}W_j^i > C_1T - \tau\right) \\
&\leq \mathbb{P}\left(-\frac{1}{n}\sum_{i=1}^{n}\left([a+\sigma\xi_j^i]_T - \mathbb{E}\left[[a+\sigma\xi_j^i]_T\right]\right) > \frac{C_1T-\tau}{2}\right) \\
&\qquad + \mathbb{P}\left(\sum_{i=1}^{n}\left(-W_j^i\right) > \frac{n\alpha(C_1T-\tau)}{4Td}\right).
\end{aligned}$$

We can now bound from above the first term using lemma 3.5.4 and the second term using Bernstein's inequality. This gives, if $C_1T \geq \tau$ and $\alpha(C_1T-\tau)/(8Td) \leq 1$

$$T_{2,j} \leq \exp\left(-\frac{n(C_1T-\tau)^2}{2^3\min\{T^2,\sigma^2\}}\right) + \exp\left(-\frac{(C_1T-\tau)^2n\alpha^2}{2^7T^2d^2}\right).$$

This ends the proof of (3.8). We now prove (3.9). If $\theta \in \Theta_d(s,a)$, we use the estimator $\hat{\eta}$ instead of $\hat{\eta}^+$ and it holds

$$\mathbb{E}\left[\frac{1}{s}|\hat{\eta}-\eta|\right] = \frac{1}{s}\sum_{j:\eta_j=0} \underbrace{\mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^n [\sigma\xi_j^i]_T + \frac{2Td}{n\alpha}\sum_{i=1}^n W_j^i\right| \geq \tau\right)}_{=\tilde{T}_{1,j}} + \frac{1}{s}\sum_{j:\eta_j=1} \underbrace{\mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^n [\theta_j+\sigma\xi_j^i]_T + \frac{2Td}{n\alpha}\sum_{i=1}^n W_j^i\right| < \tau\right)}_{=\tilde{T}_{2,j}}.$$

We first study $\tilde{T}_{1,j}$. It holds

$$\begin{aligned}
\tilde{T}_{1,j} &\leq \mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^n [\sigma\xi_j^i]_T\right| + \frac{2Td}{n\alpha}\left|\sum_{i=1}^n W_j^i\right| \geq \tau\right) \\
&\leq \mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^n [\sigma\xi_j^i]_T\right| \geq \frac{\tau}{2}\right) + \mathbb{P}\left(\left|\sum_{i=1}^n W_j^i\right| \geq \frac{\tau n\alpha}{4Td}\right) \\
&\leq 2\left[\exp\left(-\frac{n\tau^2}{2^3\min\{T^2,\sigma^2\}}\right) + \exp\left(-\frac{\tau^2 n\alpha^2}{2^7T^2d^2}\right)\right],
\end{aligned}$$

if $\tau\alpha/(8Td) < 1$, where we have used the two-sided versions of the concentration inequalities we used to prove (3.8). We now study $\tilde{T}_{2,j}$. For all j such that $\eta_j = 1$, it holds

$$\begin{aligned}
\tilde{T}_{2,j} &= \mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^n \left([\theta_j+\sigma\xi_j^i]_T - \mathbb{E}\left[[\theta_j+\sigma\xi_j^i]_T\right]\right) + \mathbb{E}\left[[\theta_j+\sigma\xi_j^1]_T\right] + \frac{2Td}{n\alpha}\sum_{i=1}^n W_j^i\right| < \tau\right) \\
&\leq \mathbb{P}\left(\left|\mathbb{E}\left[[\theta_j+\sigma\xi_j^1]_T\right]\right| - \left|\frac{1}{n}\sum_{i=1}^n \left([\theta_j+\sigma\xi_j^i]_T - \mathbb{E}\left[[\theta_j+\sigma\xi_j^i]_T\right]\right) + \frac{2Td}{n\alpha}\sum_{i=1}^n W_j^i\right| < \tau\right) \\
&= \mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^n \left([\theta_j+\sigma\xi_j^i]_T - \mathbb{E}\left[[\theta_j+\sigma\xi_j^i]_T\right]\right) + \frac{2Td}{n\alpha}\sum_{i=1}^n W_j^i\right| > \left|\mathbb{E}\left[[\theta_j+\sigma\xi_j^1]_T\right]\right| - \tau\right)
\end{aligned}$$

Now, observe that

$$\left|\mathbb{E}\left[[\theta_j+\sigma\xi_j^1]_T\right]\right| \geq \mathbb{E}\left[[\theta_j+\sigma\xi_j^1]_T\right] \geq \mathbb{E}\left[[a+\sigma\xi_j^1]_T\right],$$

if $\theta_j \geq a$ since $x \mapsto [x]_T$ is non-decreasing, and if $\theta_j \leq -a$ we have

$$\begin{aligned}
&\left|\mathbb{E}\left[[\theta_j+\sigma\xi_j^1]_T\right]\right| \geq -\mathbb{E}\left[[\theta_j+\sigma\xi_j^1]_T\right] \geq -\mathbb{E}\left[[-a+\sigma\xi_j^1]_T\right] \\
&= -\mathbb{E}\left[[-a-\sigma\xi_j^1]_T\right] = \mathbb{E}\left[[a+\sigma\xi_j^1]_T\right],
\end{aligned}$$

where we have used that $x \mapsto [x]_T$ is a non-decreasing and odd function and that $-\xi_j^1$ and ξ_j^1 have the same distribution. Moreover, we have seen in the proof of (3.8) that if $\xi \sim \mathcal{N}(0,1)$ then it holds

$$\mathbb{E}\left[[a+\sigma\xi]_T\right] \geq T\left[1-2\Phi\left(\frac{T-a}{\sigma}\right)\right],$$

where Φ denotes the standard Gaussian cumulative distribution function. Thus, if $a \geq T + \sigma b$ for some $b > 0$, it holds $\mathbb{E}\left[[a+\sigma\xi_j^1]_T\right] \geq C_1 T$ for all j such that $\eta_j = 1$ with $C_1 = 1 - 2\Phi(-b)$, and

$$\begin{aligned}
\tilde{T}_{2,j} &\leq \mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^n \left([\theta_j+\sigma\xi_j^i]_T - \mathbb{E}\left[[\theta_j+\sigma\xi_j^i]_T\right]\right) + \frac{2Td}{n\alpha}\sum_{i=1}^n W_j^i\right| > C_1T-\tau\right) \\
&\leq \mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^n \left([\theta_j+\sigma\xi_j^i]_T - \mathbb{E}\left[[\theta_j+\sigma\xi_j^i]_T\right]\right)\right| + \left|\frac{2Td}{n\alpha}\sum_{i=1}^n W_j^i\right| > C_1T-\tau\right) \\
&\leq \mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^n \left([\theta_j+\sigma\xi_j^i]_T - \mathbb{E}\left[[\theta_j+\sigma\xi_j^i]_T\right]\right)\right| > \frac{C_1T-\tau}{2}\right) \\
&\qquad + \mathbb{P}\left(\left|\sum_{i=1}^n W_j^i\right| > \frac{n\alpha(C_1T-\tau)}{4Td}\right).
\end{aligned}$$

Using the two-sided version of the concentration inequalities that we used to bound $T_{2,j}$ in the proof of (3.8), we obtain if $C_1T \geq \tau$ and $\alpha(C_1T-\tau)/(8Td) \leq 1$

$$\tilde{T}_{2,j} \leq 2\left[\exp\left(-\frac{n(C_1T-\tau)^2}{2^3\min\{T^2,\sigma^2\}}\right) + \exp\left(-\frac{(C_1T-\tau)^2 n\alpha^2}{2^7T^2d^2}\right)\right].$$

This ends the proof of (3.9).

3.5.5 Proof of Corollary 3.2.5

Let prove (3.10). Note that if the assumptions of corollary 3.2.5 are satisfied, and it $T = \sigma$ and $\tau = C_1T/2$ then the assumptions of proposition 3.2.4 are also satisfied and for all

$a \geq 2\sigma$ we have

$$\begin{aligned}\sup_{\theta\in\Theta}\mathbb{E}\left[\frac{1}{s}|\hat{\eta}^+ - \eta|\right] &\leq 2\cdot\frac{d}{s}\left[\exp\left(-\frac{C_1^2 n}{2^5}\right) + \exp\left(-\frac{C_1^2 n\alpha^2}{2^9 d^2}\right)\right] \\ &= 2\left\{\exp\left(\log\left(\frac{d}{s}\right) - \frac{C_1^2 n}{2^5}\right) + \exp\left(\log\left(\frac{d}{s}\right) - \frac{C_1^2 n\alpha^2}{2^9 d^2}\right)\right\} \\ &= 2\left\{\exp\left(-\frac{n\alpha^2}{d^2}\left[\frac{C_1^2 d^2}{2^5\alpha^2} - \frac{\log(d/s)}{n\alpha^2/d^2}\right]\right) + \exp\left(-\frac{n\alpha^2}{d^2}\left[\frac{C_1^2}{2^9} - \frac{\log(d/s)}{n\alpha^2/d^2}\right]\right)\right\}.\end{aligned}$$

The two terms appearing in the last inequality both tend to 0 as $d \to +\infty$ under the assumptions of Corollary 3.2.5, which gives (3.10). The proof of (3.11) is similar.

3.5.6 Proof of Proposition 3.2.6

The beginning of the proof is similar to the proof of Proposition 3.2.4. It holds

$$\begin{aligned}\mathbb{E}\left[\frac{1}{s}|\hat{\eta}^+ - \eta|\right] = \frac{1}{s}\sum_{j:\eta_j=0}\underbrace{\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^n[\sigma\xi_j^i]_T + \frac{2Td}{n\alpha}\sum_{i=1}^n W_j^i \geq \tau\right)}_{=T_{1,j}} \\ + \frac{1}{s}\sum_{j:\eta_j=1}\underbrace{\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^n[\theta_j + \sigma\xi_j^i]_T + \frac{2Td}{n\alpha}\sum_{i=1}^n W_j^i < \tau\right)}_{=T_{2,j}},\end{aligned}$$

and we have

$$T_{1,j} \leq \exp\left(-\frac{n\tau^2}{2^3\min\{T^2,\sigma^2\}}\right) + \exp\left(-\frac{\tau^2 n\alpha^2}{2^7 T^2 d^2}\right)$$

if $\tau\alpha/(8Td) < 1$, and

$$T_{2,j} \leq \mathbb{P}\left(-\frac{1}{n}\sum_{i=1}^n\left([a+\sigma\xi_j^i]_T - \mathbb{E}\left[[a+\sigma\xi_j^i]_T\right]\right) - \frac{2Td}{n\alpha}\sum_{i=1}^n W_j^i > \mathbb{E}\left[[a+\sigma\xi_j^1]_T\right] - \tau\right).$$

Now, we bound from below $\mathbb{E}\left[[a+\sigma\xi]_T\right]$ in a different way than in the proof of Proposition 3.2.4.

$$\begin{aligned}
\mathbb{E}\left[[a+\sigma\xi]_T\right] &= T\mathbb{P}\left(\xi > \frac{T-a}{\sigma}\right) - T\mathbb{P}\left(\xi < \frac{-T-a}{\sigma}\right) + \mathbb{E}\left[(a+\sigma\xi)I(|a+\sigma\xi| \le T)\right] \\
&= T\mathbb{P}\left(\xi > \frac{T-a}{\sigma}\right) - T\mathbb{P}\left(\xi < \frac{-T-a}{\sigma}\right) + \int_{\frac{-T-a}{\sigma}}^{\frac{T-a}{\sigma}} (a+\sigma x)\frac{1}{\sqrt{2\pi}} e^{-x^2/2}\mathrm{d}x \\
&= T\mathbb{P}\left(\xi > \frac{T-a}{\sigma}\right) - T\mathbb{P}\left(\xi < \frac{-T-a}{\sigma}\right) + a\mathbb{P}\left(\frac{-T-a}{\sigma} \le \xi \le \frac{T-a}{\sigma}\right) \\
&\qquad + \frac{\sigma}{\sqrt{2\pi}}\left[\exp\left(-\frac{(T+a)^2}{2\sigma^2}\right) - \exp\left(-\frac{(T-a)^2}{2\sigma^2}\right)\right] \\
&\ge a\mathbb{P}\left(\frac{-T-a}{\sigma} \le \xi \le \frac{T-a}{\sigma}\right) - \frac{\sigma}{\sqrt{2\pi}}\exp\left(-\frac{(T-a)^2}{2\sigma^2}\right) \\
&\ge a\mathbb{P}\left(\frac{-T+a}{\sigma} \le \xi \le \frac{T-a}{\sigma}\right) - \frac{\sigma}{\sqrt{2\pi}}\exp\left(-\frac{(T-a)^2}{2\sigma^2}\right) \\
&= a\left[1 - 2\mathbb{P}\left(\xi \ge \frac{T-a}{\sigma}\right)\right] - \frac{\sigma}{\sqrt{2\pi}}\exp\left(-\frac{(T-a)^2}{2\sigma^2}\right).
\end{aligned}$$

If $T \ge a + \sqrt{2}\sigma$, then

$$2\mathbb{P}\left(\xi \ge \frac{T-a}{\sigma}\right) \le \frac{2}{\sqrt{2\pi}} \frac{\exp\left(-\frac{(T-a)^2}{2\sigma^2}\right)}{\frac{T-a}{\sigma}} = \frac{1}{\sqrt{\pi}} \frac{\exp\left(-\left(\frac{T-a}{\sqrt{2}\sigma}\right)^2\right)}{\frac{T-a}{\sqrt{2}\sigma}} \le \frac{1}{4}.$$

If $T \ge a + \sigma\sqrt{2\log(\delta)}$ with $\delta \ge \frac{4\sigma}{a\sqrt{2\pi}}$, then

$$\frac{\sigma}{\sqrt{2\pi}}\exp\left(-\frac{(T-a)^2}{2\sigma^2}\right) \le \frac{\sigma}{\sqrt{2\pi\delta}} \le \frac{a}{4}.$$

Thus, if $T \ge a + \sigma\sqrt{2\log\left(\max\left\{e, \frac{4\sigma}{a\sqrt{2\pi}}\right\}\right)}$, then $\mathbb{E}\left[[a+\sigma\xi]_T\right] \ge a/2$, and

$$\begin{aligned}
T_{2,j} &\le \mathbb{P}\left(-\frac{1}{n}\sum_{i=1}^{n}\left([a+\sigma\xi_j^i]_T - \mathbb{E}\left[[a+\sigma\xi_j^i]_T\right]\right) - \frac{2Td}{n\alpha}\sum_{i=1}^{n} W_j^i > \frac{a}{2} - \tau\right) \\
&\le \mathbb{P}\left(-\frac{1}{n}\sum_{i=1}^{n}\left([a+\sigma\xi_j^i]_T - \mathbb{E}\left[[a+\sigma\xi_j^i]_T\right]\right) > \frac{a/2-\tau}{2}\right) \\
&\qquad + \mathbb{P}\left(\sum_{i=1}^{n}\left(-W_j^i\right) > \frac{n\alpha(a/2-\tau)}{4Td}\right).
\end{aligned}$$

We can now bound from above the first term using lemma 3.5.4 and the second term using Bernstein's inequality. This gives, if $T \geq a + \sqrt{2\log\left(\max\left\{e, \frac{4\sigma}{a\sqrt{2\pi}}\right\}\right)}$, $\tau \leq a/2$ and $\alpha(a/2-\tau)/(8Td) \leq 1$

$$T_{2,j} \leq \exp\left(-\frac{n(a/2-\tau)^2}{2^3\min\{T^2,\sigma^2\}}\right) + \exp\left(-\frac{(a/2-\tau)^2 n\alpha^2}{2^7 T^2 d^2}\right).$$

3.5.7 Proof of Corollary 3.2.7

Let prove (3.12). The chosen values of T and τ satisfy the assumptions of Proposition 3.2.6 for d large enough and yield

$$\begin{aligned}\sup_{\theta\in\Theta_d^+(s,a)} \mathbb{E}\left[\frac{1}{s}|\hat{\eta}^+ - \eta|\right] &\leq \frac{d}{s}\left[\exp\left(-\frac{na^2}{2^7\min\{T^2,\sigma^2\}}\right) + \exp\left(-\frac{a^2 n\alpha^2}{2^{11}T^2d^2}\right)\right] \\ &= \exp\left(\log\left(\frac{d}{s}\right) - \frac{na^2}{2^7\sigma^2}\right) + \exp\left(\log\left(\frac{d}{s}\right) - \frac{a^2n\alpha^2}{2^{11}T^2d^2}\right) \\ &\leq 2\exp\left(\log\left(\frac{d}{s}\right) - \frac{a^2n\alpha^2}{2^{11}T^2d^2}\right).\end{aligned}$$

Conclude using $T = a + \sigma\sqrt{2\log\left(\frac{\sqrt{n}\alpha}{d}\right)} \leq 2\sigma + \sigma\sqrt{\log\left(\frac{n\alpha^2}{d^2}\right)} \leq 2\sigma\sqrt{\log\left(\frac{n\alpha^2}{d^2}\right)}$. The proof of (3.13) is similar.

3.6 Appendix : Proofs of Section 3.3

3.6.1 Proof of Proposition 3.3.1

Note that it is sufficient to prove that $\tilde{Z}^i$ is an α-LDP view of X^i. Indeed, if $\tilde{Z}^i$ is an α-LDP view of X^i then it holds for all $z \in \mathcal{Z}$ and $x, x' \in \mathbb{R}^d$ (we omit the superscript i)

$$\begin{aligned}\frac{\mathbb{P}\left(Z=z \mid X=x\right)}{\mathbb{P}\left(Z=z \mid X=x'\right)} &= \frac{\sum_{\tilde{z}\in\{-B,B\}^d}\mathbb{P}\left(Z=z \mid \tilde{Z}=\tilde{z}, X=x\right)\mathbb{P}\left(\tilde{Z}=\tilde{z} \mid X=x\right)}{\sum_{\tilde{z}\in\{-B,B\}^d}\mathbb{P}\left(Z=z \mid \tilde{Z}=\tilde{z}, X=x'\right)\mathbb{P}\left(\tilde{Z}=\tilde{z} \mid X=x'\right)} \\ &= \frac{\sum_{\tilde{z}\in\{-B,B\}^d}\mathbb{P}\left(Z=z \mid \tilde{Z}=\tilde{z}\right)\mathbb{P}\left(\tilde{Z}=\tilde{z} \mid X=x\right)}{\sum_{\tilde{z}\in\{-B,B\}^d}\mathbb{P}\left(Z=z \mid \tilde{Z}=\tilde{z}\right)\mathbb{P}\left(\tilde{Z}=\tilde{z} \mid X=x'\right)} \\ &\leq e^{\alpha},\end{aligned}$$

where we have used that Z is independent from X conditionally to $\tilde{Z}$ and the fact that $\mathbb{P}\left(\tilde{Z}=\tilde{z} \mid X=x\right) \leq e^{\alpha}\mathbb{P}\left(\tilde{Z}=\tilde{z} \mid X=x'\right)$ for all $\tilde{z} \in \{-B,B\}^d$ if $\tilde{Z}$ is an α-LDP view of X. So, let's prove that $\tilde{Z}^i$ is an α-LDP view of X^i. In what follows, we omit once again the superscript i. We have to prove that for all $\tilde{z} \in \{-B,B\}^d$ and all $x, x' \in \mathbb{R}^d$ it holds

$$\frac{\mathbb{P}\left(\tilde{Z}=\tilde{z} \mid X=x\right)}{\mathbb{P}\left(\tilde{Z}=\tilde{z} \mid X=x'\right)} \leq e^{\alpha}.$$

Let $\tilde{z} \in \{-B,B\}^d$ and $x \in \mathbb{R}^d$. It holds

$$\begin{aligned}\mathbb{P}\left(\tilde{Z}=\tilde{z} \mid X=x\right) &= \sum_{\tilde{x}\in\{-T,T\}^d} \mathbb{P}\left(\tilde{Z}=\tilde{z} \mid X=x, \tilde{X}=\tilde{x}\right)\cdot\mathbb{P}\left(\tilde{X}=\tilde{x} \mid X=x\right)\\ &= \sum_{\tilde{x}\in\{-T,T\}^d} \mathbb{P}\left(\tilde{Z}=\tilde{z} \mid \tilde{X}=\tilde{x}\right)\cdot\mathbb{P}\left(\tilde{X}=\tilde{x} \mid X=x\right),\end{aligned}$$

and since Y and $\tilde{X}$ are independent we have

$$\begin{aligned}\mathbb{P}\left(\tilde{Z}=\tilde{z} \mid \tilde{X}=\tilde{x}\right) &= \mathbb{P}\left(\tilde{Z}=\tilde{z} \mid \tilde{X}=\tilde{x}, Y=1\right)\cdot\mathbb{P}\left(Y=1\right)\\ &\quad+\mathbb{P}\left(\tilde{Z}=\tilde{z} \mid \tilde{X}=\tilde{x}, Y=0\right)\cdot\mathbb{P}\left(Y=0\right)\\ &= \pi_\alpha\mathbb{P}\left(\tilde{Z}=\tilde{z} \mid \tilde{X}=\tilde{x}, Y=1\right)+(1-\pi_\alpha)\mathbb{P}\left(\tilde{Z}=\tilde{z} \mid \tilde{X}=\tilde{x}, Y=0\right).\end{aligned}$$

Moreover, since for $\tilde{x} \in \{-T,T\}^d$

$$\begin{aligned}&\mathrm{Card}\left(\left\{\tilde{z}\in\{-B,B\}^d \mid \langle\tilde{z},\tilde{x}\rangle>0 \text{ or } (\langle\tilde{z},\tilde{x}\rangle=0 \text{ and } \tilde{z}_1=(B/T)\tilde{x}_1)\right\}\right)\\ &\quad=\mathrm{Card}\left(\left\{\tilde{z}\in\{-B,B\}^d \mid \langle\tilde{z},\tilde{x}\rangle<0 \text{ or } (\langle\tilde{z},\tilde{x}\rangle=0 \text{ and } \tilde{z}_1=-(B/T)\tilde{x}_1)\right\}\right)=2^{d-1},\end{aligned}$$

it holds

$$\mathbb{P}\left(\tilde{Z}=\tilde{z} \mid \tilde{X}=\tilde{x}, Y=1\right)=\begin{cases}0 & \text{if } \langle\tilde{z},\tilde{x}\rangle<0 \text{ or } (\langle\tilde{z},\tilde{x}\rangle=0 \text{ and } \tilde{z}_1=-(B/T)\tilde{x}_1)\\ \frac{1}{2^{d-1}} & \text{if } \langle\tilde{z},\tilde{x}\rangle>0 \text{ or } (\langle\tilde{z},\tilde{x}\rangle=0 \text{ and } \tilde{z}_1=(B/T)\tilde{x}_1),\end{cases}$$

and

$$\mathbb{P}\left(\tilde{Z}=\tilde{z} \mid \tilde{X}=\tilde{x}, Y=0\right)=\begin{cases}\frac{1}{2^{d-1}} & \text{if } \langle\tilde{z},\tilde{x}\rangle<0 \text{ or } (\langle\tilde{z},\tilde{x}\rangle=0 \text{ and } \tilde{z}_1=-(B/T)\tilde{x}_1)\\ 0 & \text{if } \langle\tilde{z},\tilde{x}\rangle>0 \text{ or } (\langle\tilde{z},\tilde{x}\rangle=0 \text{ and } \tilde{z}_1=(B/T)\tilde{x}_1).\end{cases}$$

We thus have

$$\mathbb{P}\left(\tilde{Z}=\tilde{z}\mid\tilde{X}=\tilde{x}\right)=\begin{cases}\frac{1-\pi_\alpha}{2^{d-1}} & \text{if } \langle\tilde{z},\tilde{x}\rangle<0 \text{ or } \left(\langle\tilde{z},\tilde{x}\rangle=0 \text{ and } \tilde{z}_1=-(B/T)\tilde{x}_1\right)\\ \frac{\pi_\alpha}{2^{d-1}} & \text{if } \langle\tilde{z},\tilde{x}\rangle>0 \text{ or } \left(\langle\tilde{z},\tilde{x}\rangle=0 \text{ and } \tilde{z}_1=(B/T)\tilde{x}_1\right),\end{cases}$$

and, if we set

$$A_{\tilde{z}}=\left\{\tilde{x}\in\{-T,T\}^d:\langle\tilde{z},\tilde{x}\rangle>0 \text{ or } \left(\langle\tilde{z},\tilde{x}\rangle=0 \text{ and } \tilde{z}_1=(B/T)\tilde{x}_1\right)\right\}$$

and

$$C_{\tilde{z}}=\left\{\tilde{x}\in\{-T,T\}^d:\langle\tilde{z},\tilde{x}\rangle<0 \text{ or } \left(\langle\tilde{z},\tilde{x}\rangle=0 \text{ and } \tilde{z}_1=-(B/T)\tilde{x}_1\right)\right\},$$

we obtain

$$\mathbb{P}\left(\tilde{Z}=\tilde{z}\mid X=x\right)=\frac{\pi_\alpha}{2^{d-1}}\sum_{\tilde{x}\in A_{\tilde{z}}}\mathbb{P}\left(\tilde{X}=\tilde{x}\mid X=x\right)+\frac{1-\pi_\alpha}{2^{d-1}}\sum_{\tilde{x}\in C_{\tilde{z}}}\mathbb{P}\left(\tilde{X}=\tilde{x}\mid X=x\right).$$

Consequently, it holds for all $\tilde{z}\in\{-B,B\}^d$ and all $x\in\mathbb{R}^d$,

$$\frac{\min\{\pi_\alpha,1-\pi_\alpha\}}{2^{d-1}}\le\mathbb{P}\left(\tilde{Z}=\tilde{z}\mid X=x\right)\le\frac{\max\{\pi_\alpha,1-\pi_\alpha\}}{2^{d-1}},$$

where we have used that $A_{\tilde{z}}\sqcup C_{\tilde{z}}=\{-T,T\}^d$ and $\sum_{\tilde{x}\in\{-T,T\}^d}\mathbb{P}\left(\tilde{X}=\tilde{x}\mid X=x\right)=1$. We finally obtain for all $\tilde{z}\in\{-B,B\}^d$ and all $x,x'\in\mathbb{R}^d$,

$$\frac{\mathbb{P}\left(\tilde{Z}=\tilde{z}\mid X=x\right)}{\mathbb{P}\left(\tilde{Z}=\tilde{z}\mid X=x'\right)}\le\frac{\max\{\pi_\alpha,1-\pi_\alpha\}}{\min\{\pi_\alpha,1-\pi_\alpha\}}=\frac{\pi_\alpha}{1-\pi_\alpha}=e^\alpha.$$

3.6.2 Proof of Proposition 3.3.2

Let $x\in\mathbb{R}^d$. We first compute $\mathbb{E}\left[\tilde{Z}\mid X=x\right]$. It holds

$$\begin{aligned}\mathbb{E}\left[\tilde{Z}\mid X=x\right]&=\sum_{\tilde{x}\in\{-T,T\}^d}\mathbb{P}\left(\tilde{X}=\tilde{x}\mid X=x\right)\cdot\mathbb{E}\left[\tilde{Z}\mid X=x,\tilde{X}=\tilde{x}\right]\\&=\sum_{\tilde{x}\in\{-T,T\}^d}\mathbb{P}\left(\tilde{X}=\tilde{x}\mid X=x\right)\cdot\mathbb{E}\left[\tilde{Z}\mid\tilde{X}=\tilde{x}\right],\end{aligned}$$

and since Y and $\tilde{X}$ are independent we have

$$\begin{aligned}\mathbb{E}\left[\tilde{Z} \mid \tilde{X}=\tilde{x}\right] &= \mathbb{P}\left(Y=1\right)\cdot\mathbb{E}\left[\tilde{Z} \mid \tilde{X}=\tilde{x}, Y=1\right] + \mathbb{P}\left(Y=0\right)\cdot\mathbb{E}\left[\tilde{Z} \mid \tilde{X}=\tilde{x}, Y=0\right] \\ &= \pi_\alpha \mathbb{E}\left[\tilde{Z} \mid \tilde{X}=\tilde{x}, Y=1\right] + (1-\pi_\alpha)\mathbb{E}\left[\tilde{Z}=z \mid \tilde{X}=\tilde{x}, Y=0\right].\end{aligned}$$

Define

$$\begin{aligned}A_{\tilde{x}} &:= \left\{\tilde{z}\in\{-B,B\}^d \mid \langle\tilde{z},\tilde{x}\rangle > 0 \text{ or } \left(\langle\tilde{z},\tilde{x}\rangle = 0 \text{ and } \tilde{z}_1 = (B/T)\tilde{x}_1\right)\right\}, \\ C_{\tilde{x}} &:= \left\{\tilde{z}\in\{-B,B\}^d \mid \langle\tilde{z},\tilde{x}\rangle < 0 \text{ or } \left(\langle\tilde{z},\tilde{x}\rangle = 0 \text{ and } \tilde{z}_1 = -(B/T)\tilde{x}_1\right)\right\}.\end{aligned}$$

Conditionnally on $\left\{\tilde{X}=\tilde{x}, Y=1\right\}$, it holds $Z\sim\mathcal{U}\left(A_{\tilde{x}}\right)$. Thus,

$$\mathbb{E}\left[\tilde{Z} \mid \tilde{X}=\tilde{x}, Y=1\right] = \sum_{\tilde{z}\in A_{\tilde{x}}} \mathbb{P}\left(\tilde{Z}=\tilde{z} \mid \tilde{X}=\tilde{x}, Y=1\right)\tilde{z} = \frac{1}{\mathrm{Card}(A_{\tilde{x}})}\sum_{\tilde{z}\in A_{\tilde{x}}}\tilde{z}.$$

Similarly,

$$\begin{aligned}\mathbb{E}\left[\tilde{Z} \mid \tilde{X}=\tilde{x}, Y=0\right] &= \frac{1}{\mathrm{Card}(C_{\tilde{x}})}\sum_{\tilde{z}\in C_{\tilde{x}}}\tilde{z} = \frac{1}{\mathrm{Card}(C_{\tilde{x}})}\sum_{\tilde{z}\in A_{\tilde{x}}}(-\tilde{z}) \\ &= -\mathbb{E}\left[\tilde{Z} \mid \tilde{X}=\tilde{x}, Y=1\right],\end{aligned}$$

where we have used $\mathrm{Card}(C_{\tilde{x}}) = \mathrm{Card}(A_{\tilde{x}})$. We thus obtain

$$\mathbb{E}\left[\tilde{Z} \mid \tilde{X}=\tilde{x}\right] = \frac{2\pi_\alpha - 1}{\mathrm{Card}(A_{\tilde{x}})}\sum_{\tilde{z}\in A_{\tilde{x}}}\tilde{z},$$

and, using that $\mathrm{Card}(A_{\tilde{x}}) = 2^{d-1}$ for all $\tilde{x}\in\{-T,T\}^d$ we obtain

$$\mathbb{E}\left[\tilde{Z} \mid X=x\right] = \frac{2\pi_\alpha - 1}{2^{d-1}}\sum_{\tilde{x}\in\{-T,T\}^d}\left[\mathbb{P}\left(\tilde{X}=\tilde{x} \mid X=x\right)\cdot\sum_{\tilde{z}\in A_{\tilde{x}}}\tilde{z}\right].$$

We now compute $\sum_{\tilde{z}\in A_{\tilde{x}}}\tilde{z}$ for all $\tilde{x}\in\{-T,T\}^d$. Note that for $\tilde{z}\in\{-B,B\}^d$ and $\tilde{x}\in\{-T,T\}^d$, $\langle\tilde{z},\tilde{x}\rangle$ is a sum of d terms, each equal to $-BT$ or BT. If a denotes the number of elements of this sum equal to BT and b denotes the number of elements of this sum equal to $-BT$, then it holds $a+b=d$ and $\langle\tilde{z},\tilde{x}\rangle = aBT - bBT = BT(d-2b)$. Thus we can only have $\langle\tilde{z},\tilde{x}\rangle = kBT$, with $k\in[\![-d,d]\!]$ and $|k|$ has the same parity as d. We thus

have

$$\sum_{\tilde{z}\in A_{\tilde{x}}} \tilde{z} = \sum_{p=0}^{(d-1)/2} \sum_{\{\tilde{z}\in\{-B,B\}^d : \langle \tilde{z},\tilde{x}\rangle = (2p+1)BT\}} z, \tag{3.20}$$

if d is odd, and

$$\sum_{\tilde{z}\in A_{\tilde{x}}} \tilde{z} = \sum_{p=1}^{d/2} \sum_{\substack{\tilde{z}\in\{-B,B\}^d : \\ \langle \tilde{z},\tilde{x}\rangle = 2p\cdot BT}} \tilde{z} + \sum_{\substack{\tilde{z}\in\{-B,B\}^d : \\ \langle \tilde{z},\tilde{x}\rangle = 0 \\ \tilde{z}_1 = \frac{B}{T}\tilde{x}_1}} \tilde{z}, \tag{3.21}$$

if d is even. Now, observe that for all $\tilde{x} \in \{-T,T\}^d$, for all $j \in [\![1,d]\!]$ and for all $k \in \{0,\dots,d\}$ with the same parity as d, it holds

$$\sum_{\substack{\tilde{z}\in\{-B,B\}^d : \\ \langle \tilde{z},\tilde{x}\rangle = kBT}} \tilde{z}_j = \frac{B}{T}\left[\binom{d-1}{\frac{d+k}{2}-1} - \binom{d-1}{\frac{d+k}{2}}\right]\tilde{x}_j. \tag{3.22}$$

Indeed, for all $\tilde{z} \in \{-B,B\}^d$, for all $\tilde{x} \in \{-T,T\}^d$, and for all $k \in \{0,\dots,d\}$ with the same parity as d, it holds

$$\langle \tilde{z},\tilde{x}\rangle = k\cdot BT \iff \begin{cases} \tilde{z}_j = \frac{B}{T}\tilde{x}_j & \text{for } \frac{d+k}{2} \text{ elements } j \in [\![1,d]\!] \\ \tilde{z}_j = -\frac{B}{T}\tilde{x}_j & \text{for } \frac{d-k}{2} \text{ elements } j \in [\![1,d]\!]. \end{cases}$$

Setting $D_{k,\tilde{x}} = \{\tilde{z} \in \{-B,B\}^d : \langle \tilde{z},\tilde{x}\rangle = k\cdot BT\}$, it thus holds

$$\begin{aligned}
\sum_{\tilde{z}\in D_{k,\tilde{x}}} \tilde{z}_j &= \sum_{\tilde{z}\in D_{k,\tilde{x}}} \frac{B}{T}\tilde{x}_j \mathbb{1}\left(\tilde{z}_j = \frac{B}{T}\tilde{x}_j\right) - \sum_{z\in D_{k,\tilde{x}}} \frac{B}{T}\tilde{x}_j \mathbb{1}\left(\tilde{z}_j = -\frac{B}{T}\tilde{x}_j\right) \\
&= \frac{B}{T}\left[\mathrm{Card}\left(\tilde{z}\in D_{k,\tilde{x}} : \tilde{z}_j = \frac{B}{T}\tilde{x}_j\right) - \mathrm{Card}\left(\tilde{z}\in D_{k,\tilde{x}} : \tilde{z}_j = -\frac{B}{T}\tilde{x}_j\right)\right]\tilde{x}_j \\
&= \frac{B}{T}\left[\binom{d-1}{\frac{d+k}{2}-1} - \binom{d-1}{\frac{d+k}{2}}\right]\tilde{x}_j.
\end{aligned}$$

We now end the proof of Proposition 3.3.2 when d is odd. Combining (3.22) with (3.20), we obtain for d odd

$$\sum_{z\in A_{\tilde{x}}} \tilde{z} = \frac{B}{T}\binom{d-1}{\frac{d-1}{2}}\tilde{x},$$

and the choice of B yields

$$\begin{aligned}\mathbb{E}\left[\tilde{Z} \mid X = x\right] &= \frac{2\pi_\alpha - 1}{2^{d-1}} \frac{B}{T} \binom{d-1}{\frac{d-1}{2}} \sum_{\tilde{x} \in \{-T,T\}^d} \mathbb{P}\left(\tilde{X} = \tilde{x} \mid X = x\right) \cdot \tilde{x} \\ &= \mathbb{E}\left[\tilde{X} \mid X = x\right]\end{aligned}$$

Since for all $j \in [\![1, d]\!]$ it holds

$$\mathbb{E}\left[\tilde{X}_j \mid X = x\right] = T\left(\frac{1}{2} + \frac{[x_j]_T}{2T}\right) - T\left(\frac{1}{2} - \frac{[x_j]_T}{2T}\right) = [x_j]_T,$$

we obtain for d odd

$$\mathbb{E}\left[Z \mid X = x\right] = \mathbb{E}\left[\tilde{Z} \mid X = x\right] = \mathbb{E}\left[\tilde{X} \mid X = x\right] = f_T(x),$$

which proves Proposition 3.3.2 when d is odd. From now on, we assume that d is even. Combining (3.22) with (3.21), we obtain

$$\sum_{\tilde{z} \in A_{\tilde{x}}} \tilde{z} = \frac{B}{T} \binom{d-1}{\frac{d}{2}} \tilde{x} + \sum_{\substack{\tilde{z} \in \{-B,B\}^d : \\ \langle \tilde{z}, \tilde{x} \rangle = 0 \\ \tilde{z}_1 = \frac{B}{T}\tilde{x}_1}} \tilde{z}.$$

Now, observe that for $\tilde{z} \in \{-B, B\}^d$ and $\tilde{x} \in \{-T, T\}^d$ it holds $\langle \tilde{z}, \tilde{x} \rangle = 0$ if and only if $\tilde{z}_j = (B/T)\tilde{x}_j$ for exactly $d/2$ subscripts $j \in [\![1, d]\!]$ and $\tilde{z}_j = -(B/T)\tilde{x}_j$ for exactly $d/2$ subscripts $j \in [\![1, d]\!]$. We thus have

$$\begin{aligned}\sum_{\substack{\tilde{z} \in \{-B,B\}^d : \\ \langle \tilde{z}, \tilde{x} \rangle = 0 \\ \tilde{z}_1 = \frac{B}{T}\tilde{x}_1}} \tilde{z}_1 &= \frac{B}{T}\tilde{x}_1 \cdot \mathrm{Card}\left(\left\{\tilde{z} \in \{-B, B\}^d : \langle \tilde{z}, \tilde{x} \rangle = 0 \text{ and } \tilde{z}_1 = \frac{B}{T}\tilde{x}_1\right\}\right) \\ &= \frac{B}{T} \binom{d-1}{\frac{d}{2} - 1} \tilde{x}_1,\end{aligned}$$

and for $j \geq 2$ it holds

$$\sum_{\substack{\tilde{z}\in\{-B,B\}^d:\\ \langle\tilde{z},\tilde{x}\rangle=0\\ \tilde{z}_1=\frac{B}{T}\tilde{x}_1}} \tilde{z}_j = \frac{B}{T}\tilde{x}_j \left[\mathrm{Card}\left(\left\{\tilde{z}\in\{-B,B\}^d : \langle\tilde{z},\tilde{x}\rangle = 0, \tilde{z}_1 = \frac{B}{T}\tilde{x}_1, \tilde{z}_j = \frac{B}{T}\tilde{x}_j\right\}\right)\right.$$
$$\left. -\mathrm{Card}\left(\left\{\tilde{z}\in\{-B,B\}^d : \langle\tilde{z},\tilde{x}\rangle = 0, \tilde{z}_1 = \frac{B}{T}\tilde{x}_1, \tilde{z}_j = -\frac{B}{T}\tilde{x}_j\right\}\right)\right]$$
$$= \frac{B}{T}\left[\binom{d-2}{\frac{d}{2}-2} - \binom{d-2}{\frac{d}{2}-1}\right]\tilde{x}_j.$$

We thus obtain

$$\sum_{\tilde{z}\in A_{\tilde{x}}} \tilde{z}_j = \begin{cases} \frac{B}{T}\binom{d}{\frac{d}{2}}\tilde{x}_1 & \text{if } j = 1 \\ \frac{B}{T}\left[\binom{d-1}{\frac{d}{2}} + \binom{d-2}{\frac{d}{2}-2} - \binom{d-2}{\frac{d}{2}-1}\right]\tilde{x}_j & \text{if } j \in [\![2,d]\!] \end{cases}.$$

The choice

$$B = \frac{2^{d-1}T}{2\pi_\alpha - 1}\cdot\frac{(\frac{d}{2}-1)!\frac{d}{2}!}{(d-2)!(d-2)}$$

then yields

$$\mathbb{E}\left[\tilde{Z}_j \mid X = x\right] = \begin{cases} \frac{(2\pi_\alpha-1)B}{2^{d-1}T}\binom{d}{\frac{d}{2}}\sum_{\tilde{x}\in\{-T,T\}^d}\tilde{x}_1\mathbb{P}\left(\tilde{X}=\tilde{x}\mid X=x\right) & \text{if } j=1 \\ \frac{(2\pi_\alpha-1)B}{2^{d-1}T}\cdot\frac{(d-2)!(d-2)}{(\frac{d}{2}-1)!\frac{d}{2}!}\sum_{\tilde{x}\in\{-T,T\}^d}\tilde{x}_j\mathbb{P}\left(\tilde{X}=\tilde{x}\mid X=x\right) & \text{if } j\in[\![2,d]\!] \end{cases}$$
$$= \begin{cases} \frac{2(d-1)}{d-2}\sum_{\tilde{x}\in\{-T,T\}^d}\tilde{x}_1\mathbb{P}\left(\tilde{X}=\tilde{x}\mid X=x\right) & \text{if } j=1 \\ \sum_{\tilde{x}\in\{-T,T\}^d}\tilde{x}_j\mathbb{P}\left(\tilde{X}=\tilde{x}\mid X=x\right) & \text{if } j\in[\![2,d]\!] \end{cases}.$$

Thus, it holds $\mathbb{E}\left[Z_j \mid X = x\right] = \sum_{\tilde{x}\in\{-T,T\}^d}\mathbb{P}\left(\tilde{X}=\tilde{x}\mid X=x\right)\tilde{x}_j$ for all $j\in[\![1,d]\!]$, and

$$\mathbb{E}[Z\mid X=x] = \sum_{\tilde{x}\in\{-T,T\}^d}\mathbb{P}\left(\tilde{X}=\tilde{x}\mid X=x\right)\tilde{x} = \mathbb{E}\left[\tilde{X}\mid X=x\right] = f_T(x).$$

3.6.3 Asymptotic analysis of the value K_d defined in (3.14)

Lemma 3.6.1. *The value K_d defined in (3.14) behaves asymptotically in d as*

$$K_d \underset{d\to\infty}{\sim} \sqrt{\frac{\pi}{2}}\sqrt{d}.$$

In particular, it holds $K_d \lesssim \sqrt{d}$ *for* d *large enough.*

The proof relies on Stirling's approximation. We first deal with the case where d is odd. In this case, Stirling's approximation yields

$$K_d = 2^{d-1}\frac{\left[\left(\frac{d-1}{2}\right)!\right]^2}{(d-1)!} \underset{d\to\infty}{\sim} 2^{d-1}\cdot\pi(d-1)\left(\frac{d-1}{2e}\right)^{d-1}\cdot\left[\sqrt{2\pi(d-1)}\left(\frac{d-1}{e}\right)^{d-1}\right]^{-1}.$$

The right-hand side of this asymptotic equivalence is equal to $\sqrt{\pi/2}\sqrt{d-1}$. We thus obtain $K_d \underset{d\to\infty}{\sim} \sqrt{\pi/2}\sqrt{d}$.

We now assume that d is even. in this case, Stirling's approximation yields

$$K_d = \frac{2^{d-1}(\frac{d}{2}-1)!\frac{d}{2}!}{(d-2)!(d-2)} \underset{d\to\infty}{\sim} \frac{2^{d-1}}{d-2}\cdot\pi\sqrt{(d-2)d}\left(\frac{d-2}{2e}\right)^{\frac{d}{2}-1}\left(\frac{d}{2e}\right)^{\frac{d}{2}}\cdot\left[\sqrt{2\pi(d-2)}\left(\frac{d-2}{e}\right)^{d-2}\right]^{-1}$$

The right-hand side of this asymptotic equivalence is equal to

$$\frac{\sqrt{\pi}}{e\sqrt{2}}\sqrt{d}(d-2)^{-\frac{d}{2}}d^{\frac{d}{2}} = \frac{\sqrt{\pi}}{e\sqrt{2}}\sqrt{d}\exp\left(-\frac{d}{2}\log\left(1-\frac{2}{d}\right)\right) \underset{d\to\infty}{\sim} \sqrt{\frac{\pi}{2}}\sqrt{d},$$

which ends the proof.

3.6.4 Proof of Proposition 3.3.3

The proof is similar to the one we made in the Coordinate Local case (Proposition 3.2.4). However, in the Coordinate Global case, for all $j \in [\![1,d]\!]$ the $(Z_j^i)_i$ are bounded random variables, which will enable us to use Hoeffding's inequality instead of Lemma 3.5.4 and Bernstein's inequality.

Writting

$$|\hat{\eta}^+ - \eta| = \sum_{j:\eta_j=0}\hat{\eta}_j^+ + \sum_{j:\eta_j=1}(1-\hat{\eta}_j^+),$$

we have

$$\mathbb{E}\left[\frac{1}{s}|\hat{\eta}^+ - \eta|\right] = \frac{1}{s}\sum_{j:\eta_j=0}\underbrace{\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^n Z_j^i \geq \tau\right)}_{=T_{1,j}} + \frac{1}{s}\sum_{j:\eta_j=1}\underbrace{\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^n Z_j^i < \tau\right)}_{=T_{2,j}}.$$

We first study $T_{1,j}$. For j satisfying $\eta_j = 0$, it holds

$$\mathbb{E}\left[Z_j^i\right] = \mathbb{E}\left[\mathbb{E}\left[Z_j^i \mid X^i\right]\right] = \mathbb{E}\left[[X_j^i]_T\right] = \mathbb{E}\left[[\sigma\xi_j^i]_T\right] = 0,$$

where we have used Proposition 3.3.2. Thus, Hoeffding's inequality yields

$$T_{1,j} = \mathbb{P}\left(\sum_{i=1}^n (Z_j^i - \mathbb{E}[Z_j^i]) \geq n\tau\right) \leq \exp\left(-\frac{n\tau^2}{2B^2}\right).$$

We now study $T_{2,j}$. Let $j \in [\![1, d]\!]$ such that $\eta_j = 1$. It holds

$$\begin{aligned} T_{2,j} &= \mathbb{P}\left(\frac{1}{n}\sum_{i=1}^n \left(Z_j^i - \mathbb{E}\left[Z_j^i\right]\right) + \frac{1}{n}\sum_{i=1}^n \mathbb{E}\left[Z_j^i\right] < \tau\right) \\ &= \mathbb{P}\left(\frac{1}{n}\sum_{i=1}^n \left(-Z_j^i - \mathbb{E}\left[-Z_j^i\right]\right) > \mathbb{E}\left[Z_j^1\right] - \tau\right). \end{aligned}$$

Proposition 3.3.2 gives

$$\mathbb{E}\left[Z_j^1\right] = \mathbb{E}\left[[X_j^1]_T\right] = \mathbb{E}\left[[\theta_j + \sigma\xi_j^1]_T\right] \geq \mathbb{E}\left[[a + \sigma\xi_j^1]_T\right],$$

and we have proved in Appendix 3.5.4 that if $\xi \sim \mathcal{N}(0,1)$ then it holds

$$\mathbb{E}\left[[a + \sigma\xi]_T\right] \geq T\left[1 - 2\Phi\left(\frac{T-a}{\sigma}\right)\right],$$

where Φ denotes the standard Gaussian cumulative distribution function. Thus, if $a \geq T + \sigma b$ for some $b > 0$, it holds $\mathbb{E}\left[[a + \sigma\xi_j^{(1)}]_T\right] \geq C_1 T$ with $C_1 = 1 - 2\Phi(-b)$, and

$$\begin{aligned} T_{2,j} &\leq \mathbb{P}\left(\frac{1}{n}\sum_{i=1}^n \left(-Z_j^i - \mathbb{E}\left[-Z_j^i\right]\right) > C_1 T - \tau\right) \\ &\leq \exp\left(-\frac{n(C_1 T - \tau)^2}{2B^2}\right) \end{aligned}$$

according to Hoeffding's inequality if $C_1 T - \tau > 0$. This yields

$$\mathbb{E}\left[\frac{1}{s}|\hat{\eta}^+ - \eta|\right] \leq \frac{d - |S|}{s}\exp\left(-\frac{n\tau^2}{2B^2}\right) + \frac{|S|}{s}\exp\left(-\frac{n(C_1 T - \tau)^2}{2B^2}\right).$$

The proof of the second statement of Proposition 3.3.3 is straightforward.

3.6.5 Proof of Proposition 3.3.4

The beginning of the proof is similar to the proof of Proposition 3.3.3. It holds

$$\mathbb{E}\left[\frac{1}{s}|\hat{\eta}^+ - \eta|\right] = \frac{1}{s}\sum_{j:\eta_j=0}\underbrace{\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^n Z_j^i \geq \tau\right)}_{=T_{1,j}} + \frac{1}{s}\sum_{j:\eta_j=1}\underbrace{\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^n Z_j^i < \tau\right)}_{=T_{2,j}},$$

with

$$T_{1,j} \leq \exp\left(-\frac{n\tau^2}{2B^2}\right),$$

and

$$T_{2,j} \leq \mathbb{P}\left(\frac{1}{n}\sum_{i=1}^n\left(-Z_j^i - \mathbb{E}\left[-Z_j^i\right]\right) > \mathbb{E}\left[[a+\sigma\xi_j^i]_T\right] - \tau\right).$$

Moreover, we have proved in Appendix 3.5.6 that if $\xi \sim \mathcal{N}(0,1)$ and $T \geq a+\sigma\sqrt{2\log\left(\max\left\{e, \frac{4\sigma}{a\sqrt{2\pi}}\right\}\right)}$, then $\mathbb{E}\left[[a+\sigma\xi]_T\right] \geq a/2$. Thus, if T and τ are chosen such that $T \geq a+\sigma\sqrt{2\log\left(\max\left\{e, \frac{4\sigma}{a\sqrt{2\pi}}\right\}\right)}$, and $\tau < a/2$, Hoeffding's inequality yields

$$T_{2,j} \leq \mathbb{P}\left(\frac{1}{n}\sum_{i=1}^n\left(-Z_j^i - \mathbb{E}\left[-Z_j^i\right]\right) > \frac{a}{2} - \tau\right) \leq \exp\left(-\frac{n(a/2-\tau)^2}{2B^2}\right).$$

3.6.6 Proof of Proposition 3.3.6

For $i = 1, \ldots, d$, define the vector $\omega_i \in \{0,1\}^d$ by $\omega_{i,j} = 1$ if $j = i$, $\omega_{i,j} = 0$ if $j \neq i$ and define P_{ω_i} as the mutlivariate normal distribution $\mathcal{N}(a\omega_i, \sigma^2 I_d)$. For $i \neq j$ if holds

$$|\eta(P_{\omega_i}) - \eta(P_{\omega_j})| = |\omega_i - \omega_j| = 2.$$

The private Fano method (Proposition 2 in [30]) thus yields

$$\inf_{Q\in\mathcal{Q}_\alpha}\inf_{\hat{\eta}\in\mathcal{T}}\sup_{\theta\in\Theta_d^+(s,a)}\mathbb{E}_{Q(P_\theta^{\otimes n})}|\hat{\eta}-\eta| \geq \frac{1}{2}\left\{1 - \frac{n(e^\alpha-1)^2}{d\log(d)}\left[\sup_{\gamma\in\mathbb{B}_\infty(\mathbb{R}^d)}\sum_{i=1}^d(\varphi_{\omega_i}(\gamma))^2\right] - \frac{\log(2)}{\log(d)}\right\},$$

with

$$\mathbb{B}_\infty(\mathbb{R}^d) = \left\{\gamma \in L_\infty(\mathbb{R}^d) \mid \|\gamma\|_\infty \leq 1\right\},$$

$$\varphi_{\omega_i}(\gamma) = \int_{\mathcal{X}}\gamma(x)(dP_{\omega_i}(x) - d\bar{P}(x)) = \int_{\mathbb{R}^d}\gamma(x)(f_{\omega_i}(x) - \bar{f}(x))dx,$$

where f_{ω_i} is the density of P_{ω_i} and $\bar{f} = (1/d)\sum_{i=1}^d f_{\omega_i}$. We have

$$\begin{aligned}\sum_{i=1}^d (\varphi_{\omega_i}(\gamma))^2 &= \sum_{i=1}^d \left(\int_{\mathbb{R}^d} \gamma(x)(f_{\omega_i}(x) - \bar{f}(x))dx\right)\left(\int_{\mathbb{R}^d} \gamma(y)(f_{\omega_i}(y) - \bar{f}(y))dy\right) \\ &= \int_{\mathbb{R}^d} \gamma(x)\left[\int_{\mathbb{R}^d}\left(\sum_{i=1}^d (f_{\omega_i}(x) - \bar{f}(x))(f_{\omega_i}(y) - \bar{f}(y))\right)\gamma(y)dy\right]dx.\end{aligned}$$

Let Φ denote the density of the $\mathcal{N}(0, \sigma^2 Id)$ distribution. If $\gamma \in \mathbb{B}_\infty(\mathbb{R}^d)$ then $\gamma \in L_2(\mathbb{R}^d, d\Phi)$, $\|\gamma\|_{L_2(\mathbb{R}^d, d\Phi)} \leq 1$, and we can write

$$\begin{aligned}\sum_{i=1}^d (\varphi_{\omega_i}(\gamma))^2 &= \int_{\mathbb{R}^d} \gamma(x)\left[\int_{\mathbb{R}^d}\left(\sum_{i=1}^d \frac{f_{\omega_i}(x) - \bar{f}(x)}{\Phi(x)} \cdot \frac{f_{\omega_i}(y) - \bar{f}(y)}{\Phi(y)}\right)\gamma(y)\Phi(y)dy\right]\Phi(x)dx \\ &= \langle \gamma, K\gamma\rangle_{L_2(\mathbb{R}^d, d\Phi)},\end{aligned}$$

where

$$\begin{array}{rcccl} K & : & L_2(\mathbb{R}^d, d\Phi) & \to & L_2(\mathbb{R}^d, d\Phi) \\ & & \gamma & \mapsto & \int_{\mathbb{R}^d}\left(\sum_{i=1}^d \frac{f_{\omega_i} - \bar{f}}{\Phi}(\cdot) \cdot \frac{f_{\omega_i}(y) - \bar{f}(y)}{\Phi(y)}\right)\gamma(y)\Phi(y)dy \end{array}$$

Note that we can rewrite

$$K\gamma = \sum_{i=1}^d \left[\left\langle \frac{f_{\omega_i} - \bar{f}}{\Phi}, \gamma\right\rangle_{L_2(\mathbb{R}^d, d\Phi)} \cdot \frac{f_{\omega_i} - \bar{f}}{\Phi}\right].$$

This expression implies that K is an operator of finite rank (it is thus a compact operator), K is self-adjoint, and $\langle K\gamma, \gamma\rangle \geq 0$ for all $\gamma \in L_2(\mathbb{R}^d, d\Phi)$. In particular, the last point implies that the eigenvalues of K are non-negative. We have

$$\begin{aligned}\sup_{\gamma \in \mathbb{B}_\infty(\mathbb{R}^d)} \sum_{i=1}^d (\varphi_{\omega_i}(\gamma))^2 &\leq \sup_{\{\gamma \in L_2(\mathbb{R}^d, d\Phi) : \|\gamma\|^2_{L_2(\mathbb{R}^d, d\Phi)} \leq 1\}} \langle \gamma, K\gamma\rangle_{L_2(\mathbb{R}^d, d\Phi)} \\ &= \sup_{\{\gamma \in L_2(\mathbb{R}^d, d\Phi) : \|\gamma\|^2_{L_2(\mathbb{R}^d, d\Phi)} = 1\}} \langle \gamma, K\gamma\rangle_{L_2(\mathbb{R}^d, d\Phi)} \\ &= \sup_{\{\gamma \in L_2(\mathbb{R}^d, d\Phi) : \|\gamma\|^2_{L_2(\mathbb{R}^d, d\Phi)} = 1\}} \left|\langle \gamma, K\gamma\rangle_{L_2(\mathbb{R}^d, d\Phi)}\right| \\ &= \|K\|,\end{aligned}$$

where the last equality follows from the fact that $\left(L_2(\mathbb{R}^d, d\Phi), \langle\cdot,\cdot\rangle_{L_2(\mathbb{R}^d, d\Phi)}\right)$ is an Hilbert space and K is self-adjoint. Since K is also compact and since the eigenvalues of K are

non-negative it follows

$$\sup_{\gamma\in\mathbb{B}_\infty(\mathbb{R}^d)}\sum_{i=1}^{d}\left(\varphi_{\omega_i}(\gamma)\right)^2 \leq \|K\| = \max\{|\lambda| : \lambda \in VP(T)\} = \max\{\lambda : \lambda \in VP(T)\},$$

where $VP(T)$ is the set of all the eigenvalues of K. It remains to compute this maximum. By definition, λ is an eigenvalue of K if $\lambda I - K$ is not injective. For $\lambda \neq 0$, the Fredholm alternative for compact self-adjoint operators (see for instance [42], p.209) implies that $\lambda I - K$ is not injective if and only if $\lambda I - K$ is not surjective. Thus, the non-zero eigenvalues of K are the values of $\lambda \in \mathbb{R}^*$ such that the operator $\lambda I - K$ is not surjective. For $\lambda \in \mathbb{R}$, let A_λ be the matrix with coefficients

$$(A_\lambda)_{ij} = \left\langle \frac{f_{\omega_i} - \bar{f}}{\Phi}, \frac{f_{\omega_j} - \bar{f}}{\Phi} \right\rangle_{L_2(\mathbb{R}^d, d\Phi)} - \lambda\delta_{ij}, \quad i,j \in [\![1,d]\!],$$

where δ is the Kronecker delta. The following result proves that if λ is a non-zero eigenvalue of K then it holds $\mathrm{Det}(A_\lambda) = 0$

Lemma 3.6.2. *Let $\lambda \in \mathbb{R}$, $\lambda \neq 0$. If $\mathrm{Det}(A_\lambda) \neq 0$ then $\lambda I - K$ is surjective.*

Proof. To lighten the notations, set $\langle\cdot,\cdot\rangle_{2,\Phi} = \langle\cdot,\cdot\rangle_{L_2(\mathbb{R}^d,d\Phi)}$. Let $\lambda \in \mathbb{R}$, $\lambda \neq 0$ and assume that $\mathrm{Det}(A_\lambda) \neq 0$. We prove that for all $g \in L_2(\mathbb{R}^d, d\Phi)$ there exists $\gamma \in L_2(\mathbb{R}^d, d\Phi)$ such that $g = (\lambda I - K)\gamma$. Consider $g \in L_2(\mathbb{R}^d, d\Phi)$. Since $\mathrm{Det}(A_\lambda) \neq 0$, the matrix A_λ is invertible and for all $v \in \mathbb{R}^d$ there exists $\xi \in \mathbb{R}^d$ such that $v = A_\lambda\xi$. In particular, for

$$v = \left(\left\langle \frac{f_{\omega_1} - \bar{f}}{\Phi}, g \right\rangle_{2,\Phi}, \ldots, \left\langle \frac{f_{\omega_d} - \bar{f}}{\Phi}, g \right\rangle_{2,\Phi} \right)^T,$$

there exists $\xi \in \mathbb{R}^d$ such that $v = A_\lambda\xi$, that is

$$\left\langle \frac{f_{\omega_i} - \bar{f}}{\Phi}, g \right\rangle_{2,\Phi} = (A_\lambda\xi)_i = \sum_{j=1}^{d} \left\langle \frac{f_{\omega_i} - \bar{f}}{\Phi}, \frac{f_{\omega_j} - \bar{f}}{\Phi} \right\rangle_{2,\Phi} \xi_j - \lambda\xi_i$$

for all $i \in [\![1,d]\!]$. Define

$$\gamma = \frac{1}{\lambda}g - \frac{1}{\lambda}\sum_{j=1}^{d}\xi_j \frac{f_{\omega_j} - \bar{f}}{\Phi}.$$

We have

$$\begin{aligned}(\lambda I - K)\gamma &= \lambda\gamma - K\gamma \\ &= g - \sum_{i=1}^{d} \xi_i \frac{f_{\omega_i} - \bar{f}}{\Phi} - \sum_{i=1}^{d} \left[\left\langle \frac{f_{\omega_i} - \bar{f}}{\Phi}, \gamma \right\rangle_{L_2(\mathbb{R}^d, d\Phi)} \cdot \frac{f_{\omega_i} - \bar{f}}{\Phi} \right] \\ &= g - \sum_{i=1}^{d} \underbrace{\left[\xi_i + \frac{1}{\lambda} \left\langle \frac{f_{\omega_i} - \bar{f}}{\Phi}, g \right\rangle_{2,\Phi} - \frac{1}{\lambda} \sum_{j=1}^{d} \xi_j \left\langle \frac{f_{\omega_i} - \bar{f}}{\Phi}, \frac{f_{\omega_j} - \bar{f}}{\Phi} \right\rangle_{2,\Phi} \right]}_{=0} \frac{f_{\omega_i} - \bar{f}}{\Phi} \\ &= g,\end{aligned}$$

which concludes the proof of the Lemma. □

We now find the values of λ for which we have $\mathrm{Det}(A_\lambda) = 0$. To do so, we first make explicit the coefficients of A_λ. It holds

$$\begin{aligned}\left\langle \frac{f_{\omega_i} - \bar{f}}{\Phi}, \frac{f_{\omega_j} - \bar{f}}{\Phi} \right\rangle_{2,\Phi} &= \left\langle \frac{f_{\omega_i}}{\Phi}, \frac{f_{\omega_j}}{\Phi} \right\rangle_{2,\Phi} - \left\langle \frac{f_{\omega_i}}{\Phi}, \frac{\bar{f}}{\Phi} \right\rangle_{2,\Phi} - \left\langle \frac{\bar{f}}{\Phi}, \frac{f_{\omega_j}}{\Phi} \right\rangle_{2,\Phi} + \left\langle \frac{\bar{f}}{\Phi}, \frac{\bar{f}}{\Phi} \right\rangle_{2,\Phi} \\ &= \left\langle \frac{f_{\omega_i}}{\Phi}, \frac{f_{\omega_j}}{\Phi} \right\rangle_{2,\Phi} - \frac{1}{d} \sum_{k=1}^{d} \left\langle \frac{f_{\omega_i}}{\Phi}, \frac{f_{\omega_k}}{\Phi} \right\rangle_{2,\Phi} - \frac{1}{d} \sum_{k=1}^{d} \left\langle \frac{f_{\omega_k}}{\Phi}, \frac{f_{\omega_j}}{\Phi} \right\rangle_{2,\Phi} \\ &\qquad + \frac{1}{d^2} \sum_{k=1}^{d} \sum_{l=1}^{d} \left\langle \frac{f_{\omega_k}}{\Phi}, \frac{f_{\omega_l}}{\Phi} \right\rangle_{2,\Phi},\end{aligned}$$

and, if we denote by $\langle \cdot, \cdot \rangle_2$ the usual scalar product on $\mathbb{R}^d$, we have

$$\begin{aligned}
\left\langle \frac{f_{\omega_i}}{\Phi}, \frac{f_{\omega_j}}{\Phi} \right\rangle_{2,\Phi} &= \int_{\mathbb{R}^d} \frac{\frac{1}{(2\pi\sigma^2)^d} \exp\left(-\frac{\|x-a\omega_i\|_2^2}{2\sigma^2}\right) \exp\left(-\frac{\|x-a\omega_j\|_2^2}{2\sigma^2}\right)}{\frac{1}{(2\pi\sigma^2)^{d/2}} \exp\left(-\frac{\|x\|_2^2}{2\sigma^2}\right)} \mathrm{d}x \\
&= \frac{1}{(2\pi\sigma^2)^{d/2}} \int_{\mathbb{R}^d} \exp\left(-\frac{\|x\|_2^2 + \|a\omega_i\|_2^2 - 2\langle x, a\omega_i\rangle + \|a\omega_j\|_2^2 - 2\langle x, a\omega_j\rangle}{2\sigma^2}\right) \mathrm{d}x \\
&= \exp\left(\frac{\|a(\omega_i+\omega_j)\|_2^2 - \|a\omega_i\|_2^2 - \|a\omega_j\|_2^2}{2\sigma^2}\right) \\
&\quad \cdot \frac{1}{(2\pi\sigma^2)^{d/2}} \int_{\mathbb{R}^d} \exp\left(-\frac{\|x - a(\omega_i+\omega_j)\|_2^2}{2\sigma^2}\right) \mathrm{d}x \\
&= \exp\left(\frac{a^2\langle \omega_i, \omega_j\rangle_2}{\sigma^2}\right) \\
&= \begin{cases} \exp(a^2/\sigma^2) & \text{if } j = i \\ 1 & \text{if } j \neq i. \end{cases}
\end{aligned}$$

We thus obtain

$$\left\langle \frac{f_{\omega_i} - \bar{f}}{\Phi}, \frac{f_{\omega_j} - \bar{f}}{\Phi} \right\rangle_{2,\Phi} = \begin{cases} \left(1 - \frac{1}{d}\right)\left[\exp\left(\frac{a^2}{\sigma^2}\right) - 1\right] & \text{if } j = i \\ \frac{1}{d}\left[1 - \exp\left(\frac{a^2}{\sigma^2}\right)\right] \text{ if } j \neq i. \end{cases}$$

Write

$$C_1 = \left(1 - \frac{1}{d}\right)\left[\exp\left(\frac{a^2}{\sigma^2}\right) - 1\right],$$

and

$$C_2 = \frac{1}{d}\left[1 - \exp\left(\frac{a^2}{\sigma^2}\right)\right].$$

The matrix A_λ has its diagonal elements equal to $C_1 - \lambda$ and the other coefficients equal to C_2. Operations on the rows and columns of A_λ yield

$$\begin{aligned}
\mathrm{Det}(A_\lambda) &= (C_1 + (d-1)C_2 - \lambda)(C_1 - C_2 - \lambda)^{d-1} \\
&= -\lambda\left(\exp\left(\frac{a^2}{\sigma^2}\right) - 1 - \lambda\right)^{d-1}
\end{aligned}$$

Thus, the operator K has only one non-zero eigenvalue and it is equal to $\exp\left(\frac{a^2}{\sigma^2}\right) - 1$.

We finally obtain

$$\begin{aligned}\inf_{Q\in\mathcal{Q}_\alpha}\inf_{\hat{\eta}\in\mathcal{T}}\sup_{\theta\in\Theta_d^+(s,a)}\mathbb{E}_{Q(P_\theta^{\otimes n})}|\hat{\eta}-\eta| &\geq \frac{1}{2}\left(1-\frac{n(e^\alpha-1)^2}{d\log(d)}\left[\exp\left(\frac{a^2}{\sigma^2}\right)-1\right]-\frac{\log(2)}{\log(d)}\right)\\ &\geq \frac{1}{4}\left(1-\frac{2n(e^\alpha-1)^2}{d\log(d)}\left[\exp\left(\frac{a^2}{\sigma^2}\right)-1\right]\right),\end{aligned}$$

if $d\geq 4$.

Chapter 4

Goodness of fit testing for Hölder continuous densities under local differential privacy

Abstract: *We address the problem of goodness-of-fit testing for Hölder continuous densities under local differential privacy constraints. We study minimax separation rates when only non-interactive privacy mechanisms are allowed to be used and when both non-interactive and sequentially interactive can be used for privatisation. We propose privacy mechanisms and associated testing procedures whose analysis enables us to obtain upper bounds on the minimax rates. These results are complemented with lower bounds. By comparing these bounds, we show that the proposed privacy mechanisms and tests are optimal up to at most a logarithmic factor for several choices of f_0 including densities from uniform, normal, Beta, Cauchy, Pareto, exponential distributions. In particular, we observe that the results are deteriorated in the private setting compared to the non-private one. Moreover, we show that sequentially interactive mechanisms improve upon the results obtained when considering only non-interactive privacy mechanisms.*
Based on [25].

4.1 Introduction

Over the past few years, data privacy has become a fundamental problem in statistical data analysis. While more and more personal data are collected each day, stored and analyzed, private data analysis aims at publishing valid statistical results without compromising the privacy of the individuals whose data are analysed. Differential privacy has emerged from this line of research as a strong mathematical framework which provides rigorous privacy

guarantees.

Global differential privacy has been formalized by Dwork et al. [33]. Their definition requires a curator who gathers the confidential data of n individuals and generates a privatized output from this complete information. Only this privatized output can be released. In a nutshell, the differential privacy constraints require that altering a single entry in the original dataset does not affect the probability of a privatized output too much. One intuition behind this definition is that if the distribution of the privatized output does not depend too much on any single element of the database, then it should be difficult for an adversary to guess if one given person is in the database or not. We refer the reader to [80] for a precise definition of global differential privacy and more discussion on its testing interpretation. In this paper, we will rather focus on the stronger notion of local differential privacy for which no trusted curator is needeed. In the local setup, each individual generates a privatized version of its true data on its own machine, and only the privatized data are collected for analysis. Thus, the data-owners do not have to share their true data with anyone else. However, some interaction between the n individuals can be allowed. We will consider two specific classes of locally differentially privacy mechanisms : non-interactive and sequentially interactive privacy mechanisms, respectively. In the local non-interactive scenario, each individual generates a private view Z_i of its original data X_i on its own machine independently of all the other individuals. In the sequentially interactive scenario, the privatized data $Z_1, \ldots, Z_n$ are generated such that the i-th individual has access to the previously privatized data $Z_1, \ldots, Z_{i-1}$ in addition to the original data X_i in order to generate its own Z_i.

In this paper, we study a goodness-of-fit testing problem for densities under local differential privacy constraints. Goodness-of-fit testing problems consist in testing whether n independent and identically distributed random variables $X_1, ..., X_n$ were drawn from a specified distribution P_0 or from any other distribution P with $d(P_0, P) \geq \rho$ for some distance between distributions d and some *separation parameter* $\rho > 0$. Here, the considered distributions will be assumed to have Hölder smooth densities and we will measure the separation between distributions using the L_1 norm which corresponds (up to a constant) to the total variation distance. Moreover, only privatised data $Z_1, ..., Z_n$ are supposed available to be used in order to design testing procedures. Therefore we proceed in two steps: first randomize the original sample into a private sample, then build a test using the latter sample. Optimality is shown over all test procedures and additionally over all privacy mechanisms satisfying the privacy constraints. We adopt a minimax point of view

and aim at determining the private minimax testing radius which is the smallest separation parameter for which there exists a private testing procedure whose first type and second type error probabilities are bounded from above by a constant fixed in advance.

Contributions

Our contributions can be summarized as follows. First, when non-interactive privacy mechanisms are used, we present an α-locally differentially private such mechanism and construct a testing procedure based on the privatized data. Its analysis indicates how to tune the parameters of the test statistic and the threshold of the test procedure in order to get a least upper bound on the non interactive testing radius. This result is further complemented with a lower bound.

Next, we prove that these bounds can be improved when allowing for sequential interaction. When previously privatized random variables are publicly available, we may proceed in two steps in order to improve on the detection rates. The first part of the sample is privatized as in the non-interactive case and it is used to acquire partial information on the unknown probability density. This information is further encoded in the private versions of the second part of the sample and the whole procedure benefits and attains faster rates of detection. This idea was previously introduced in [15] and was also successful for testing discrete distributions in [10].

Finally, we investigate the optimality of our results for many choices of the null density f_0. We prove that our lower bounds and upper bounds match up to a constant in the sequentially interactive scenario, and up to a logarithmic factor in the non-interactive scenario, for several f_0 including densities from uniform, gaussian, beta, Cauchy, Pareto and exponential distributions.

Related work

Goodness-of-fit testing for separation norm $\|\cdot\|_1$ has recently received great attention in the non-private setting. Valiant and Valiant [75] studies the case of discrete distributions. Given a discrete distribution P_0 and an unknown discrete distribution P, they tackle the problem of finding how many samples from P one should obtain to be able to distinguish with high probability the case that $P = P_0$ from the case that $\|P - P_0\|_1 \geq \varepsilon$. They provide both upper bounds and lower bounds on this sample complexity as a function of ε and the null hypothesis P_0. Other testing procedures for this problem have been

proposed in [19], and [7] has revisited the problem in a minimax framework similar to the one considered in this paper (without privacy constraints). Note that before these papers, the majority of the works on this problem focused on the case where P_0 is the uniform distribution, or considered a worst-case setting. The upper and lower bounds obtained in [75] and [7] appear to match in most usual cases but do not match for some pathological distributions. This problem has been fixed in [18], where the authors provide matching upper and lower bounds on the minimax separation distance for separation norm $\|\cdot\|_t$, t in $[1, 2]$. As for the continuous case, [7] studies goodness-of-fit testing for densities with separation norm $\|\cdot\|_1$, focusing on the case of Hölder continuous densities. As it has already been observed for the discrete case, they prove that the local minimax testing radius (or minimax separation distance) strongly depends on the null distribution. We extend their results to the private setting.

Many papers have been devoted to the study of testing problems under global differential privacy constraints. This includes goodness-of-fit testing [37, 2, 4, 16, 77], independence testing [37, 77] and closeness testing [2, 4]. In the local setting of differential privacy, [44, 45, 43] study simple hypothesis testing, and [36, 65, 3] consider independence testing. Some of these references and a few others also deal with goodness-of-fit testing under local differential privacy constraints: [36] studies the asymptotic distribution of several test statistics used for fitting multinomial distributions, while [65] and [3] provide upper and lower bounds on the sample complexity for fitting more general but finitely supported discrete distributions. However, [3] considers only the case where the null distribution P_0 is the uniform distribution, and both papers prove lower bounds only with respect to the choice of the test statistic for a fixed specific privacy mechanism. In the minimax results below we prove optimality over all test statistics and also over all privacy mechanisms submitted to the local differential privacy constraints.

Minimax goodness-of-fit testing for discrete random variables has first been studied with $\mathbb{L}_2$ separation norm in [51]. They consider the non-interactive scenario exclusively, and their lower bound result is proven for the uniform distribution P_0 under the null. Lam-Weil *et al.* [51] also tackles the problem of goodness-of-fit testing for continuous random variables with $\|\cdot\|_2$ separation norm. They are the first to study minimax testing rates for the problem of goodness-of-fit testing for compactly supported densities over Besov balls $\mathcal{B}^s_{2,\infty}(L)$ in the setting of non-interactive local differential privacy. They provide an upper bound which holds for any density f_0, and a matching lower bound in the special case where f_0 is the uniform density over $[0, 1]$. In a parallel work, [15] investigates

the estimation of the integrated square of a density over general Besov classes $\mathcal{B}^s_{p,q}$, and prove that allowing for sequential interaction improves over the results obtained in the non-interactive scenario in terms of minimax estimation rates. As an application, they discuss non-interactive and sequentially interactive L_2-goodness-of-fit testing for densities supported on $[0,1]$ which lie in Besov balls. They thus extend the results obtained in [51] to more general Besov balls, to the interactive scenario, and to the case where f_0 is not assumed to be the uniform distribution, but has to be bounded from below on its support.

Later, locally differentially private goodness-of-fit testing for discrete random variables (not necessarily finite supported) has been studied in [10] in a minimax framework. The authors aim at computing the minimax testing rates when $d(P,P_0) = \sum_{j=1}^{d} |P(j) - P_0(j)|^i$, $i \in \{1,2\}$. They provide upper bounds on the minimax testing rates by constructing and analysing specific private testing procedures, complement these results with lower bounds, and investigate the optimality of their results for several choices of the null distribution P_0. Interestingly, they tackle both the sequentially interactive case and the non-interactive case and prove that the minimax testing rates are improved when sequentially interaction is allowed. Such a phenomenon appears neither for simple hypothesis testing [43], nor for many estimation problems (see for instance [30, 63, 13]).

We pursue these works by considering goodness-of-fit testing of Hölder-smooth probability densities and the separation norm $\|\cdot\|_1$. Moreover, similarly to [7], we consider densities with Hölder smoothness β in (0,1] and that can tend to 0 on their support, with possibly unbounded support. Our goal is to show how differential privacy affects the minimax separation radius for this goodness-of-fit test. Balakrishnan and Wasserman[7], following works in discrete testing initiated by [75], have shown that two procedures need to be aggregated in this case. They split the support of the density f_0 into a compact set B where f_0 is bounded from below by some positive constant and they build a weighted $\mathbb{L}_2$ test on this set; then they build a tail test on $\overline{B}$ which is based on estimates of the total probabilities $(P - P_0)(\overline{B})$. They show that the separation rates are of order

$$\left(\frac{(\int_B f_0(x)^\gamma dx)^{1/\gamma}}{n} \right)^{\frac{2\beta}{4\beta+d}}, \quad \text{where } \gamma = \frac{2\beta}{3\beta+d},$$

for $d-$dimensional observations and depend of f_0 via an integral functional. The cut-off (choice of B) will depend on n and their separation rates are not minimax optimal due to different cut-offs in the upper and lower bounds.

We show that under local differential privacy constraints, we get for an optimal choice

of B the separation rates

$$|B|^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}}$$

when only non interactive privacy mechanisms are allowed, and we show that better rates are obtained

$$|B|^{\frac{\beta+1}{2\beta+1}}(n\alpha^2)^{-\frac{2\beta}{4\beta+2}}$$

when interactive privacy mechanims are allowed (using previously published privatized information). We see that our rates only depend on f_0 in a global way through the length $|B|$ of the set B and that explains why we do not need to weight the $\mathbb{L}_2$ test statistic. Further work will include extension to more general Hölder and Besov classes with $\beta > 0$ and adaptation to the smoothness β by aggregation of an increasing number of tests as introduced by [69].

Organization of the paper

The paper is organized as follows. In Section 4.2 we introduce the notion of local differential privacy and describe the minimax framework considered in the rest of the paper. In Section 4.3 we introduce a non-interactive privacy mechanism and an associated testing procedure. Its analysis leads to an upper bound on the non-interactive testing radius which is complemented by a lower bound. In Section 4.4 we give a lower bound on the testing radius for the sequentially interactive scenario and present a sequentially interactive testing procedure which improves on the rates of the non interactive case. In Section 4.5 we prove that our results are optimal (at most up to a logarithmic factor) for several choices of the null density f_0.

4.2 Problem statement

Let $(X_1, ..., X_n) \in \mathcal{X}^n$ be i.i.d. with common probability density function (pdf) $f : \mathcal{X} \to \mathbb{R}_+$. We assume that f belongs to the smoothness class $H(\beta, L)$ for some smoothness $0 < \beta \leq 1$ and $L > 0$, where

$$H(\beta, L) = \left\{ f : \mathcal{X} \to \mathbb{R}_+ \ : \ |f(x) - f(y)| \leq L|x - y|^\beta, \quad \forall x, y \in \mathcal{X} \right\}.$$

In the sequel, we will omit the space $\mathcal{X}$ in the definition of functions f and f_0 and integrals, and we will choose a set B such that $B \subset \mathcal{X}$ and denote by $\overline{B} = \mathcal{X} \setminus B$.

Given a probability density function f_0 in $H(\beta, L_0)$ for some $L_0 < L$, we want to solve the goodness-of-fit test

$$\begin{aligned} H_0 &: f \equiv f_0 \\ H_1(\rho) &: f \in H(\beta, L) \text{ and } \|f - f_0\|_1 \geq \rho, \end{aligned}$$

where $\rho > 0$ under an α-local differential privacy constraint. We will consider two classes of locally differentially private mechanisms : sequentially interactive mechnisms and non-interactive mechanisms. In the sequentially interactive scenario, privatized data $Z_1, \ldots, Z_n$ are obtained by successively applying suitable Markov kernels : given $X_i = x_i$ and $Z_1 = z_1, \ldots, Z_{i-1} = z_{i-1}$, the i-th data-holder draws

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

for some Markov kernel $Q_i : \mathscr{Z} \times \mathcal{X} \times \mathcal{Z}^{i-1} \to [0,1]$ where the measure spaces of the non-private and private data are denoted with $(\mathcal{X}, \mathscr{X})$ and $(\mathcal{Z}, \mathscr{Z})$, respectively. We say that the sequence of Markov kernels $(Q_i)_{i=1,\ldots,n}$ provides α-local differential privacy or that $Z_1, \ldots, Z_n$ are α-local differentially private views of $X_1, \ldots, X_n$ if

$$\sup_{A \in \mathscr{Z}} \sup_{z_1, \ldots, z_{i-1} \in \mathcal{Z}} \sup_{x, x' \in \mathcal{X}} \frac{Q_i(A \mid X_i = x, Z_1 = z_1, \ldots, Z_{i-1} = z_{i-1})}{Q_i(A \mid X_i = x', Z_1 = z_1, \ldots, Z_{i-1} = z_{i-1})} \leq e^{\alpha}, \text{ for all } i = 1, \ldots, n. \tag{4.1}$$

We will denote by $\mathcal{Q}_\alpha$ the set of all α-LDP sequentially interactive mechanisms. In the non-interactive scenario Z_i depends only on X_i but not on Z_k for $k < i$. We have

$$Z_i \sim Q_i(\cdot \mid X_i = x_i),$$

and condition (4.1) becomes

$$\sup_{A \in \mathscr{Z}} \sup_{x, x' \in \mathcal{X}} \frac{Q_i(A \mid X_i = x)}{Q_i(A \mid X_i = x')} \leq e^{\alpha}, \text{ for all } i = 1, \ldots, n.$$

We will denote by $\mathcal{Q}_\alpha^{\mathrm{NI}}$ the set of all α-LDP non-interactive mechanisms. Given an α-LDP privacy mechansim Q, let $\Phi_Q = \{\phi : \mathcal{Z}^n \to \{0,1\}\}$ denote the set of all tests based on $Z_1, \ldots Z_n$.

The sequentially interactive α-LDP minimax testing risk is given by

$$\mathcal{R}_{n,\alpha}(f_0,\rho) := \inf_{Q\in\mathcal{Q}_\alpha}\inf_{\phi\in\Phi_Q}\sup_{f\in H_1(\rho)}\left\{\mathbb{P}_{Q_{f_0}^n}(\phi=1)+\mathbb{P}_{Q_f^n}(\phi=0)\right\}.$$

We define similarly the non-interactive α-LDP minimax testing risk $\mathcal{R}^{\mathrm{NI}}_{n,\alpha}(f_0,\rho)$, where the first infimum is taken over the set $\mathcal{Q}^{\mathrm{NI}}_\alpha$ instead of $\mathcal{Q}_\alpha$. Given $\gamma\in(0,1)$, we study the α-LDP minimax testing radius defined by

$$\mathcal{E}_{n,\alpha}(f_0,\gamma) := \inf\left\{\rho>0 : \mathcal{R}_{n,\alpha}(f_0,\rho)\le\gamma\right\},$$

and we define similarly $\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma)$.

4.3 Non-interactive Privacy Mechanisms

In this section we design a non-interactive α-locally differentially private mechanism and the associated testing procedure. We study successively its first and second type error probabilities in order to obtain an upper bound on the testing radius $\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma)$. We then present a lower bound on the testing radius. The test and privacy mechanism proposed in this section will turn out to be (nearly) optimal for many choices of f_0 since the lower bound and the upper bound match up to a logarithmic factor for several f_0, see Section 4.5 for many examples.

4.3.1 Upper bound in the non-interactive scenario

We propose a testing procedure that, like [7], combines an $\mathbb{L}_2$ procedure on a bulk set B where the density f_0 under the null is bounded away from 0 by some (small) constant and an $\mathbb{L}_1$ procedure on the tail $\overline{B}$. However, we note that, unlike [7], the rate depends on f_0 in a global way, only through the length $|B|$ of the set B. Our procedure also translates to the case of continuous distributions the one proposed by Berret and Butucea [10] for locally private testing of discrete distributions. It consists in the following steps:

1. Consider a compact set $B\subset\mathbb{R}$ (its choice depends on f_0, and on values of n and α).
2. Using the first half of the (privatized) data, define an estimator S_B of $\int_B(f-f_0)^2$.
3. Using the second half of the (privatized) data, define an estimator T_B of $\int_{\bar{B}}(f-f_0)$.

4. Reject H_0 if either $S_B \geq t_1$ or $T_B \geq t_2$.

Assume without loss of generality that the sample size is even and equal to $2n$ so that we can split the data into equal parts, $X_1, \ldots, X_n$ and $X_{n+1}, \ldots, X_{2n}$. Let $B \subset \mathbb{R}$ be a nonempty compact set, and let $(B_j)_{j=1,\ldots,N}$ be a partition of B, $h > 0$ be the bandwidth and $(x_1, \ldots, x_N)$ be the centering points, that is $B_j = [x_j - h, x_j + h]$ for all $j \in [\![1, N]\!]$. Let $\psi : \mathbb{R} \to \mathbb{R}$ be a function satisfying the following assumptions.

Assumption 4.3.1. ψ is a bounded function supported in $[-1, 1]$ such that

$$\int_{-1}^{1} \psi(t)\mathrm{d}t = 1, \quad \text{and} \quad \int_{-1}^{1} |t|^{\beta}|\psi(t)|\mathrm{d}t < \infty.$$

In particular, Assumption 4.3.1 implies that $\psi_h(x_j - y) = 0$ if $y \notin B_j$, where $\psi_h(u) = \frac{1}{h}\psi(\frac{u}{h})$.
We now define our first privacy mechanism. For $i \in [\![1, n]\!]$ and $j \in [\![1, N]\!]$ set

$$Z_{ij} = \frac{1}{h}\psi\left(\frac{x_j - X_i}{h}\right) + \frac{2\|\psi\|_\infty}{\alpha h} W_{ij},$$

where $(W_{ij})_{i\in[\![1,n]\!],j\in[\![1,N]\!]}$ is a sequence of i.i.d Laplace(1) random variables. Using these privatized data, we define the following U-statistic of order 2.

$$S_B := \sum_{j=1}^{N} \frac{1}{n(n-1)} \sum_{i \neq k} (Z_{ij} - f_0(x_j))(Z_{kj} - f_0(x_j)).$$

The second half of the sample is used to design a tail test. For all $i \in [\![n+1, 2n]\!]$ set

$$Z_i = \pm c_\alpha, \text{ with probabilities } \frac{1}{2}\left(1 \pm \frac{I(X_i \notin B)}{c_\alpha}\right),$$

where $c_\alpha = (e^\alpha + 1)/(e^\alpha - 1)$. Using these private data, we define the following statistic.

$$T_B = \frac{1}{n} \sum_{i=n+1}^{2n} Z_i - \int_{\overline{B}} f_0.$$

We then put

$$\Phi = \begin{cases} 1 & \text{if } S_B \geq t_1 \text{ or } T_B \geq t_2 \\ 0 & \text{otherwise} \end{cases}, \tag{4.2}$$

where

$$t_1 = \frac{3}{2}L_0^2 C_\beta^2 N h^{2\beta} + \frac{196\|\psi\|_\infty^2\sqrt{N}}{\gamma n\alpha^2 h^2}, \quad t_2 = \sqrt{\frac{20}{n\alpha^2\gamma}}, \tag{4.3}$$

with $C_\beta = \int_{-1}^{1} |u|^\beta |\psi(u)| \mathrm{d}u$. The privacy mechanism that outputs $(Z_1, \ldots, Z_n, Z_{n+1}, \ldots, Z_{2n})$ is non-interactive since for all $i \in [\![1, 2n]\!]$ Z_i depends only on X_i. The following result establishes that this mechanism also provides α-local differential privacy. Its proof is deferred to Section 4.6.1 in the Appendix.

Proposition 4.3.2. *For all $i \in [\![1, 2n]\!]$, Z_i is an α-locally differentially private view of X_i.*

The following proposition studies the properties of the test statistics. Its proof is given in the Appendix 4.6.2.

Proposition 4.3.3. *1. It holds*

$$\mathbb{E}_{Q_f^n}[S_B] = \sum_{j=1}^{N} \left([\psi_h * f](x_j) - f_0(x_j)\right)^2. \tag{4.4}$$

Under Assumption 4.3.1 it also holds if $\alpha \in (0, 1]$

$$\mathrm{Var}_{Q_f^n}(S_B) \leq \frac{36\|\psi\|_\infty^2}{n\alpha^2 h^2} \sum_{j=1}^{N} \left([\psi_h * f](x_j) - f_0(x_j)\right)^2 + \frac{164\|\psi\|_\infty^4 N}{n(n-1)\alpha^4 h^4}. \tag{4.5}$$

2. It holds

$$\mathbb{E}_{Q_f^n}[T_B] = \int_{\overline{B}} (f - f_0), \quad \textit{and} \quad \mathrm{Var}_{Q_f^n}(T_B) = \frac{1}{n}\left(c_\alpha^2 - \left(\int_{\overline{B}} f\right)^2\right).$$

The study of the first and second type error probabilities of the test Φ in (4.2) with a convenient choice of h leads to the following upper bound on $\mathcal{E}_{n,\alpha}^{\mathrm{NI}}(f_0, \gamma)$.

Theorem 4.3.4. *Assume that $\alpha \in (0, 1)$ and $\beta \leq 1$. The test procedure Φ in (4.2) with t_1 and t_2 in (4.3) and bandwidth h given by $h \asymp |B|^{-1/(4\beta+3)}(n\alpha^2)^{-2/(4\beta+3)}$ attains the following bound on the separation rate*

$$\mathcal{E}_{n,\alpha}^{NI}(f_0, \gamma) \leq C(L, \gamma, \psi) \cdot \left\{ |B|^{\frac{3\beta+3}{4\beta+3}} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}} + \int_{\overline{B}} f_0 + \frac{1}{\sqrt{n\alpha^2}} \right\},$$

for all compact set $B \subset \mathbb{R}$.

The proof can be found in Appendix 4.6.2. Note that the tightest upper bound is obtained for the sets B that minimize the right-hand sides in Theorem 4.3.4.
In order to do this, we note that the upper bounds sum a term which increases with B, a term which decreases with B: $\int_{\overline{B}} f_0$ and a term $1/\sqrt{n\alpha^2}$ free of B. Thus we suggest to choose $B = B_{n,\alpha}$ as a level set

$$B_{n,\alpha} \in \arg \inf_{B \text{ compact set}} \left\{ \int_{\overline{B}} f_0 \geq |B|^{\frac{3\beta+3}{4\beta+3}} (nz_\alpha^2)^{-\frac{2\beta}{4\beta+3}} + \frac{1}{\sqrt{n\alpha^2}} \text{ and } \inf_B f_0 \geq \sup_{\overline{B}} f_0 \right\}. \quad (4.6)$$

4.3.2 Lower bound in the non-interactive scenario

We now complete the study of the testing radius $\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0, \gamma)$ with the following lower bound.

Theorem 4.3.5. *Let $\alpha > 0$. Assume that $\beta \leq 1$. Set $z_\alpha = e^{2\alpha} - e^{-2\alpha}$. For all compact set $B \subset \mathbb{R}$ satisfying*

$$|B|^{\beta/(4\beta+3)} C_0(B) \geq C(nz_\alpha^2)^{-2\beta/(4\beta+3)} \quad (4.7)$$

for some $C > 0$ where $C_0(B) = \min\{f_0(x) : x \in B\}$, it holds

$$\mathcal{E}^{NI}_{n,\alpha}(f_0, \gamma) \geq C(\psi, b, \gamma, L, L_0) \left[\log \left(C|B|^{\frac{4\beta+4}{4\beta+3}} (nz_\alpha^2)^{\frac{2}{4\beta+3}} \right) \right]^{-1} |B|^{\frac{3\beta+3}{4\beta+3}} (nz_\alpha^2)^{-\frac{2\beta}{4\beta+3}}.$$

It is easy to see that our upper and lower bounds are optimal (when α is bounded) up to a logarithmic factor if the support $\mathcal{X}$ of f_0 is compact with $c_1 \leq |\mathcal{X}| \leq c_2$ for two constants $c_1 > 0$ and $c_2 > 0$ and if f_0 is bounded from below on $\mathcal{X}$. Indeed, for such functions, the choice $B = \mathcal{X}$ yields an upper bound of order $(n\alpha^2)^{-\frac{2\beta}{4\beta+3}}$. Moreover, (4.7) holds with this choice of B and Theorem 4.3.5 proves that the upper bound is optimal up to a logarithmic factor. In the case of densities with bounded support but which can tend to 0 on their support, and in the case of densities with unbounded support, we suggest to choose $B = B_{n,\alpha}$ as defined in (4.6) both in the upper and lower bounds. In the examples considered in Section 4.5, the choice of $B = B_{n,\alpha}$ for the upper bound also satisfies (4.7) and yields optimal bounds (up to a logarithmic factor).

Proof of Theorem 4.3.5. We use the well-known reduction technique. The idea is to build a family $\{f_\nu : \nu \in \mathcal{V}\}$ that belong to the alternative set of densities $H_1(\rho)$ and then reduce the test problem to testing between f_0 and the mixture of the f_ν. Our construction of such functions is inspired by the one proposed in [51] for goodness-of-fit testing over Besov

Balls $\mathcal{B}^s_{2,\infty}$ in the special case where f_0 is the uniform distribution over $[0,1]$, and in [15] for the minimax estimation over Besov ellipsoids $\mathcal{B}^s_{p,q}$ of the integrated square of a density supported in $[0,1]$. However, we need to make some modifications in order to consider Hölder smoothness instead of Besov smoothness and to tackle the case of densities with unbounded support.

Let $B \subset \mathbb{R}$ be a nonempty compact set, and let $(B_j)_{j=1,\dots,N}$ be a partition of B, $h>0$ be the bandwidth and $(x_1,\dots,x_N)$ be the centering points, that is $B_j = [x_j - h, x_j + h]$ for all $j \in [\![1,N]\!]$. Let $\psi : [-1,1] \to \mathbb{R}$ be such that $\psi \in H(\beta, L)$, $\int \psi = 0$ and $\int \psi^2 = 1$. For $j \in [\![1,N]\!]$, define

$$\psi_j : t \in \mathbb{R} \mapsto \frac{1}{\sqrt{h}} \psi\left(\frac{t - x_j}{h}\right).$$

Note that the support of ψ_j is B_j, $\int \psi_j = 0$ and $(\psi_j)_{j=1,\dots,N}$ is an orthonormal family.

Fix a privacy mechanism $Q = (Q_1,\dots,Q_n) \in \mathcal{Q}^{\mathrm{NI}}_\alpha$. According to lemma B.3 in [15], we can consider for every $i \in [\![1,n]\!]$ a probability measure μ_i on $\mathcal{Z}_i$ and a family of μ_i-densities $(q_i(\cdot \mid x))_{x\in\mathbb{R}}$ such that for every $x \in \mathbb{R}$ one has $dQ_i(\cdot \mid x) = q_i(\cdot \mid x) d\mu_i$ and $e^{-\alpha} \le q_i(\cdot \mid x) \le e^\alpha$. Denote by $g_{0,i}(z_i) = \int_{\mathbb{R}} q_i(z_i \mid x) f_0(x) \mathrm{d}x$ the density of Z_i when X_i has density f_0. Define for all $i = 1,\dots,n$ the operator $K_i : L_2(\mathbb{R}) \to L_2(\mathcal{Z}_i, d\mu_i)$ by

$$K_i f = \int_{\mathbb{R}} \frac{q_i(\cdot \mid x) f(x) \mathbb{1}_B(x)}{\sqrt{g_{0,i}(\cdot)}} \mathrm{d}x, \quad f \in L_2(\mathbb{R}).$$

Note that this operator is well-defined since $g_{0,i}(z_i) \ge \int_{\mathbb{R}} e^{-\alpha} f_0(x) \mathrm{d}x = e^{-\alpha} > 0$ for all z_i. Observe that its adjoint operator $K_i^\star$ is given by

$$K_i^\star : \ell \in L_2(\mathcal{Z}_i, d\mu_i) \mapsto \int_{\mathcal{Z}_i} \frac{\ell(z_i) q_i(z_i \mid \cdot) \mathbb{1}_B(\cdot)}{\sqrt{g_{0,i}(z_i)}} \mathrm{d}\mu_i(z_i).$$

Using Fubini's theorem we thus have for all $f \in L_2(\mathbb{R})$

$$\begin{aligned} K_i^\star K_i f &= \int_{\mathcal{Z}_i} \left(\int_{\mathbb{R}} \frac{q_i(z_i \mid y) f(y) \mathbb{1}_B(y)}{\sqrt{g_{0,i}(z_i)}} \mathrm{d}y \right) \frac{q_i(z_i \mid \cdot) \mathbb{1}_B(\cdot)}{\sqrt{g_{0,i}(z_i)}} \mathrm{d}\mu_i(z_i) \\ &= \int_{\mathbb{R}} \left(\int_{\mathcal{Z}_i} \frac{q_i(z_i \mid y) q_i(z_i \mid \cdot) \mathbb{1}_B(y) \mathbb{1}_B(\cdot)}{g_{0,i}(z_i)} \mathrm{d}\mu_i(z_i) \right) f(y) \mathrm{d}y, \end{aligned}$$

meaning that $K_i^\star K_i$ is an integral operator with kernel $F_i(x,y) = \int_{\mathcal{Z}_i} \frac{q_i(z_i|x) q_i(z_i|y) \mathbb{1}_B(x) \mathbb{1}_B(y)}{g_{0,i}(z_i)} \mathrm{d}\mu_i(z_i)$.

Define the operator

$$K = \frac{1}{n}\sum_{i=1}^{n} K_i^\star K_i,$$

which is symmetric and positive semidefinite. Define also

$$W_N = \text{span}\{\psi_j, j = 1, \dots, N\}.$$

Let $(v_1, \dots, v_N)$ be an orthonormal family of eigenfunctions of K as an operator on the linear $L_2(\mathbb{R})$-subspace W_N. Note that since v_k can be written as a linear combination of the ψ_j's, it holds $\int_{\mathbb{R}} v_k = 0$ and $\text{Supp}(v_k) \subset B$. We also denote by $\lambda_1^2, \dots, \lambda_N^2$ the corresponding eigenvalues. Note that they are non-negative.

Define the functions

$$f_\nu : x \in \mathbb{R} \mapsto f_0(x) + \delta \sum_{j=1}^{N} \frac{\nu_j}{\tilde{\lambda}_j} v_j(x),$$

where for $j = 1, \dots, N$ $\nu_j \in \{-1, 1\}$, $\delta > 0$ may depend on B,h, N, ψ, γ, L, L_0, β, n and α, and will be specified later, and

$$\tilde{\lambda_j} = \max\left\{\frac{\lambda_j}{z_\alpha}, \sqrt{2h}\right\}, \quad z_\alpha = e^{2\alpha} - e^{-2\alpha}.$$

The following lemma shows that for δ properly chosen, for most of the possible $\nu \in \{-1, 1\}^N$, f_ν is a density belonging to $H(\beta, L)$ and f_ν is sufficiently far away from f_0 in a L_1 sense.

Lemma 4.3.6. *Let $\mathbb{P}_\nu$ denote the uniform distribution on $\{-1, 1\}^N$. Let $b > 0$. If the parameter δ appearing in the definition of f_ν satisfies*

$$\delta \leq \frac{h}{\sqrt{\log(2N/b)}} \min\left\{\frac{C_0(B)}{\|\psi\|_\infty}, \frac{1}{2}\left(1 - \frac{L_0}{L}\right) h^\beta\right\},$$

where $C_0(B) := \min\{f_0(x) : x \in B\}$, then there exists a subset $A_b \subseteq \{-1, 1\}^N$ with $\mathbb{P}_\nu(A_b) \geq 1 - b$ such that

i) $f_\nu \geq 0$ and $\int f_\nu = 1$, for all $\nu \in A_b$,

ii) $f_\nu \in H(\beta, L)$, for all $\nu \in A_b$,

iii) $\|f_\nu - f_0\|_1 \geq \frac{3C_1}{8}\frac{\delta N}{\sqrt{\log\left(\frac{2N}{b}\right)}}$, *for all* $\nu \in A_b$, *with* $C_1 = \int_{-1}^{1}|\psi|$.

Denote by $g_{\nu,i}(z_i) = \int_{\mathbb{R}} q_i(z_i \mid x) f_\nu(x)\mathrm{d}x$ the density of Z_i when X_i has density f_ν, and

$$dQ_n(z_1,\dots,z_n) = \mathbb{E}_\nu\left[\prod_{i=1}^{n} g_{\nu,i}(z_i)\mathrm{d}\mu_i(z_i)\right].$$

If δ is chosen such that $\delta \leq \frac{h}{\sqrt{\log(2N/b)}}\min\left\{\frac{C_0(B)}{\|\psi\|_\infty}, \frac{1}{2}\left(1-\frac{L_0}{L}\right)h^\beta\right\}$, setting

$$\rho^\star = \frac{3C_1}{8}\frac{\delta N}{\sqrt{\log\left(\frac{2N}{b}\right)}},$$

we deduce from the above lemma that if

$$\mathbb{E}_{Q^n_{f_0}}\left[\left(\frac{dQ_n}{dQ^n_{f_0}}\right)^2\right] \leq 1 + (1-\gamma-b)^2 \text{ for all } Q \in \mathcal{Q}^{\mathrm{NI}}_\alpha, \tag{4.8}$$

then it holds

$$\inf_{Q\in\mathcal{Q}^{\mathrm{NI}}_\alpha}\inf_{\phi\in\Phi_Q}\sup_{f\in H_1(\rho^\star)}\left\{\mathbb{P}_{Q^n_{f_0}}(\phi=1)+\mathbb{P}_{Q^n_f}(\phi=0)\right\} \geq \gamma,$$

where $H_1(\rho^\star) := \{f \in H(\beta,L) : f \geq 0, \int f = 1, \|f-f_0\|_1 \geq \rho^\star\}$, and consequently $\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) \geq \rho^\star$. Indeed, if (4.8) holds, then we have

$$\begin{aligned}
&\inf_{Q\in\mathcal{Q}^{\mathrm{NI}}_\alpha}\inf_{\phi\in\Phi_Q}\sup_{f\in H_1(\rho^\star)}\left\{\mathbb{P}_{Q^n_{f_0}}(\phi=1)+\mathbb{P}_{Q^n_f}(\phi=0)\right\}\\
&\geq \inf_{Q\in\mathcal{Q}^{\mathrm{NI}}_\alpha}\inf_{\phi\in\Phi_Q}\left(\mathbb{P}_{Q^n_{f_0}}(\phi=1)+\sup_{\nu\in A_b}\mathbb{P}_{Q^n_{f_\nu}}(\phi=0)\right)\\
&\geq \inf_{Q\in\mathcal{Q}^{\mathrm{NI}}_\alpha}\inf_{\phi\in\Phi_Q}\left(\mathbb{P}_{Q^n_{f_0}}(\phi=1)+\mathbb{E}_\nu\left[I(\nu\in A_b)\mathbb{P}_{Q^n_{f_\nu}}(\phi=0)\right]\right),
\end{aligned}$$

and

$$\begin{aligned}
\mathbb{E}_\nu\left[I(\nu\in A_b)\mathbb{P}_{Q^n_{f_\nu}}(\phi=0)\right] &= \mathbb{P}_{Q_n}(\phi=0) - \mathbb{E}_\nu\left[I(\nu\in A_b^c)\mathbb{P}_{Q^n_{f_\nu}}(\phi=0)\right]\\
&\geq \mathbb{P}_{Q_n}(\phi=0) - \mathbb{P}_\nu(A_b^c)\\
&\geq \mathbb{P}_{Q_n}(\phi=0) - b.
\end{aligned}$$

Thus, if (4.8) holds, we have

$$\begin{aligned}
&\inf_{Q\in\mathcal{Q}_\alpha^{\mathrm{NI}}}\inf_{\phi\in\Phi_Q}\sup_{f\in H_1(\rho^\star)}\left\{\mathbb{P}_{Q_{f_0}^n}(\phi=1)+\mathbb{P}_{Q_f^n}(\phi=0)\right\}\\
&\geq \inf_{Q\in\mathcal{Q}_\alpha^{\mathrm{NI}}}\inf_{\phi\in\Phi_Q}\left(\mathbb{P}_{Q_{f_0}^n}(\phi=1)+\mathbb{P}_{Q_n}(\phi=0)-b\right)\\
&\geq \inf_{Q\in\mathcal{Q}_\alpha^{\mathrm{NI}}}\left(1-\mathrm{TV}(Q_n,Q_{f_0}^n)-b\right)\\
&= \inf_{Q\in\mathcal{Q}_\alpha^{\mathrm{NI}}}\left(1-b-\sqrt{\mathbb{E}_{Q_{f_0}^n}\left[\left(\frac{dQ_n}{dQ_{f_0}^n}\right)^2\right]-1}\right)\geq\gamma.
\end{aligned}$$

We now prove that (4.8) holds under an extra assumption on δ.

We have that

$$\begin{aligned}
&\mathbb{E}_{Q_{f_0}^n}\left[\left(\frac{dQ_n}{dQ_{f_0}^n}\right)^2\right]=\mathbb{E}_{Q_{f_0}^n}\left[\left(\frac{\mathbb{E}_\nu\left[\prod_{i=1}^n g_{\nu,i}(Z_i)\right]}{\prod_{i=1}^n g_{0,i}(Z_i)}\right)^2\right]\\
&=\mathbb{E}_{Q_{f_0}^n}\left[\mathbb{E}_{\nu,\nu'}\prod_{i=1}^n\left(1+\delta\sum_{k=1}^N\frac{\nu_k}{\tilde{\lambda}_k}\cdot\frac{\langle q_i(Z_i\mid\cdot),v_k\rangle}{g_{0,i}(Z_i)}\right)\cdot\left(1+\delta\sum_{k=1}^N\frac{\nu'_k}{\tilde{\lambda}_k}\cdot\frac{\langle q_i(Z_i\mid\cdot),v_k\rangle}{g_{0,i}(Z_i)}\right)\right]\\
&=\mathbb{E}_{\nu,\nu'}\prod_{i=1}^n\left(1+\delta\sum_{k=1}^N\frac{\nu_k}{\tilde{\lambda}_k}\mathbb{E}_{Q_{f_0}}\left[\frac{\langle q_i(Z_i\mid\cdot),v_k\rangle}{g_{0,i}(Z_i)}\right]+\delta\sum_{k=1}^N\frac{\nu'_k}{\tilde{\lambda}_k}\mathbb{E}_{Q_{f_0}}\left[\frac{\langle q_i(Z_i\mid\cdot),v_k\rangle}{g_{0,i}(Z_i)}\right]\right.\\
&\qquad\left.+\delta^2\sum_{k_1,k_2=1}^N\frac{\nu_{k_1}\nu'_{k_2}}{\tilde{\lambda}_{k_1}\tilde{\lambda}_{k_2}}\mathbb{E}_{Q_{f_0}}\left[\frac{\langle q_i(Z_i\mid\cdot),v_{k_1}\rangle\langle q_i(Z_i\mid\cdot),v_{k_2}\rangle}{(g_{0,i}(Z_i))^2}\right]\right),
\end{aligned}$$

where we have interverted $\mathbb{E}_{Q_{f_0}^n}$ and $\mathbb{E}_{\nu,\nu'}$ and used the independence of the Z_i, $i=1,\dots,n$. Now, observe that

$$\begin{aligned}
\mathbb{E}_{Q_{f_0}}\left[\frac{\langle q_i(Z_i\mid\cdot),v_k\rangle}{g_{0,i}(Z_i)}\right]&=\int_{\mathcal{Z}_i}\frac{\langle q_i(z_i\mid\cdot),v_k\rangle}{g_{0,i}(z_i)}\cdot g_{0,i}(z_i)\mathrm{d}\mu_i(z_i)\\
&=\int_{\mathcal{Z}_i}\left(\int_{\mathbb{R}}q_i(z_i\mid x)v_k(x)\mathrm{d}x\right)\mathrm{d}\mu_i(z_i)\\
&=\int_{\mathbb{R}}v_k=0,
\end{aligned}$$

and, using that $\mathrm{Supp}(v_k) \subset B$ for all k,

$$\begin{aligned}
&\mathbb{E}_{Q_{f_0}}\left[\frac{\langle q_i(Z_i \mid \cdot), v_{k_1}\rangle\langle q_i(Z_i \mid \cdot), v_{k_2}\rangle}{(g_{0,i}(Z_i))^2}\right] \\
&= \int_{\mathcal{Z}_i} \frac{\langle q_i(z_i \mid \cdot), v_{k_1}\rangle\langle q_i(z_i \mid \cdot), v_{k_2}\rangle}{(g_{0,i}(z_i))^2} \cdot g_{0,i}(z_i)\mathrm{d}\mu_i(z_i) \\
&= \int_{\mathcal{Z}_i} \frac{1}{g_{0,i}(z_i)} \left(\int_{\mathbb{R}} q_i(z_i \mid x) v_{k_1}(x)\mathrm{d}x\right)\left(\int_{\mathbb{R}} q_i(z_i \mid y) v_{k_2}(y)\mathrm{d}y\right)\mathrm{d}\mu_i(z_i) \\
&= \int_{\mathbb{R}}\int_{\mathbb{R}} \left(\int_{\mathcal{Z}_i} \frac{q_i(z_i \mid x) q_i(z_i \mid y)\mathbb{1}_B(x)\mathbb{1}_B(y)}{g_{0,i}(z_i)}\mathrm{d}\mu_i(z_i)\right) v_{k_1}(x) v_{k_2}(y)\mathrm{d}x\mathrm{d}y \\
&= \int_{\mathbb{R}}\int_{\mathbb{R}} F_i(x,y) v_{k_1}(x) v_{k_2}(y)\mathrm{d}x\mathrm{d}y = \langle v_{k_1}, K_i^\star K_i v_{k_2}\rangle.
\end{aligned}$$

Using $1 + x \leq \exp(x)$, we thus obtain

$$\begin{aligned}
\mathbb{E}_{Q_{f_0}^n}\left[\left(\frac{dQ_n}{dQ_{f_0}^n}\right)^2\right] &= \mathbb{E}_{\nu,\nu'}\prod_{i=1}^n\left(1 + \delta^2 \sum_{k_1,k_2=1}^N \frac{\nu_{k_1}\nu'_{k_2}}{\tilde{\lambda}_{k_1}\tilde{\lambda}_{k_2}}\langle v_{k_1}, K_i^\star K_i v_{k_2}\rangle\right) \\
&\leq \mathbb{E}_{\nu,\nu'}\left[\exp\left(\delta^2 \sum_{i=1}^n \sum_{k_1,k_2=1}^N \frac{\nu_{k_1}\nu'_{k_2}}{\tilde{\lambda}_{k_1}\tilde{\lambda}_{k_2}}\langle v_{k_1}, K_i^\star K_i v_{k_2}\rangle\right)\right] \\
&= \mathbb{E}_{\nu,\nu'}\left[\exp\left(n\delta^2 \sum_{k_1,k_2=1}^N \frac{\nu_{k_1}\nu'_{k_2}}{\tilde{\lambda}_{k_1}\tilde{\lambda}_{k_2}}\langle v_{k_1}, K v_{k_2}\rangle\right)\right] \\
&= \mathbb{E}_{\nu,\nu'}\left[\exp\left(n\delta^2 \sum_{k_1,k_2=1}^N \frac{\nu_{k_1}\nu'_{k_2}}{\tilde{\lambda}_{k_1}\tilde{\lambda}_{k_2}} \cdot \lambda_{k_2}^2\langle v_{k_1}, v_{k_2}\rangle\right)\right] \\
&\leq \mathbb{E}_{\nu,\nu'}\left[\exp\left(n\delta^2 z_\alpha^2 \sum_{k=1}^N \nu_k\nu'_k\right)\right],
\end{aligned}$$

where we have used that

$$\frac{\lambda_k^2}{\tilde{\lambda}_k^2} = \frac{\lambda_k^2}{\max\{z_\alpha^{-2}\lambda_k^2, 2h\}} \leq z_\alpha^2.$$

Now, using that for $k = 1, \ldots, N$, ν_k, ν'_k are Rademacher distributed and independent random variables, we obtain

$$\begin{aligned}
&\mathbb{E}_{Q_{f_0}^n}\left[\left(\frac{dQ_n}{dQ_{f_0}^n}\right)^2\right] \leq \mathbb{E}_{\nu,\nu'}\left[\prod_{k=1}^N \exp\left(n\delta^2 z_\alpha^2 \nu_k\nu'_k\right)\right] \\
&= \mathbb{E}_\nu\left[\prod_{k=1}^N \cosh\left(n\delta^2 z_\alpha^2 \nu_k\right)\right] = \prod_{k=1}^N \cosh\left(n\delta^2 z_\alpha^2\right) \leq \exp\left(\frac{N n^2 \delta^4 z_\alpha^4}{2}\right),
\end{aligned}$$

where the last inequality follows from $\cosh(x) \leq \exp(x^2/2)$ for all $x \in \mathbb{R}$. Thus, (4.8) holds as soon as

$$\delta \leq \left[\frac{2\log\left(1+(1-b-\gamma)^2\right)}{Nn^2 z_\alpha^4}\right]^{1/4}.$$

Finally, taking $\delta = \min\left\{\frac{h}{\sqrt{\log(2N/b)}}\min\left\{\frac{C_0(B)}{\|\psi\|_\infty}, \frac{1}{2}\left(1-\frac{L_0}{L}\right)h^\beta\right\}, \left[\frac{2\log\left(1+(1-b-\gamma)^2\right)}{Nn^2 z_\alpha^4}\right]^{1/4}\right\}$, we obtain

$$\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) \geq C(\psi,b,\gamma)\frac{1}{\sqrt{\log\left(2N/b\right)}}\min\left\{\frac{|B|}{\sqrt{\log(2N/b)}}\min\left\{\frac{C_0(B)}{\|\psi\|_\infty}, \frac{1}{2}\left(1-\frac{L_0}{L}\right)h^\beta\right\}, \frac{N^{3/4}}{\sqrt{nz_\alpha^2}}\right\}.$$

If B is chosen such that $C_0(B) = \min\{f_0(x), x \in B\} \geq Ch^\beta$, then the bound becomes

$$\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) \geq C(\psi,b,\gamma,L,L_0)\frac{1}{\sqrt{\log\left(2N/b\right)}}\min\left\{\frac{|B|h^\beta}{\sqrt{\log(2N/b)}}, \frac{N^{3/4}}{\sqrt{nz_\alpha^2}}\right\},$$

and the choice $h \asymp |B|^{-1/(4\beta+3)}(nz_\alpha^2)^{-2/(4\beta+3)}$ yields

$$\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) \geq C(\psi,b,\gamma,L,L_0)\left[\log\left(C|B|^{\frac{4\beta+4}{4\beta+3}}(nz_\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1}|B|^{\frac{3\beta+3}{4\beta+3}}(nz_\alpha^2)^{-\frac{2\beta}{4\beta+3}}.$$

Note that with this choice of h, the condition $C_0(B) \geq Ch^\beta$ becomes

$$|B|^{\beta/(4\beta+3)}C_0(B) \geq C(nz_\alpha^2)^{-2\beta/(4\beta+3)}.$$

□

4.4 Interactive Privacy Mechanisms

In this section, we prove that the results obtained in Section 4.3 can be improved when sequential interaction is allowed between data-holders.

4.4.1 Upper bound in the interactive scenario

We first propose a testing procedure which relies on some sequential interaction between data-holders. We then prove that this test achieves a better separation rate than the one obtained in Section 4.3.

We assume that the sample size is equal to $3n$ so that we can split the data in three parts. Like in the non-interactive scenario, we consider a non empty compact set $B \subset \mathbb{R}$, and $B = \bigcup_{j=1}^{N} B_j$ a partition of B with $|B_j| = 2h$ for all $j \in [\![1, N]\!]$.

With the first third of the data, $X_1, \dots, X_n$, we generate privatized arrays $Z_i = (Z_{ij})_{j=1,\dots,N}$ that will be used to estimate $p(j) := \int_{B_j} f$. Let's consider the following privacy mechanism. We first generate an i.i.d. sequence $(W_{ij})_{i\in[\![1,n]\!],j\in[\![1,N]\!]}$ of Laplace(1) random variables and for $i = 1, \dots, n$ and $j = 1, \dots, N$ we set

$$Z_{ij} = I(X_i \in B_j) + \frac{2}{\alpha} W_{ij}.$$

For each $j = 1, \dots, N$, we then build an estimator of $p(j) := \int_{B_j} f$ via

$$\widehat{p}_j = \frac{1}{n} \sum_{i=1}^{n} Z_{ij}.$$

We now privatize the second third of the data. Set $c_\alpha = \frac{e^\alpha+1}{e^\alpha-1}$ and $\tau = (n\alpha^2)^{-1/2}$. For all $i \in [\![n+1, 2n]\!]$, we generate $Z_i \in \{-c_\alpha\tau, c_\alpha\tau\}$ using the estimator $\widehat{p}_j$ and the true data X_i by

$$\mathbb{P}\left(Z_i = \pm c_\alpha\tau \mid X_i \in B_j\right) = \frac{1}{2}\left(1 \pm \frac{[\widehat{p}_j - p_0(j)]_{-\tau}^{\tau}}{c_\alpha\tau}\right),$$

$$\mathbb{P}\left(Z_i = \pm c_\alpha\tau \mid X_i \in \bar{B}\right) = \frac{1}{2},$$

where $[x]_{-\tau}^{\tau} = \max\{-\tau, \min(x, \tau)\}$, and $p_0(j) = \int_{B_j} f_0$. We then define the test statistic

$$D_B = \frac{1}{n} \sum_{i=n+1}^{2n} Z_i - \sum_{j=1}^{N} p_0(j)[\widehat{p}_j - p_0(j)]_{-\tau}^{\tau}.$$

The analysis of the mean and variance of this statistic can be found in Appendix 4.7.2. It will be crucial in the analysis of our final test procedure.
Finally, we define the same tail test statistic as in Section 4.3. For all $i \in [\![2n+1, 3n]\!]$, a private view Z_i of X_i is generated by

$$Z_i = \pm c_\alpha, \text{ with probabilities } \frac{1}{2}\left(1 \pm \frac{I(X_i \notin B)}{c_\alpha}\right),$$

and we set

$$T_B = \frac{1}{n}\sum_{i=2n+1}^{3n} Z_i - \int_{\overline{B}} f_0.$$

The final test is

$$\Phi = \begin{cases} 1 & \text{if } D_B \geq t_1 \text{ or } T_B \geq t_2 \\ 0 & \text{otherwise} \end{cases}, \tag{4.9}$$

where

$$t_1 = \frac{2\sqrt{5}}{n\alpha^2\sqrt{\gamma}}, \qquad t_2 = \sqrt{\frac{20}{n\alpha^2\gamma}}. \tag{4.10}$$

We denote the privacy mechanism that outputs $(Z_1, \ldots, Z_n, Z_{n+1}, \ldots, Z_{2n}, Z_{2n+1}, \ldots, Z_{3n})$ by Q. It is sequentially interactive since each Z_i for $i \in [\![n+1, 2n]\!]$ depends on the privatized data $(Z_1, \ldots, Z_n)$ through $\widehat{p}_j$, but does not depend on the other Z_k, $k \in [\![n+1, 2n]\!]$, $k \neq i$. The following result establishes that this mechanism provides α-local differential privacy. Its proof is deferred to Appendix 4.7.1.

Proposition 4.4.1. *The sequentially interactive privacy mechanism Q provides α-local differential privacy.*

The following Proposition gives properties of the test statistic D_B. Its proof is in the Appendix 4.7.2.

Proposition 4.4.2. *1. It holds $\mathbb{E}_{Qf^n}[D_B] = \sum_{j=1}^N \{p(j) - p_0(j)\}\mathbb{E}\left[[\widehat{p}_j - p_0(j)]_{-\tau}^{\tau}\right]$. In particular, $\mathbb{E}_{Qf_0^n}[D_B] = 0$. Moreover, we have*

$$\mathbb{E}_{Qf^n}[D_B] \geq \frac{1}{6}D_\tau(f) - 6\frac{\tau}{\sqrt{n}}, \tag{4.11}$$

with $D_\tau(f) = \sum_{j=1}^N |p(j) - p_0(j)| \min\{|p(j) - p_0(j)|, \tau\}$ where we recall that $p(j) := \int_{B_j} f$.

2. It holds

$$\mathrm{Var}_{Qf^n}(D_B) \leq \frac{5}{(n\alpha^2)^2} + 67\frac{D_\tau(f)}{n\alpha^2}.$$

The following result presents an upper bound on $\mathcal{E}_{n,\alpha}(f_0, \gamma)$. Its proof is in Appendix 4.7.3.

Theorem 4.4.3. *Assume that $\alpha \in (0, 1)$ and $\beta < 1$. The test procedure Φ in (4.9) with t_1 and t_2 in (4.10) and bandwidth h given by*

$$h \asymp |B|^{-\frac{1}{2\beta+1}}(n\alpha^2)^{-\frac{1}{2\beta+1}},$$

attains the following bound on the separation rate

$$\mathcal{E}_{n,\alpha}(f_0,\gamma) \leq C(L,L_0,\gamma)\left\{|B|^{\frac{\beta+1}{2\beta+1}}(n\alpha^2)^{-\frac{\beta}{2\beta+1}} + \int_{\overline{B}} f_0 + \frac{1}{\sqrt{n\alpha^2}}\right\}.$$

This result indicates to choose the optimal set $B = B_{n,\alpha}$ as a level set

$$B_{n,\alpha} = \arg \inf_{B \text{ compact set}} \left\{\int_{\overline{B}} f_0 \geq |B|^{\frac{\beta+1}{2\beta+1}}(n\alpha^2)^{-\frac{\beta}{2\beta+1}} + \frac{1}{\sqrt{n\alpha^2}} \text{ and } \inf_B f_0 \geq \sup_{\overline{B}} f_0\right\}. \tag{4.12}$$

4.4.2 Lower bound in the interactive scenario

In this subsection we complement the study of $\mathcal{E}_{n,\alpha}(f_0,\gamma)$ with a lower bound. This lower bound will turn out to match the upper bound for several f_0, proving the optimality of the test and privacy mechanism proposed in the previous subsection for several f_0. See Section 4.5 for the optimality.

Theorem 4.4.4. *Let $\alpha \in (0,1)$. Assume that $\beta \leq 1$. Set $z_\alpha = e^{2\alpha} - e^{-2\alpha}$. For all compact set $B \subset \mathbb{R}$ satisfying*

$$|B|^{\beta/(2\beta+1)} C_0(B) \geq C(nz_\alpha^2)^{-\beta/(2\beta+1)} \tag{4.13}$$

for some $C > 0$ where $C_0(B) = \min\{f_0(x) : x \in B\}$, it holds

$$\mathcal{E}_{n,\alpha}(f_0,\gamma) \geq C(\psi,\gamma,L,L_0)|B|^{\frac{\beta+1}{2\beta+1}}(nz_\alpha^2)^{-\frac{\beta}{2\beta+1}}.$$

The proof is deferred to Appendix 4.7.4. Let us note that the same comment after Theorem 4.3.5 holds in this case. In all examples, we choose the set $B_{n,\alpha}$ as defined in (4.12) and show that it checks the condition (4.13) giving thus minimax optimality of the testing rates.

4.5 Examples

In this section, we investigate the optimality of our lower and upper bounds for some examples of densities f_0. For all the examples studied below, our bounds are optimal (up to a constant) in the interactive scenario, and optimal up to a logarithmic factor in the non-interactive scenario.

	Non-private separation rate	Private separation rate, non-interactive scenario (up to a log factor)	Private separation rate, interactive scenario
$\mathcal{U}([a,b])$	$n^{-2/5}$	$(n\alpha^2)^{-2/7}$	$(n\alpha^2)^{-1/3}$
$\mathcal{N}(0,1)$	$n^{-2/5}$	$\log(n\alpha^2)^{3/7}(n\alpha^2)^{-2/7}$	$\log(n\alpha^2)^{1/3}(n\alpha^2)^{-1/3}$
Beta(a,b)	$n^{-2/5}$	$(n\alpha^2)^{-2/7}$	$(n\alpha^2)^{-1/3}$
Spiky null	$n^{-2/5}$	$(n\alpha^2)^{-2/7}$	$(n\alpha^2)^{-1/3}$
Cauchy$(0,a)$	$(\log n)^{4/5}n^{-2/5}$	$(n\alpha^2)^{-2/13}$	$(n\alpha^2)^{-1/5}$
Pareto(a,k)	$n^{-2k/(2+3k)}$	$(n\alpha^2)^{-2k/(7k+6)}$	$(n\alpha^2)^{-k/(3k+2)}$
Exp(λ)	$n^{-2/5}$	$\log(n\alpha^2)^{6/7}(n\alpha^2)^{-2/7}$	$\log(n\alpha^2)^{2/3}(n\alpha^2)^{-1/3}$

Table 4.1: Some examples of separation rates for different choices of densities f_0 and $\beta = 1$. The non-private separation rates can be found in [7]

The densities considered in this section are Hölder continuous with exponent β for all $\beta \in (0,1]$ unless otherwise specified. The results are stated for n large enough and $\alpha \in (0,1)$ such that $n\alpha^2 \to +\infty$ as $n \to \infty$. They are summarised in Table 4.1 for $\beta = 1$ and compared to the non-private separation rates. The proofs can be found in Appendix 4.8.

Example 4.5.1. Assume that f_0 is the density of the continuous uniform distribution on $[a,b]$ where a and b are two constants satisfying $a < b$, that is

$$f_0(x) = \frac{1}{b-a} I(x \in [a,b]).$$

Taking $B = [a,b]$ in Theorems 4.3.5, 4.3.4, 4.4.4 and 4.4.3 yields the following bounds on the minimax radius

$$\left[\log\left(C(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}} \lesssim \mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) \lesssim (n\alpha^2)^{-\frac{2\beta}{4\beta+3}},$$

and

$$\mathcal{E}_{n,\alpha}(f_0,\gamma) \asymp (n\alpha^2)^{-\frac{\beta}{2\beta+1}}$$

Example 4.5.2. Assume that f_0 is the density of the Pareto distribution with parameters $a > 0$ and $k > 0$, that is

$$f_0(x) = \frac{ka^k}{x^{k+1}} I(x \geq a).$$

It holds

$$\left[\log\left(C(n\alpha^2)^{\frac{4\beta+4}{4\beta+3}\cdot\frac{2\beta}{k(4\beta+3)+3\beta+3}+\frac{2}{4\beta+3}}\right)\right]^{-1}(n\alpha^2)^{-\frac{2k\beta}{k(4\beta+3)+3\beta+3}} \lesssim \mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) \lesssim (n\alpha^2)^{-\frac{2k\beta}{k(4\beta+3)+3\beta+3}},$$

and

$$\mathcal{E}_{n,\alpha}(f_0,\gamma) \asymp (n\alpha^2)^{-\frac{k\beta}{k(2\beta+1)+\beta+1}}.$$

Example 4.5.3. Assume that f_0 is the density of the exponential distribution with parameter $\lambda > 0$, that is

$$f_0(x) = \lambda\exp(-\lambda x)I(x \geq 0).$$

It holds

$$\left[\log\left(C\log(n\alpha^2)^{\frac{4\beta+4}{4\beta+3}}(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1}\log(n\alpha^2)^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}} \lesssim \mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) \lesssim \log(n\alpha^2)^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}},$$

and

$$\mathcal{E}_{n,\alpha}(f_0,\gamma) \asymp \log(n\alpha^2)^{\frac{\beta+1}{2\beta+1}}(n\alpha^2)^{-\frac{\beta}{2\beta+1}}$$

Example 4.5.4. Assume that f_0 is the density of the normal distribution with parameters 0 and 1, that is

$$f_0(x) = \frac{1}{\sqrt{2\pi}}\exp\left(-\frac{x^2}{2}\right).$$

It holds

$$\left[\log\left(C\log(n\alpha^2)^{\frac{4\beta+4}{2(4\beta+3)}}(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1}\log(n\alpha^2)^{\frac{3\beta+3}{2(4\beta+3)}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}} \lesssim \mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma),$$

$$\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) \lesssim \log(n\alpha^2)^{\frac{3\beta+3}{2(4\beta+3)}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}},$$

and

$$\mathcal{E}_{n,\alpha}(f_0,\gamma) \asymp \log(n\alpha^2)^{\frac{\beta+1}{2(2\beta+1)}}(n\alpha^2)^{-\frac{\beta}{2\beta+1}}$$

Example 4.5.5. Assume that f_0 is the density of the Cauchy distribution with parameters 0 and $a > 0$, that is

$$f_0(x) = \frac{1}{\pi a}\frac{a^2}{x^2+a^2}.$$

It holds

$$\left[\log\left(C(n\alpha^2)^{\frac{4\beta+4}{4\beta+3}\cdot\frac{2\beta}{7\beta+6}+\frac{2}{4\beta+3}}\right)\right]^{-1}(n\alpha^2)^{-\frac{2\beta}{7\beta+6}} \lesssim \mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) \lesssim (n\alpha^2)^{-\frac{2\beta}{7\beta+6}},$$

and

$$\mathcal{E}_{n,\alpha}(f_0,\gamma) \asymp (n\alpha^2)^{-\frac{\beta}{3\beta+2}}$$

Example 4.5.6. Assume that the density f_0 is given by

$$f_0(x) = \begin{cases} L_0 x & \text{if } 0 \le x \le \frac{1}{\sqrt{L_0}} \\ 2\sqrt{L_0} - L_0 x & \text{if } \frac{1}{\sqrt{L_0}} \le x \le \frac{2}{\sqrt{L_0}} \\ 0 & \text{otherwise.} \end{cases}$$

It holds

$$\left[\log\left(C(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}} \lesssim \mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) \lesssim (n\alpha^2)^{-\frac{2\beta}{4\beta+3}},$$

and

$$\mathcal{E}_{n,\alpha}(f_0,\gamma) \asymp (n\alpha^2)^{-\frac{\beta}{2\beta+1}}$$

Example 4.5.7. Assume that f_0 is the density of the Beta distribution with parameters $a \ge 1$ and $b \ge 1$, that is

$$f_0(x) = \frac{1}{B(a,b)} x^{a-1}(1-x)^{b-1} I(0 < x < 1), \tag{4.14}$$

where $B(\cdot,\cdot)$ is the Beta function. It holds

$$\left[\log\left(C(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}} \lesssim \mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) \lesssim (n\alpha^2)^{-\frac{2\beta}{4\beta+3}},$$

and

$$\mathcal{E}_{n,\alpha}(f_0,\gamma) \asymp (n\alpha^2)^{-\frac{\beta}{2\beta+1}}.$$

Note that the density f_0 given by (4.14) can be defined for all $a > 0$ and $b > 0$. However, f_0 is Hölder continuous for no exponent $\beta \in (0,1]$ if $a < 1$ or $b < 1$. Note also that if $a = 1$ and $b = 1$ then f_0 is the density of the continuous uniform distribution on $[0,1]$, and this case has already been tackled in Example 4.5.1. Now, if $a = 1$ and $b > 1$ (respectively $a > 1$ and $b = 1$), one can check that f_0 is Hölder continuous with exponent β for all $\beta \in (0, \min\{b-1, 1\}]$ (respectively $\beta \in (0, \min\{a-1, 1\}]$). Finally, if $a > 1$ and $b > 1$ then f_0 is is Hölder continuous with exponent β for all $\beta \in (0, \min\{a-1, b-1, 1\}]$.

4.6 Appendix : Proofs of Section 4.3

4.6.1 Proof of Proposition 4.3.2

Let $i \in [\![1, n]\!]$. Set $\sigma := 2\|\psi\|_\infty/(\alpha h)$. The conditional density of Z_i given $X_i = y$ can be written as

$$q^{Z_i|X_i=y}(z) = \prod_{j=1}^{N} \frac{1}{2\sigma} \exp\left(-\frac{|z_j - \psi_h(x_j - y)|}{\sigma}\right).$$

Thus, by the reverse and the ordinary triangle inequality,

$$\begin{aligned}
\frac{q^{Z_i|X_i=y}(z)}{q^{Z_i|X_i=y'}(z)} &= \prod_{j=1}^{N} \exp\left(\frac{|z_j - \psi_h(x_j - y')| - |z_j - \psi_h(x_j - y)|}{\sigma}\right) \\
&\leq \prod_{j=1}^{N} \exp\left(\frac{|\psi_h(x_j - y') - \psi_h(x_j - y)|}{\sigma}\right) \\
&\leq \exp\left(\frac{1}{\sigma h} \sum_{j=1}^{N} \left|\psi\left(\frac{x_j - y'}{h}\right) - \psi\left(\frac{x_j - y}{h}\right)\right|\right) \\
&\leq \exp\left(\frac{1}{\sigma h} \sum_{j=1}^{N} \left[\left|\psi\left(\frac{x_j - y'}{h}\right)\right| + \left|\psi\left(\frac{x_j - y}{h}\right)\right|\right]\right) \\
&\leq \exp\left(\frac{2\|\psi\|_\infty}{\sigma h}\right) \\
&\leq \exp(\alpha),
\end{aligned}$$

where the second to last inequality follows from the fact that for a fixed y the quantity $\psi((x_j - y)/h)$ is non-zero for at most one coefficient $j \in [\![1, N]\!]$. This is a consequence of Assumption 4.3.1. This proves that Z_i is an α-locally differentially private view of X_i for all $i \in [\![1, n]\!]$.

Consider now $i \in [\![n+1, 2n]\!]$. For all $j \in [\![1, N]\!]$ it holds

$$\frac{\mathbb{P}\left(Z_i = c_\alpha \mid X_i \notin B\right)}{\mathbb{P}\left(Z_i = c_\alpha \mid X_i \in B_j\right)} = 1 + \frac{1}{c_\alpha} = \frac{2e^\alpha}{e^\alpha + 1}.$$

Since $2 \leq e^\alpha + 1 \leq 2e^\alpha$, we obtain

$$e^{-\alpha} \leq 1 \leq \frac{\mathbb{P}\left(Z_i = c_\alpha \mid X_i \notin B\right)}{\mathbb{P}\left(Z_i = c_\alpha \mid X_i \in B_j\right)} \leq e^\alpha.$$

It also holds

$$\frac{\mathbb{P}\left(Z_i = -c_\alpha \mid X_i \notin B\right)}{\mathbb{P}\left(Z_i = -c_\alpha \mid X_i \in B_j\right)} = 1 - \frac{1}{c_\alpha} = \frac{2}{e^\alpha + 1} \in [e^{-\alpha}, e^\alpha].$$

Now, for all $(j,k) \in [\![1, N]\!]^2$ it holds

$$\frac{\mathbb{P}\left(Z_i = c_\alpha \mid X_i \in B_k\right)}{\mathbb{P}\left(Z_i = c_\alpha \mid X_i \in B_j\right)} = \frac{\mathbb{P}\left(Z_i = -c_\alpha \mid X_i \in B_k\right)}{\mathbb{P}\left(Z_i = -c_\alpha \mid X_i \in B_j\right)} = 1 \in [e^{-\alpha}, e^\alpha].$$

This proves that Z_i is an α-locally differentially private view of X_i for all $i \in [\![n+1, 2n]\!]$.

4.6.2 Proof of Theorem 4.3.4

Proof of Proposition 4.3.3. 1. Equality (4.4) follows from the independance of Z_i and Z_k for $i \neq k$ and from $\mathbb{E}[Z_{ij}] = \psi_h * f(x_j)$. We now prove (4.5). Set $a_{h,j} := \psi_h * f(x_j)$ and let us define

$$\widehat{U}_B = \frac{1}{n(n-1)} \sum_{i \neq k} \sum_{j=1}^{N} \left(Z_{ij} - a_{h,j}\right)\left(Z_{kj} - a_{h,j}\right),$$

$$\widehat{V}_B = \frac{2}{n} \sum_{i=1}^{n} \sum_{j=1}^{N} \left(a_{h,j} - f_0(x_j)\right)\left(Z_{ij} - a_{h,j}\right),$$

and observe that we have

$$S_B = \widehat{U}_B + \widehat{V}_B + \sum_{j=1}^{N} (a_{h,j} - f_0(x_j))^2.$$

Note that $\mathrm{Cov}(\widehat{U}_B, \widehat{V}_B) = 0$. We thus have

$$\mathrm{Var}(S_B) = \mathrm{Var}(\widehat{U}_B) + \mathrm{Var}(\widehat{V}_B),$$

and we will bound from above $\mathrm{Var}(\widehat{U}_B)$ and $\mathrm{Var}(\widehat{V}_B)$ separately. We begin with $\mathrm{Var}(\widehat{V}_B)$. Since $\widehat{V}_B$ is centered, it holds

$$\begin{aligned}\mathrm{Var}(\widehat{V}_B) &= \mathbb{E}[\widehat{V}_B^2] \\ &= \frac{4}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{N} \sum_{t=1}^{n} \sum_{k=1}^{N} \left(a_{h,j} - f_0(x_j)\right)\left(a_{h,k} - f_0(x_k)\right) \mathbb{E}\left[\left(Z_{ij} - a_{h,j}\right)\left(Z_{tk} - a_{h,k}\right)\right].\end{aligned}$$

Note that if $t \neq i$, the independance of Z_i and Z_t yields

$$\mathbb{E}\left[\left(Z_{ij} - a_{h,j}\right)\left(Z_{tk} - a_{h,k}\right)\right] = 0.$$

Moreover, since the W_{ij}, $j = 1, \ldots, N$ are independent of X_i and $\mathbb{E}[W_{ij}] = 0$ we have

$$\begin{aligned}
&\mathbb{E}\left[\left(Z_{ij} - a_{h,j}\right)\left(Z_{ik} - a_{h,k}\right)\right] \\
&= \mathbb{E}\left[\left(\psi_h\left(x_j - X_i\right) + \frac{2\|\psi\|_\infty}{\alpha h} W_{ij} - a_{h,j}\right)\left(\psi_h\left(x_k - X_i\right) + \frac{2\|\psi\|_\infty}{\alpha h} W_{ik} - a_{h,k}\right)\right] \\
&= \mathbb{E}\left[\psi_h\left(x_j - X_i\right)\psi_h\left(x_k - X_i\right)\right] - a_{h,k}\mathbb{E}\left[\psi_h\left(x_j - X_i\right)\right] + \frac{4\|\psi\|_\infty^2}{\alpha^2 h^2}\mathbb{E}\left[W_{ij}W_{ik}\right] \\
&\qquad - a_{h,j}\mathbb{E}\left[\psi_h\left(x_k - X_i\right)\right] + a_{h,j}a_{h,k} \\
&= \left[\int \left(\psi_h\left(x_j - y\right)\right)^2 f(y)\mathrm{d}y + \frac{8\|\psi\|_\infty^2}{\alpha^2 h^2}\right] I(j = k) - a_{h,j}a_{h,k},
\end{aligned}$$

where the last equality is a consequence of Assumption 4.3.1. We thus obtain

$$\begin{aligned}
\mathrm{Var}(\widehat{V}_B) &= \frac{4}{n}\sum_{j=1}^{N}\left(a_{h,j} - f_0(x_j)\right)^2\left[\int(\psi_h\left(x_j - y\right))^2 f(y)\mathrm{d}y + \frac{8\|\psi\|_\infty^2}{\alpha^2 h^2}\right] \\
&\qquad - \frac{4}{n}\sum_{j=1}^{N}\sum_{k=1}^{N}\left(a_{h,j} - f_0(x_j)\right)\left(a_{h,k} - f_0(x_k)\right)a_{h,j}a_{h,k} \\
&= \frac{4}{n}\sum_{j=1}^{N}\left(a_{h,j} - f_0(x_j)\right)^2\left[\int(\psi_h\left(x_j - y\right))^2 f(y)\mathrm{d}y + \frac{8\|\psi\|_\infty^2}{\alpha^2 h^2}\right] \\
&\qquad - \frac{4}{n}\left(\sum_{j=1}^{N}\left(a_{h,j} - f_0(x_j)\right)a_{h,j}\right)^2 \\
&\leq \frac{4}{n}\sum_{j=1}^{N}\left(a_{h,j} - f_0(x_j)\right)^2\left[\int(\psi_h\left(x_j - y\right))^2 f(y)\mathrm{d}y + \frac{8\|\psi\|_\infty^2}{\alpha^2 h^2}\right].
\end{aligned}$$

Now, $\int(\psi_h\left(x_j - y\right))^2 f(y)\mathrm{d}y \leq \|\psi_h\|_\infty^2 \leq \|\psi\|_\infty^2/h^2 \leq \|\psi\|_\infty^2/(\alpha^2 h^2)$ if $\alpha \in (0, 1]$. We finally obtain

$$\mathrm{Var}(\widehat{V}_B) \leq \frac{36\|\psi\|_\infty^2}{n\alpha^2 h^2}\sum_{j=1}^{N}\left(a_{h,j} - f_0(x_j)\right)^2.$$

We now bound from above $\mathrm{Var}(\widehat{U}_B)$. One can rewrite $\widehat{U}_B$ as

$$\widehat{U}_B = \frac{1}{n(n-1)}\sum_{i \neq k} h(Z_i, Z_k),$$

where

$$h(Z_i, Z_k) = \sum_{j=1}^{N} (Z_{ij} - a_{h,j})(Z_{kj} - a_{h,j}).$$

Using a result for the variance of a U-statistic (see for instance Lemma A, p.183 in [64]), we have

$$\binom{n}{2} \mathrm{Var}(\widehat{U}_B) = 2(n-2)\zeta_1 + \zeta_2,$$

where

$$\zeta_1 = \mathrm{Var}\left(\mathbb{E}\left[h(Z_1, Z_2) \mid Z_1\right]\right), \text{ and } \zeta_2 = \mathrm{Var}\left(h(Z_1, Z_2)\right).$$

We have $\zeta_1 = 0$ since $\mathbb{E}\left[h(Z_1, Z_2) \mid Z_1\right] = 0$ and thus

$$\mathrm{Var}(\widehat{U}_B) = \frac{2}{n(n-1)} \mathrm{Var}\left(h(Z_1, Z_2)\right).$$

Write

$$\begin{aligned}
h(Z_1, Z_2) &= \sum_{j=1}^{N} \left(\psi_h(x_j - X_1) + \frac{2\|\psi\|_\infty}{\alpha h} W_{1j} - a_{h,j}\right)\left(\psi_h(x_j - X_2) + \frac{2\|\psi\|_\infty}{\alpha h} W_{2j} - a_{h,j}\right) \\
&= \sum_{j=1}^{N} \left(\psi_h(x_j - X_1) - a_{h,j}\right)\left(\psi_h(x_j - X_2) - a_{h,j}\right) + \frac{4\|\psi\|_\infty^2}{\alpha^2 h^2} \sum_{j=1}^{N} W_{1j} W_{2j} \\
&\quad + \frac{2\|\psi\|_\infty}{\alpha h} \sum_{j=1}^{N} W_{1j}(\psi_h(x_j - X_2) - a_{h,j}) + \frac{2\|\psi\|_\infty}{\alpha h} \sum_{j=1}^{N} W_{2j}(\psi_h(x_j - X_1) - a_{h,j}) \\
&=: \tilde{T}_1 + \tilde{T}_2 + \tilde{T}_3 + \tilde{T}_4.
\end{aligned}$$

We thus have $\mathrm{Var}(h(Z_1, Z_2)) = \sum_{i=1}^{4} \mathrm{Var}(\tilde{T}_i) + 2\sum_{i<j} \mathrm{Cov}(\tilde{T}_i, \tilde{T}_j)$. Observe that $\mathrm{Cov}(\tilde{T}_i, \tilde{T}_j) = 0$ for $i < j$ and $\mathrm{Var}(\tilde{T}_3) = \mathrm{Var}(\tilde{T}_4)$. We thus have

$$\mathrm{Var}(h(Z_1, Z_2)) = \mathrm{Var}(\tilde{T}_1) + \mathrm{Var}(\tilde{T}_2) + 2\mathrm{Var}(\tilde{T}_3).$$

The independence of the random variables $(W_{ij})_{i,j}$ yields

$$\mathrm{Var}(\tilde{T}_2) = \frac{64\|\psi\|_\infty^4 N}{\alpha^4 h^4}.$$

The independence of the random variables $(W_{ij})_{i,j}$ and their independence with X_2 yield

$$\begin{aligned}
\mathrm{Var}(\tilde{T}_3) &= \mathbb{E}\left[\tilde{T}_3^2\right] \\
&= \frac{4\|\psi\|_\infty^2}{\alpha^2 h^2}\mathbb{E}\left[\sum_{j=1}^N W_{1j}(\psi_h(x_j - X_2) - a_{h,j})\sum_{k=1}^N W_{1k}(\psi_h(x_k - X_2) - a_{h,k})\right] \\
&= \frac{4\|\psi\|_\infty^2}{\alpha^2 h^2}\sum_{j=1}^N\sum_{k=1}^N \mathbb{E}\left[W_{1j}W_{1k}\right]\mathbb{E}\left[(\psi_h(x_j - X_2) - a_{h,j})(\psi_h(x_k - X_2) - a_{h,k})\right] \\
&= \frac{8\|\psi\|_\infty^2}{\alpha^2 h^2}\sum_{j=1}^N \mathbb{E}\left[(\psi_h(x_j - X_2) - a_{h,j})^2\right] \\
&\leq \frac{8\|\psi\|_\infty^2}{\alpha^2 h^2}\sum_{j=1}^N \mathbb{E}\left[(\psi_h(x_j - X_2))^2\right].
\end{aligned}$$

Now, since $y \mapsto \psi_h(x_j - y)$ is null outside B_j (consequence of Assumption 4.3.1), it holds

$$\sum_{j=1}^N \mathbb{E}\left[(\psi_h(x_j - X_2))^2\right] = \sum_{j=1}^N \int_{B_j} (\psi_h(x_j - y))^2 f(y)dy \leq \|\psi_h\|_\infty^2 \sum_{j=1}^N \int_{B_j} f \leq \|\psi_h\|_\infty^2,$$

and thus

$$\mathrm{Var}(\tilde{T}_3) \leq \frac{8\|\psi\|_\infty^4}{\alpha^2 h^4}.$$

By independence of X_1 and X_2, it holds $\mathbb{E}[\tilde{T}_1] = 0$, and

$$\begin{aligned}
\mathrm{Var}(\tilde{T}_1) &= \mathbb{E}\left[\tilde{T}_1^2\right] \\
&= \sum_{j=1}^{N}\sum_{k=1}^{N} \mathbb{E}\left[\left(\psi_h\left(x_j - X_1\right) - a_{h,j}\right)\left(\psi_h\left(x_j - X_2\right) - a_{h,j}\right)\right. \\
&\qquad\qquad \left.\cdot\left(\psi_h\left(x_k - X_1\right) - a_{h,k}\right)\left(\psi_h\left(x_k - X_2\right) - a_{h,k}\right)\right] \\
&= \sum_{j=1}^{N}\sum_{k=1}^{N} \mathbb{E}\left[\left(\psi_h\left(x_j - X_1\right) - a_{h,j}\right)\left(\psi_h\left(x_k - X_1\right) - a_{h,k}\right)\right] \\
&\qquad\qquad \cdot \mathbb{E}\left[\left(\psi_h\left(x_j - X_2\right) - a_{h,j}\right)\left(\psi_h\left(x_k - X_2\right) - a_{h,k}\right)\right] \\
&= \sum_{j=1}^{N}\sum_{k=1}^{N} \left[\int \psi_h(x_j - y)\psi_h(x_k - y) f(y)\mathrm{d}y - a_{h,j}a_{h,k}\right]^2 \\
&= \sum_{j=1}^{N}\sum_{k=1}^{N} \left(\int \psi_h(x_j - y)\psi_h(x_k - y) f(y)\mathrm{d}y\right)^2 + \sum_{j=1}^{N}\sum_{k=1}^{N} a_{h,j}^2 a_{h,k}^2 \\
&\qquad\qquad - 2\sum_{j=1}^{N}\sum_{k=1}^{N} a_{h,j}a_{h,k}\int \psi_h(x_j - y)\psi_h(x_k - y) f(y)\mathrm{d}y.
\end{aligned}$$

Assumption 4.3.1 yields $\int \psi_h(x_j - y)\psi_h(x_k - y) f(y)\mathrm{d}y = 0$ if $j \neq k$. We thus obtain

$$\mathrm{Var}(\tilde{T}_1) = \sum_{j=1}^{N}\left(\int (\psi_h(x_j - y))^2 f(y)\mathrm{d}y\right)^2 - 2\sum_{j=1}^{N} a_{h,j}^2 \int \left(\psi_h(x_j - y)\right)^2 f(y)\mathrm{d}y + \left(\sum_{j=1}^{N} a_{h,j}^2\right)^2.$$

Now, since $y \mapsto \psi_h(x_j - y)$ is null outside B_j (consequence of Assumption 4.3.1), observe that

$$\sum_{j=1}^{N}\left(\int (\psi_h(x_j - y))^2 f(y)\mathrm{d}y\right)^2 \leq \frac{\|\psi\|_\infty^4}{h^4}\sum_{j=1}^{N}\left(\int_{B_j} f\right)^2 \leq \frac{\|\psi\|_\infty^4}{h^4}\sum_{j=1}^{N}\int_{B_j} f \leq \frac{\|\psi\|_\infty^4}{h^4},$$

and

$$\left(\sum_{j=1}^{N} a_{h,j}^2\right)^2 = \left(\sum_{j=1}^{N}\left(\int \psi_h(x_j - y) f(y)\mathrm{d}y\right)^2\right)^2 \leq \frac{\|\psi\|_\infty^4}{h^4}\left[\sum_{j=1}^{N}\left(\int_{B_j} f\right)^2\right]^2 \leq \frac{\|\psi\|_\infty^4}{h^4},$$

yielding $\mathrm{Var}(\tilde{T}_1) \leq 2\frac{\|\psi\|_\infty^4}{h^4}$. We thus have

$$\mathrm{Var}(\widehat{U}_B) \leq \frac{2}{n(n-1)}\left[2\frac{\|\psi\|_\infty^4}{h^4} + \frac{64\|\psi\|_\infty^4 N}{\alpha^4 h^4} + \frac{16\|\psi\|_\infty^4}{\alpha^2 h^4}\right] \leq \frac{164\|\psi\|_\infty^4 N}{n(n-1)\alpha^4 h^4}.$$

Finally,

$$\mathrm{Var}(S_B) \leq \frac{36\|\psi\|_\infty^2}{n\alpha^2 h^2} \sum_{j=1}^{N} \left(a_{h,j} - f_0(x_j)\right)^2 + \frac{164\|\psi\|_\infty^4 N}{n(n-1)\alpha^4 h^4}.$$

2. For all $i \in [\![n+1, 2n]\!]$ it holds

$$\begin{aligned}
\mathbb{E}_{Q_f^n}[Z_i] &= \mathbb{E}\left[Z_i \mid X_i \notin B\right] \mathbb{P}\left(X_i \notin B\right) + \sum_{j=1}^{N} \mathbb{E}\left[Z_i \mid X_i \in B_j\right] \mathbb{P}\left(X_i \in B_j\right) \\
&= \left[c_\alpha \cdot \frac{1}{2}\left(1 + \frac{1}{c_\alpha}\right) - c_\alpha \cdot \frac{1}{2}\left(1 - \frac{1}{c_\alpha}\right)\right] \mathbb{P}\left(X_i \notin B\right) + \sum_{j=1}^{N} \left[c_\alpha \cdot \frac{1}{2} - c_\alpha \cdot \frac{1}{2}\right] \mathbb{P}\left(X_i \in B_j\right) \\
&= \mathbb{P}\left(X_i \notin B\right).
\end{aligned}$$

This yields $\mathbb{E}_{Q_f^n}[T_B] = \int_{\overline{B}}(f - f_0)$, and using the independence of the Z_i, $i = n+1, \ldots, 2n$ we obtain

$$\mathrm{Var}_{Q_f^n}[T_B] = \frac{1}{n^2} \sum_{i=n+1}^{2n} \mathrm{Var}(Z_i) = \frac{1}{n^2} \sum_{i=n+1}^{2n} \left[\mathbb{E}[Z_i^2] - \mathbb{E}[Z_i]^2\right] = \frac{1}{n}\left(c_\alpha^2 - \left(\int_{\overline{B}} f\right)^2\right).$$

□

We can now proove Theorem 4.3.4. We first prove that the choice of t_1 and t_2 in (4.3) gives $\mathbb{P}_{Q_{f_0}^n}(\Phi = 1) \leq \gamma/2$. Since $\mathbb{E}_{Q_{f_0}^n}[T_B] = 0$, Chebyshev's inequality and Proposition 4.3.3 yield for $\alpha \in (0, 1]$

$$\mathbb{P}_{Q_{f_0}^n}(T_B \geq t_2) \leq \mathbb{P}_{Q_{f_0}^n}(|T_B| \geq t_2) \leq \frac{\mathrm{Var}_{Q_{f_0}^n}(T_B)}{t_2^2} \leq \frac{c_\alpha^2}{n t_2^2} \leq \frac{5}{n\alpha^2 t_2^2} = \frac{\gamma}{4}.$$

If $t_1 > \mathbb{E}_{Q_{f_0}^n}[S_B] = \sum_{j=1}^{N} \left([\psi_h * f_0](x_j) - f_0(x_j)\right)^2$, then Chebychev's inequality and Propo-

sition 4.3.3 yield

$$\begin{aligned}\mathbb{P}_{Q^n_{f_0}}(S_B \geq t_1) &\leq \mathbb{P}_{Q^n_{f_0}}(|S_B - \mathbb{E}_{Q^n_{f_0}}[S_B]| \geq t_1 - \mathbb{E}_{Q^n_{f_0}}[S_B]) \\ &\leq \frac{\mathrm{Var}_{Q^n_{f_0}}(S_B)}{(t_1 - \mathbb{E}_{Q^n_{f_0}}[S_B])^2} \\ &\leq \frac{\frac{36\|\psi\|_\infty^2}{n\alpha^2h^2}\sum_{j=1}^N ([\psi_h * f_0](x_j) - f_0(x_j))^2}{\left(t_1 - \sum_{j=1}^N ([\psi_h * f_0](x_j) - f_0(x_j))^2\right)^2} \\ &\qquad + \frac{\frac{164\|\psi\|_\infty^4 N}{n(n-1)\alpha^4h^4}}{\left(t_1 - \sum_{j=1}^N ([\psi_h * f_0](x_j) - f_0(x_j))^2\right)^2}.\end{aligned}$$

Observe that

$$t_1 \geq \sum_{j=1}^N ([\psi_h * f_0](x_j) - f_0(x_j))^2 + \max\left\{\sqrt{\frac{288\|\psi\|_\infty^2}{\gamma n\alpha^2h^2}\sum_{j=1}^N ([\psi_h * f_0](x_j) - f_0(x_j))^2}, \sqrt{\frac{1312\|\psi\|_\infty^4 N}{\gamma n(n-1)\alpha^4h^4}}\right\}.$$

Indeed for $f \in H(\beta, L)$ with $\beta \leq 1$ it holds $|[\psi_h * f](x_j) - f(x_j)| \leq LC_\beta h^\beta$ for all $j \in [\![1, N]\!]$ where $C_\beta = \int_{-1}^1 |u|^\beta |\psi(u)| \mathrm{d}u$, and thus using $ab \leq a^2/2 + b^2/2$ we obtain

$$\begin{aligned}&\sum_{j=1}^N ([\psi_h * f_0](x_j) - f_0(x_j))^2 + \max\left\{\sqrt{\frac{288\|\psi\|_\infty^2}{\gamma n\alpha^2h^2}\sum_{j=1}^N ([\psi_h * f_0](x_j) - f_0(x_j))^2}, \sqrt{\frac{1312\|\psi\|_\infty^4 N}{\gamma n(n-1)\alpha^4h^4}}\right\} \\ &\quad\leq L_0^2C_\beta^2 Nh^{2\beta} + \max\left\{\frac{1}{2}L_0^2C_\beta^2 Nh^{2\beta} + \frac{144\|\psi\|_\infty^2}{\gamma n\alpha^2h^2}, \sqrt{\frac{1312\|\psi\|_\infty^4 N}{\gamma n(n-1)\alpha^4h^4}}\right\} \\ &\quad\leq \frac{3}{2}L_0^2C_\beta^2 Nh^{2\beta} + \frac{144\|\psi\|_\infty^2}{\gamma n\alpha^2h^2} + \frac{52\|\psi\|_\infty^2\sqrt{N}}{\sqrt{\gamma}n\alpha^2h^2} \\ &\quad\leq \frac{3}{2}L_0^2C_\beta^2 Nh^{2\beta} + \frac{196\|\psi\|_\infty^2\sqrt{N}}{\gamma n\alpha^2h^2} = t_1.\end{aligned}$$

Then it holds

$$\begin{aligned}\mathbb{P}_{Q^n_{f_0}}(S_B \geq t_1) &\leq \frac{\frac{36\|\psi\|_\infty^2}{n\alpha^2h^2}\sum_{j=1}^N ([\psi_h * f_0](x_j) - f_0(x_j))^2}{(t_1 - \sum_{j=1}^N ([\psi_h * f_0](x_j) - f_0(x_j))^2)^2} + \frac{\frac{164\|\psi\|_\infty^4 N}{n(n-1)\alpha^4h^4}}{(t_1 - \sum_{j=1}^N ([\psi_h * f_0](x_j) - f_0(x_j))^2)^2} \\ &\leq \frac{\gamma}{8} + \frac{\gamma}{8} \leq \frac{\gamma}{4},\end{aligned}$$

and thus

$$\mathbb{P}_{Q_{f_0}^n}(\Phi = 1) \leq \mathbb{P}_{Q_{f_0}^n}(T_B \geq t_2) + \mathbb{P}_{Q_{f_0}^n}(S_B \geq t_1) \leq \frac{\gamma}{2}.$$

We now exhibit $\rho_1, \rho_2 > 0$ such that

$$\begin{cases} \int_B |f - f_0| \geq \rho_1 \Rightarrow \mathbb{P}_{Q_f^n}(S_B < t_1) \leq \gamma/2 \\ \int_{\bar{B}} |f - f_0| \geq \rho_2 \Rightarrow \mathbb{P}_{Q_f^n}(T_B < t_2) \leq \gamma/2. \end{cases}$$

In this case, for all $f \in H(\beta, L)$ satisfying $\|f - f_0\|_1 \geq \rho_1 + \rho_2$ it holds

$$\mathbb{P}_{Q_{f_0}^n}(\Phi = 1) + \mathbb{P}_{Q_f^n}(\Phi = 0) \leq \frac{\gamma}{2} + \min\left\{\mathbb{P}_{Q_f^n}(S_B < t_1), \mathbb{P}_{Q_f^n}(T_B < t_2)\right\} \leq \frac{\gamma}{2} + \frac{\gamma}{2} = \gamma,$$

since $\int_B |f-f_0| + \int_{\bar{B}} |f-f_0| = \|f-f_0\|_1 \geq \rho_1+\rho_2$ implies $\int_B |f-f_0| \geq \rho_1$ or $\int_{\bar{B}} |f-f_0| \geq \rho_2$. Consequently, $\rho_1 + \rho_2$ will provide an upper bound on $\mathcal{E}_{n,\alpha}^{\mathrm{NI}}(f_0, \gamma)$.

If $\int_{\overline{B}}(f - f_0) = \mathbb{E}_{Q_f^n}[T_B] > t_2$ then Chebychev's inequality yields

$$\begin{aligned} \mathbb{P}_{Q_f^n}(T_B < t_2) &= \mathbb{P}_{Q_f^n}\left(\mathbb{E}_{Q_f^n}[T_B] - T_B > \mathbb{E}_{Q_f^n}[T_B] - t_2\right) \\ &\leq \mathbb{P}_{Q_f^n}\left(\left|\mathbb{E}_{Q_f^n}[T_B] - T_B\right| > \mathbb{E}_{Q_f^n}[T_B] - t_2\right) \\ &\leq \frac{\mathrm{Var}_{Q_f^n}(T_B)}{\left(\mathbb{E}_{Q_f^n}[T_B] - t_2\right)^2} \\ &\leq \frac{c_\alpha^2}{n\left(\int_{\overline{B}}(f - f_0) - t_2\right)^2}. \end{aligned}$$

Now, observe that

$$\int_{\bar{B}}(f - f_0) \geq \int_{\bar{B}} |f - f_0| - 2\int_{\bar{B}} f_0.$$

Thus, setting

$$\rho_2 = 2\int_{\bar{B}} f_0 + \left(1 + \frac{1}{\sqrt{2}}\right) t_2,$$

we obtain that $\int_{\bar{B}} |f - f_0| \geq \rho_2$ implies

$$\mathbb{P}_{Q_f^n}(T_B < t_2) \leq \frac{2c_\alpha^2}{nt_2^2} \leq \frac{10}{n\alpha^2 t_2^2} = \frac{\gamma}{2}.$$

We now exhibit ρ_1 such that $\int_B |f - f_0| \geq \rho_1$ implies $\mathbb{P}_{Q_f^n}(S_B < t_1) \leq \gamma/2$. First note that

if the following relation holds

$$\mathbb{E}_{Q_f^n}[S_B] = \sum_{j=1}^{N} |[\psi_h * f](x_j) - f_0(x_j)|^2 \geq t_1 + \sqrt{\frac{2\mathrm{Var}_{Q_f^n}(S_B)}{\gamma}}, \tag{4.15}$$

then Chebychev's inequality yields

$$\mathbb{P}_{Q_f^n}(S_B < t_1) \leq \mathbb{P}_{Q_f^n}\left(S_B \leq \mathbb{E}_{Q_f^n}[S_B] - \sqrt{\frac{2\mathrm{Var}_{Q_f^n}(S_B)}{\gamma}}\right) \leq \frac{\gamma}{2}.$$

Using $\sqrt{a+b} \leq \sqrt{a} + \sqrt{b}$ for all $a, b > 0$ and $ab \leq a^2/2 + b^2/2$ we have

$$\begin{aligned}
\sqrt{\frac{2\mathrm{Var}_{Q_f^n}(S_B)}{\gamma}} &\leq \sqrt{\frac{72\|\psi\|_\infty^2}{\gamma n\alpha^2 h^2}\sum_{j=1}^{N}\left([\psi_h * f](x_j) - f_0(x_j)\right)^2 + \frac{328\|\psi\|_\infty^4 N}{\gamma n(n-1)\alpha^4 h^4}} \\
&\leq \sqrt{\frac{72\|\psi\|_\infty^2}{\gamma n\alpha^2 h^2}\sum_{j=1}^{N}\left([\psi_h * f](x_j) - f_0(x_j)\right)^2} + \sqrt{\frac{656\|\psi\|_\infty^4 N}{\gamma n^2\alpha^4 h^4}} \\
&\leq \frac{1}{2}\sum_{j=1}^{N}\left([\psi_h * f](x_j) - f_0(x_j)\right)^2 + \frac{36\|\psi\|_\infty^2}{\gamma n\alpha^2 h^2} + \frac{26\|\psi\|_\infty^2\sqrt{N}}{\sqrt{\gamma} n\alpha^2 h^2} \\
&\leq \frac{1}{2}\sum_{j=1}^{N}\left([\psi_h * f](x_j) - f_0(x_j)\right)^2 + \frac{62\|\psi\|_\infty^2\sqrt{N}}{\gamma n\alpha^2 h^2}.
\end{aligned}$$

Thus, if

$$\sum_{j=1}^{N} |[\psi_h * f](x_j) - f_0(x_j)|^2 \geq 2\left[t_1 + \frac{62\|\psi\|_\infty^2\sqrt{N}}{\gamma n\alpha^2 h^2}\right] \tag{4.16}$$

then (4.15) holds and we have $\mathbb{P}_{Q_f^n}(S_B < t_1) \leq \gamma/2$. We now link $\sum_{j=1}^{N} |[\psi_h * f](x_j) - f_0(x_j)|^2$ to $\int_B |f - f_0|$. According to Cauchy-Schwarz inequality we have

$$\left(\sum_{j=1}^{N} |[\psi_h * f](x_j) - f_0(x_j)|\right)^2 \leq N\sum_{j=1}^{N} |[\psi_h * f](x_j) - f_0(x_j)|^2.$$

We also have

$$\begin{aligned}
&\left|\int_B |f-f_0| - \sum_{j=1}^N 2h|\psi_h * f(x_j) - f_0(x_j)|\right| \\
&\quad = \left|\sum_{j=1}^N \int_{B_j} |f-f_0| - \sum_{j=1}^N 2h|\psi_h * f(x_j) - f_0(x_j)|\right| \\
&\quad = \left|\sum_{j=1}^N \int_{B_j} (|f(x)-f_0(x)| - |\psi_h * f(x_j) - f_0(x_j)|)\,\mathrm{d}x\right| \\
&\quad \le \sum_{j=1}^N \int_{B_j} |f(x) - f_0(x) - \psi_h * f(x_j) + f_0(x_j)|\,\mathrm{d}x \\
&\quad \le \sum_{j=1}^N \int_{B_j} (|f(x)-f(x_j)| + |f(x_j) - \psi_h * f(x_j)| + |f_0(x_j) - f_0(x)|)\,\mathrm{d}x \\
&\quad \le \left[1 + C_\beta + \frac{L_0}{L}\right] Lh^\beta |B|.
\end{aligned}$$

We thus have

$$\sum_{j=1}^N |[\psi_h * f](x_j) - f_0(x_j)|^2 \ge \frac{1}{4Nh^2}\left(\int_B |f-f_0| - \left[1 + C_\beta + \frac{L_0}{L}\right] Lh^\beta |B|\right)^2.$$

Thus, if

$$\int_B |f-f_0| \ge \left[1 + C_\beta + \frac{L_0}{L}\right] Lh^\beta |B| + 2h\sqrt{N}\sqrt{2t_1 + \frac{124\|\psi\|_\infty^2\sqrt{N}}{\gamma n\alpha^2 h^2}} =: \rho_1$$

then (4.16) holds and we have $\mathbb{P}_{Q_f^n}(S_B < t_1) \le \gamma/2$. Consequently

$$\begin{aligned}
\mathcal{E}_{n,\alpha}^{\mathrm{NI}}(f_0,\gamma) &\le \rho_1 + \rho_2 \\
&\le \left[1 + C_\beta + \frac{L_0}{L}\right] Lh^\beta |B| + 2h\sqrt{N}\sqrt{2t_1 + \frac{124\|\psi\|_\infty^2\sqrt{N}}{\gamma n\alpha^2 h^2}} + 2\int_{\bar{B}} f_0 + \left(1 + \frac{1}{\sqrt{2}}\right) t_2 \\
&\le C(L, L_0, \beta, \gamma, \psi)\left[h^\beta |B| + Nh^{\beta+1} + \frac{N^{3/4}}{\sqrt{n\alpha^2}} + \int_{\bar{B}} f_0 + \frac{1}{\sqrt{n\alpha^2}}\right] \\
&\le C(L, L_0, \beta, \gamma, \psi)\left[h^\beta |B| + \frac{|B|^{3/4}}{h^{3/4}\sqrt{n\alpha^2}} + \int_{\bar{B}} f_0 + \frac{1}{\sqrt{n\alpha^2}}\right]
\end{aligned}$$

where we have used $\sqrt{a+b} \le \sqrt{a} + \sqrt{b}$ for $a, b > 0$ to obtain the second to last inequality.

Taking $h \asymp |B|^{-1/(4\beta+3)}(n\alpha^2)^{-2/(4\beta+3)}$ yields

$$\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) \le C(L,L_0,\beta,\gamma,\psi)\left[|B|^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}} + \int_{\overline{B}} f_0 + \frac{1}{\sqrt{n\alpha^2}}\right].$$

4.6.3 Proof of Lemma 4.3.6

For $j = 1,\dots,N$, write

$$v_j = \sum_{k=1}^{N} a_{kj}\psi_k.$$

Note that since $(\psi_1,\dots,\psi_N)$ and $(v_1,\dots,v_N)$ are two orthonormal bases of W_N, the matrix $(a_{kj})_{kj}$ is orthogonal. We can write

$$f_\nu(x) = f_0(x) + \delta\sum_{j=1}^{N}\sum_{k=1}^{N}\frac{\nu_j a_{kj}}{\tilde{\lambda}_j}\psi_k(x), \quad x\in\mathbb{R}.$$

Define

$$A_b = \left\{\nu\in\{-1,1\}^N : \left|\sum_{j=1}^{N}\frac{\nu_j a_{kj}}{\tilde{\lambda}_j}\right| \le \frac{1}{\sqrt{h}}\sqrt{\log\left(\frac{2N}{b}\right)} \text{ for all } 1\le k\le N\right\}.$$

The union bound and Hoeffding inequality yield

$$\begin{aligned}
\mathbb{P}_\nu(A_b^c) &\le \sum_{k=1}^{N}\mathbb{P}\left(\left|\sum_{j=1}^{N}\frac{\nu_j a_{kj}}{\tilde{\lambda}_j}\right| > \frac{1}{\sqrt{h}}\sqrt{\log\left(\frac{2N}{b}\right)}\right)\\
&\le \sum_{k=1}^{N} 2\exp\left(-\frac{2\log\left(\frac{2N}{b}\right)}{h\sum_{j=1}^{N}4\frac{a_{kj}^2}{\tilde{\lambda}_j^2}}\right)\\
&\le b,
\end{aligned}$$

where the last inequality follows from $\tilde{\lambda}_j^2 \ge 2h$ for all j and $\sum_{j=1}^{N} a_{kj}^2 = 1$. We thus have $\mathbb{P}_\nu(A_b) \ge 1-b$.

We now prove *i*). Since $\int\psi_k = 0$ for all $k = 1,\dots,n$, it holds $\int f_\nu = \int f_0 = 1$ for all ν. Since $\mathrm{Supp}(\psi_k) = B_k$ for all $k = 1,\dots,N$, it holds $f_\nu \equiv f_0$ on B^c and thus f_ν is non-negative on B^c. Now, for $x\in B_k$ it holds

$$f_\nu(x) = f_0(x) + \delta\sum_{j=1}^{N}\frac{\nu_j a_{kj}}{\tilde{\lambda}_j}\psi_k(x) \ge C_0(B) - \frac{\delta\|\psi\|_\infty}{\sqrt{h}}\left|\sum_{j=1}^{N}\frac{\nu_j a_{kj}}{\tilde{\lambda}_j}\right|.$$

Moreover, for any $\nu \in A_b$, we have

$$\frac{\delta\|\psi\|_\infty}{\sqrt{h}}\left|\sum_{j=1}^N \frac{\nu_j a_{kj}}{\tilde{\lambda}_j}\right| \leq \frac{\delta\|\psi\|_\infty}{h}\sqrt{\log\left(\frac{2N}{b}\right)} \leq C_0(B)$$

since δ is assumed to satisfy $\delta \leq \frac{h}{\sqrt{\log(2N/b)}} \min\left\{\frac{C_0(B)}{\|\psi\|_\infty}, \frac{1}{2}\left(1-\frac{L_0}{L}\right)h^\beta\right\}$. Thus, f_ν is non-negative on $\mathbb{R}$ for all $\nu \in A_b$.

To prove *ii*), we have to show that $|f_\nu(x) - f_\nu(y)| \leq L|x-y|^\beta$, for all $\nu \in A_b$, for all $x, y \in \mathbb{R}$. Since $f_\nu \equiv f_0$ on B^c and $f_0 \in H(\beta, L_0)$, this result is trivial for $x, y \in B^c$. If $x \in B_l$ and $y \in B_k$ it holds

$$\begin{aligned}
|f_\nu(x) - f_\nu(y)| &\leq |f_0(x) - f_0(y)| + \left|\delta\sum_{j=1}^N \frac{\nu_j a_{lj}}{\tilde{\lambda}_j}\psi_l(x) - \delta\sum_{j=1}^N \frac{\nu_j a_{kj}}{\tilde{\lambda}_j}\psi_k(y)\right| \\
&\leq L_0|x-y|^\beta + \left|\delta\sum_{j=1}^N \frac{\nu_j a_{lj}}{\tilde{\lambda}_j}\psi_l(x) - \delta\sum_{j=1}^N \frac{\nu_j a_{lj}}{\tilde{\lambda}_j}\psi_l(y)\right| \\
&\qquad + \left|\delta\sum_{j=1}^N \frac{\nu_j a_{kj}}{\tilde{\lambda}_j}\psi_k(x) - \delta\sum_{j=1}^N \frac{\nu_j a_{kj}}{\tilde{\lambda}_j}\psi_k(y)\right| \\
&\leq L_0|x-y|^\beta + \frac{\delta}{\sqrt{h}}\left|\sum_{j=1}^N \frac{\nu_j a_{lj}}{\tilde{\lambda}_j}\right|\left|\psi\left(\frac{x-x_l}{h}\right) - \psi\left(\frac{y-x_l}{h}\right)\right| \\
&\qquad + \frac{\delta}{\sqrt{h}}\left|\sum_{j=1}^N \frac{\nu_j a_{kj}}{\tilde{\lambda}_j}\right|\left|\psi\left(\frac{x-x_k}{h}\right) - \psi\left(\frac{y-x_k}{h}\right)\right| \\
&\leq L_0|x-y|^\beta + \frac{\delta}{h^{\beta+1/2}}\left|\sum_{j=1}^N \frac{\nu_j a_{lj}}{\tilde{\lambda}_j}\right| \cdot L|x-y|^\beta + \frac{\delta}{h^{\beta+1/2}}\left|\sum_{j=1}^N \frac{\nu_j a_{kj}}{\tilde{\lambda}_j}\right| \cdot L|x-y|^\beta \\
&= \left(\frac{L_0}{L} + \frac{\delta}{h^{\beta+1/2}}\left|\sum_{j=1}^N \frac{\nu_j a_{lj}}{\tilde{\lambda}_j}\right| + \frac{\delta}{h^{\beta+1/2}}\left|\sum_{j=1}^N \frac{\nu_j a_{kj}}{\tilde{\lambda}_j}\right|\right) L|x-y|^\beta,
\end{aligned}$$

where we have used $\psi \in H(\beta, L)$. Observe that for all $k = 1, \ldots, n$ and for all $\nu \in A_b$ it holds

$$\frac{\delta}{h^{\beta+1/2}}\left|\sum_{j=1}^N \frac{\nu_j a_{kj}}{\tilde{\lambda}_j}\right| \leq \frac{\delta}{h^{\beta+1}} \cdot \sqrt{\log\left(\frac{2N}{b}\right)} \leq \frac{1}{2}\left(1-\frac{L_0}{L}\right),$$

since δ is assumed to satisfy $\delta \leq \frac{h}{\sqrt{\log(2N/b)}} \min\left\{\frac{C_0(B)}{\|\psi\|_\infty}, \frac{1}{2}\left(1-\frac{L_0}{L}\right)h^\beta\right\}$. Thus, it holds $|f_\nu(x) - f_\nu(y)| \leq L|x-y|^\beta$ for all $\nu \in A_b$, $x \in B_l$ and $y \in B_k$. The case $x \in B^c$ and $y \in B_k$ can be handled in a similar way, which ends the proof of *ii*).

We now prove *iii*). It holds

$$\begin{aligned}\int_{\mathbb{R}} |f_\nu - f_0| &= \int_{\mathbb{R}} \left| \delta \sum_{j=1}^N \frac{\nu_j}{\tilde{\lambda}_j} v_j(x) \right| \mathrm{d}x = \delta \sum_{k=1}^N \int_{B_k} \left| \sum_{j=1}^N \frac{\nu_j}{\tilde{\lambda}_j} v_j(x) \right| \mathrm{d}x \\ &= \delta \sum_{k=1}^N \int_{B_k} \left| \sum_{j=1}^N \frac{\nu_j a_{kj}}{\tilde{\lambda}_j} \psi_k(x) \right| \mathrm{d}x \\ &= \delta \sum_{k=1}^N \left| \sum_{j=1}^N \frac{\nu_j a_{kj}}{\tilde{\lambda}_j} \right| \int_{B_k} |\psi_k(x)| \, \mathrm{d}x \\ &= C_1 \delta \sqrt{h} \sum_{k=1}^N \left| \sum_{j=1}^N \frac{\nu_j a_{kj}}{\tilde{\lambda}_j} \right|,\end{aligned}$$

where $C_1 = \int_{-1}^1 |\psi|$. For all $\nu \in A_b$ it thus holds

$$\int_{\mathbb{R}} |f_\nu - f_0| \geq C_1 \frac{\delta h}{\sqrt{\log\left(\frac{2N}{b}\right)}} \sum_{k=1}^N \left| \sum_{j=1}^N \frac{\nu_j a_{kj}}{\tilde{\lambda}_j} \right|^2.$$

Moreover,

$$\begin{aligned}\sum_{k=1}^N \left| \sum_{j=1}^N \frac{\nu_j a_{kj}}{\tilde{\lambda}_j} \right|^2 &= \sum_{k=1}^N \left(\sum_{j=1}^N \left(\frac{\nu_j a_{kj}}{\tilde{\lambda}_j} \right)^2 + \sum_{j \neq l} \frac{\nu_j a_{kj}}{\tilde{\lambda}_j} \frac{\nu_l a_{kl}}{\tilde{\lambda}_l} \right) \\ &= \sum_{j=1}^N \frac{1}{\tilde{\lambda}_j^2} \sum_{k=1}^N a_{kj}^2 + \sum_{j \neq l} \frac{\nu_j \nu_l}{\tilde{\lambda}_j \tilde{\lambda}_l} \sum_{k=1}^N a_{kj} a_{kl} \\ &= \sum_{j=1}^N \frac{1}{\tilde{\lambda}_j^2},\end{aligned}$$

since the matrix $(a_{kj})_{k,j}$ is orthogonal. Thus, for all $\nu \in A_b$ it holds

$$\|f_\nu - f_0\|_1 \geq C_1 \frac{\delta h}{\sqrt{\log\left(\frac{2N}{b}\right)}} \sum_{j=1}^N \frac{1}{\tilde{\lambda}_j^2}.$$

Set $\mathcal{J} = \{j \in [\![1, N]\!] : z_\alpha^{-1}\lambda_j \geq \sqrt{2h}\}$, we have for all $\nu \in A_b$

$$\begin{aligned}
\|f_\nu - f_0\|_1 &\geq C_1 \frac{\delta h}{\sqrt{\log\left(\frac{2N}{b}\right)}} \sum_{j=1}^{N} \left(\frac{1}{2h} I(z_\alpha^{-1}\lambda_j < \sqrt{2h}) + \frac{z_\alpha^2}{\lambda_j^2} I(z_\alpha^{-1}\lambda_j \geq \sqrt{2h}) \right) \\
&= C_1 \frac{\delta h}{\sqrt{\log\left(\frac{2N}{b}\right)}} \left(\frac{1}{2h}(N - |\mathcal{J}|) + \sum_{j\in\mathcal{J}} \frac{z_\alpha^2}{\lambda_j^2} \right) \\
&\geq C_1 \frac{\delta h}{\sqrt{\log\left(\frac{2N}{b}\right)}} \left(\frac{N}{2h} - \frac{|\mathcal{J}|}{2h} + z_\alpha^2 |\mathcal{J}|^2 \left(\sum_{j\in\mathcal{J}} \lambda_j^2 \right)^{-1} \right) \\
&= C_1 \frac{\delta N}{2\sqrt{\log\left(\frac{2N}{b}\right)}} \left(1 - \frac{|\mathcal{J}|}{N} + \left(\frac{|\mathcal{J}|}{N}\right)^2 |B| z_\alpha^2 \left(\sum_{j\in\mathcal{J}} \lambda_j^2 \right)^{-1} \right),
\end{aligned}$$

where the second to last inequality follows from the inequality between harmonic and artithmetic means. Now,

$$\begin{aligned}
\sum_{j\in\mathcal{J}} \lambda_j^2 \leq \sum_{j=1}^{N} \lambda_j^2 &= \sum_{j=1}^{N} \langle K v_j, v_j \rangle \\
&= \sum_{j=1}^{N} \left\langle \frac{1}{n} \sum_{i=1}^{n} \int_{\mathbb{R}} \left(\int_{\mathcal{Z}_i} \frac{q_i(z_i \mid y) q_i(z_i \mid \cdot) \mathbb{1}_B(y) \mathbb{1}_B(\cdot)}{g_{0,i}(z_i)} \mathrm{d}\mu_i(z_i) \right) v_j(y) \mathrm{d}y, v_j \right\rangle \\
&= \frac{1}{n} \sum_{i=1}^{n} \int_{\mathcal{Z}_i} \sum_{j=1}^{N} \left(\int_{\mathbb{R}} \int_{\mathbb{R}} \frac{q_i(z_i \mid y) q_i(z_i \mid x) \mathbb{1}_B(y) \mathbb{1}_B(x)}{g_{0,i}(z_i)} v_j(x) v_j(y) \mathrm{d}x \mathrm{d}y \right) \mathrm{d}\mu_i(z_i) \\
&= \frac{1}{n} \sum_{i=1}^{n} \int_{\mathcal{Z}_i} \sum_{j=1}^{N} \left(\int_{\mathbb{R}} \frac{q_i(z_i \mid x) \mathbb{1}_B(x)}{g_{0,i}(z_i)} v_j(x) \mathrm{d}x \right)^2 g_{0,i}(z_i) \mathrm{d}\mu_i(z_i) \\
&= \frac{1}{n} \sum_{i=1}^{n} \int_{\mathcal{Z}_i} \sum_{j=1}^{N} \left(\int_{\mathbb{R}} \left(\frac{q_i(z_i \mid x)}{g_{0,i}(z_i)} - e^{-2\alpha} \right) \mathbb{1}_B(x) v_j(x) \mathrm{d}x \right)^2 g_{0,i}(z_i) \mathrm{d}\mu_i(z_i),
\end{aligned}$$

since $\int \mathbb{1}_B(x) v_j(x) dx = 0$. Recall that q_i satisfies $e^{-\alpha} \leq q_i(z_i \mid x) \leq e^\alpha$ for all $z_i \in \mathcal{Z}_i$ and all $x \in \mathbb{R}$. This implies $e^{-\alpha} \leq g_{0,i}(z_i) \leq e^\alpha$, and therefore $0 \leq f_{i,z_i}(x) := \frac{q_i(z_i|x)}{g_{0,i}(z_i)} - e^{-2\alpha} \leq z_\alpha$.

Writing $f_{i,z_i,B} = \mathbb{1}_B \cdot f_{i,z_i}$, we have

$$\sum_{j=1}^{N}\left(\int_{\mathbb{R}}\left(\frac{q_i(z_i \mid x)}{g_{0,i}(z_i)} - e^{-2\alpha}\right)\mathbb{1}_B(x)v_j(x)\mathrm{d}x\right)^2 = \sum_{j=1}^{N}\langle f_{i,z_i,B}, v_j\rangle^2 = \left\|\sum_{j=1}^{N}\langle f_{i,z_i,B}, v_j\rangle v_j\right\|_2^2$$
$$= \left\|\mathrm{Proj}_{\mathrm{Vect}(v_1,\dots,v_N)}(f_{i,z_i,B})\right\|_2^2$$
$$\leq \|f_{i,z_i,B}\|_2^2 \leq z_\alpha^2|B|.$$

Moreover, $\int_{\mathcal{Z}_i} g_{0,i}(z_i)\mathrm{d}\mu_i(z_i) = \int_{\mathbb{R}}(\int_{\mathcal{Z}_i} q_i(z_i \mid x)\mathrm{d}\mu_i(z_i))f_0(x)\mathrm{d}x = \int_{\mathbb{R}} f_0 = 1$. This gives $\sum_{j\in\mathcal{J}}\lambda_j^2 \leq z_\alpha^2|B|$ and for all $\nu \in A_b$

$$\|f_\nu - f_0\|_1 \geq C_1\frac{\delta N}{2\sqrt{\log\left(\frac{2N}{b}\right)}}\left(1 - \frac{|\mathcal{J}|}{N} + \left(\frac{|\mathcal{J}|}{N}\right)^2\right) \geq \frac{3C_1}{8}\frac{\delta N}{\sqrt{\log\left(\frac{2N}{b}\right)}}.$$

4.7 Appendix : Proofs of Section 4.4

4.7.1 Proof of Proposition 4.4.1

Let $i \in [\![1, n]\!]$. Since Z_i depends only on X_i, condition (4.1) reduces to

$$\frac{q^{Z_i|X_i=y}(z)}{q^{Z_i|X_i=y'}(z)} \leq e^\alpha, \quad \forall y, y' \in \mathbb{R}, \forall z \in \mathbb{R}^N, \tag{4.17}$$

where $q^{Z_i|X_i=y}$ denotes the conditional density of Z_i given $X_i = y$. It holds

$$q^{Z_i|X_i=y}(z) = \prod_{j=1}^{N}\frac{\alpha}{4}\exp\left(-\frac{\alpha|z_j - I(y \in B_j)|}{2}\right).$$

Thus, by the reverse and the ordinary triangle inequality,

$$\begin{aligned}\frac{q^{Z_i|X_i=y}(z)}{q^{Z_i|X_i=y'}(z)} &= \prod_{j=1}^{N} \exp\left(\frac{\alpha\left[|z_j - I(y' \in B_j)| - |z_j - I(y \in B_j)|\right]}{2}\right) \\ &\leq \prod_{j=1}^{N} \exp\left(\frac{\alpha|I(y \in B_j) - I(y' \in B_j)|}{2}\right) \\ &= \exp\left(\frac{\alpha}{2}\sum_{j=1}^{N}|I(y \in B_j) - I(y' \in B_j)|\right) \\ &\leq \exp(\alpha),\end{aligned}$$

which proves (4.17).
Consider now $i \in [\![n+1, 2n]\!]$. Since Z_i depends only on X_i and on $Z_1, \ldots, Z_n$, condition (4.1) reduces for $i \in [\![n+1, 2n]\!]$ to

$$\frac{\mathbb{P}\left(Z_i = z \mid X_i \in A, Z_1 = z_1, \ldots, Z_n = z_n\right)}{\mathbb{P}\left(Z_i = z \mid X_i \in F, Z_1 = z_1, \ldots, Z_n = z_n\right)} \in [e^{-\alpha}, e^{\alpha}] \tag{4.18}$$

for all $z \in \{-c_\alpha\tau, c_\alpha\tau\}$, $A, F \in \{\overline{B}, B_1, \ldots, B_N\}$ and $z_1, \ldots, z_n \in \mathbb{R}^N$. For all $j, k \in [\![1, N]\!]$, for all $z_1, \ldots, z_n$ it holds

$$\frac{\mathbb{P}\left(Z_i = c_\alpha\tau \mid X_i \in B_j, Z_1 = z_1, \ldots, Z_n = z_n\right)}{\mathbb{P}\left(Z_i = c_\alpha\tau \mid X_i \in B_k, Z_1 = z_1, \ldots, Z_n = z_n\right)} = \frac{1 + \frac{[\hat{p}_j - p_0(j)]_{-\tau}^{\tau}}{c_\alpha\tau}}{1 + \frac{[\hat{p}_k - p_0(k)]_{-\tau}^{\tau}}{c_\alpha\tau}} \in \left[\frac{c_\alpha - 1}{c_\alpha + 1}, \frac{c_\alpha + 1}{c_\alpha - 1}\right] = [e^{-\alpha}, e^{\alpha}],$$

and a similar result holds for $z = -c_\alpha\tau$. For all $j \in [\![1, N]\!]$, for all $z_1, \ldots, z_n$ it holds

$$\frac{\mathbb{P}\left(Z_i = c_\alpha\tau \mid X_i \in B_j, Z_1 = z_1, \ldots, Z_n = z_n\right)}{\mathbb{P}\left(Z_i = c_\alpha\tau \mid X_i \in \overline{B}, Z_1 = z_1, \ldots, Z_n = z_n\right)} = 1 + \frac{[\hat{p}_j - p_0(j)]_{-\tau}^{\tau}}{c_\alpha\tau} \in \left[1 - \frac{1}{c_\alpha}, 1 + \frac{1}{c_\alpha}\right] \subset [e^{-\alpha}, e^{\alpha}],$$

and a similar result holds for $z = -c_\alpha\tau$. This ends the proof of (4.18).
Consider now $i \in [\![2n+1, 3n]\!]$. Since Z_i depends only on X_i, condition (4.1) reduces for $i \in [\![2n+1, 3n]\!]$ to

$$\frac{\mathbb{P}\left(Z_i = z \mid X_i \in A\right)}{\mathbb{P}\left(Z_i = z \mid X_i \in F\right)} \in [e^{-\alpha}, e^{\alpha}], \quad \forall A, F \in \{\overline{B}, B_1, \ldots, B_N\}, \forall z \in \{-c_\alpha, c_\alpha\}.$$

We have already proved this in the proof of Proposition 4.3.2.

4.7.2 Analysis of the mean and variance of the statistic D_B

Proof of Proposition 4.4.2. 1. For all $i \in [\![n+1, 2n]\!]$ it holds

$$\begin{aligned}
&\mathbb{P}\left(Z_i = \pm c_\alpha \tau \mid Z_1, \dots, Z_n\right) \\
&\quad = \sum_{j=1}^{N} \mathbb{P}\left(Z_i = \pm c_\alpha \tau \mid X_i \in B_j\right) \mathbb{P}(X_i \in B_j) + \mathbb{P}\left(Z_i = \pm c_\alpha \tau \mid X_i \in \bar{B}\right) \mathbb{P}(X_i \in \bar{B}) \\
&\quad = \sum_{j=1}^{N} \frac{1}{2} \left(1 \pm \frac{[\widehat{p}_j - p_0(j)]_{-\tau}^{\tau}}{c_\alpha \tau}\right) p(j) + \frac{1}{2} \int_{\bar{B}} f.
\end{aligned}$$

For $i \in [\![n+1, 2n]\!]$ we thus have

$$\begin{aligned}
\mathbb{E}[Z_i \mid Z_1, \dots, Z_n] &= c_\alpha \tau \mathbb{P}(Z_i = c_\alpha \tau \mid Z_1, \dots, Z_n) - c_\alpha \tau \mathbb{P}(Z_i = -c_\alpha \tau \mid Z_1, \dots, Z_n) \\
&= \sum_{j=1}^{N} p(j) [\widehat{p}_j - p_0(j)]_{-\tau}^{\tau}.
\end{aligned}$$

Thus,

$$\mathbb{E}[D_B] = \mathbb{E}\left[\mathbb{E}[D_B \mid Z_1, \dots, Z_n]\right] = \sum_{j=1}^{N} \{p(j) - p_0(j)\} \mathbb{E}\left[[\widehat{p}_j - p_0(j)]_{-\tau}^{\tau}\right].$$

The proof of (4.11) is similar to the proof of Theorem 3 in [10].

2. Write

$$\mathrm{Var}(D_B) = \mathbb{E}\left[\mathrm{Var}\left(D_B \mid Z_1, \dots, Z_n\right)\right] + \mathrm{Var}\left(\mathbb{E}\left[D_B \mid Z_1, \dots, Z_n\right]\right).$$

It holds

$$\mathbb{E}\left[D_B \mid Z_1, \dots, Z_n\right] = \sum_{j=1}^{N} \{p(j) - p_0(j)\} [\widehat{p}_j - p_0(j)]_{-\tau}^{\tau},$$

and

$$\begin{aligned}
\mathrm{Var}\left(D_B \mid Z_1,\dots,Z_n\right) &= \mathrm{Var}\left(\frac{1}{n}\sum_{i=n+1}^{2n} Z_i - \sum_{j=1}^{N} p_0(j)[\widehat{p}_j - p_0(j)]_{-\tau}^{\tau} \mid Z_1,\dots,Z_n\right)\\
&= \mathrm{Var}\left(\frac{1}{n}\sum_{i=n+1}^{2n} Z_i \mid Z_1,\dots,Z_n\right)\\
&= \frac{1}{n^2}\sum_{i=n+1}^{2n} \mathrm{Var}\left(Z_i \mid Z_1,\dots,Z_n\right)\\
&\leq \frac{1}{n^2}\sum_{i=n+1}^{2n} \mathbb{E}\left[Z_i^2 \mid Z_1,\dots,Z_n\right]\\
&\leq \frac{c_\alpha^2\tau^2}{n},
\end{aligned}$$

where we have used the independence of the random variables $(Z_i)_{i=n+1,\dots,2n}$ conditionnally on $Z_1,\dots,Z_n$. This gives

$$\begin{aligned}
\mathrm{Var}(D_B) \leq \frac{c_\alpha^2\tau^2}{n} &+ \sum_{j=1}^{N}\{p(j)-p_0(j)\}^2\mathrm{Var}\left([\widehat{p}_j - p_0(j)]_{-\tau}^{\tau}\right)\\
&+ \sum_{j_1\neq j_2}\{p(j_1)-p_0(j_1)\}\{p(j_2)-p_0(j_2)\}\mathrm{Cov}([\widehat{p}_{j_1} - p_0(j_1)]_{-\tau}^{\tau}, [\widehat{p}_{j_2} - p_0(j_2)]_{-\tau}^{\tau}).
\end{aligned}$$

Set $P_j = [\widehat{p}_j - p_0(j)]_{-\tau}^{\tau}$. We will prove that

$$\mathrm{Var}(P_j) \leq \frac{10}{n\alpha^2}\exp\left(-\frac{n\alpha^2(p(j)-p_0(j))^2}{168}\right), \quad \forall j \in [\![1,N]\!], \tag{4.19}$$

and

$$|\mathrm{Cov}(P_{j_1}, P_{j_2})| \leq \frac{2p(j_1)p(j_2)}{n}\exp\left(-\frac{n\alpha^2\left[(p(j_1)-p_0(j_1))^2 + (p(j_2)-p_0(j_2))^2\right]}{336}\right) \tag{4.20}$$

for all $j_1, j_2 \in [\![1,N]\!]$, $j_1 \neq j_2$. We admit these results for the moment and finish the proof

of Proposition 4.4.2. Using (4.19) and (4.20) we obtain

$$\begin{aligned}
\mathrm{Var}(D_B) &\leq \frac{c_\alpha^2\tau^2}{n} + \frac{10}{n\alpha^2}\sum_{j=1}^{N}\{p(j)-p_0(j)\}^2 \exp\left(-\frac{n\alpha^2(p(j)-p_0(j))^2}{168}\right) \\
&\qquad + \frac{2}{n}\left[\sum_{j=1}^{N}|p(j)-p_0(j)|p(j)\exp\left(-\frac{n\alpha^2(p(j)-p_0(j))^2}{336}\right)\right]^2 \\
&\leq \frac{c_\alpha^2\tau^2}{n} + \frac{10}{n\alpha^2}\sum_{j=1}^{N}\{p(j)-p_0(j)\}^2 \exp\left(-\frac{n\alpha^2(p(j)-p_0(j))^2}{168}\right) \\
&\qquad + \frac{2}{n}\left[\sum_{j=1}^{N}p(j)^2\right]\left[\sum_{j=1}^{N}|p(j)-p_0(j)|^2\exp\left(-\frac{n\alpha^2(p(j)-p_0(j))^2}{168}\right)\right] \\
&\leq \frac{c_\alpha^2\tau^2}{n} + \frac{12}{n\alpha^2}\sum_{j=1}^{N}|p(j)-p_0(j)|^2\exp\left(-\frac{n\alpha^2(p(j)-p_0(j))^2}{168}\right),
\end{aligned}$$

where the second to last inequality follows from Cauchy Schwarz inequality. Now, observe that if $a_j := |p(j)-p_0(j)| \neq 0$, then we can write

$$|p(j)-p_0(j)|\exp\left(-\frac{n\alpha^2(p(j)-p_0(j))^2}{168}\right) = \min\{\tau, a_j\}\cdot\frac{a_j/\tau}{\min\{1, a_j/\tau\}}\exp\left(-\frac{1}{168}\left(\frac{a_j}{\tau}\right)^2\right),$$

where we recall that $\tau = 1/\sqrt{n\alpha^2}$. The study of the function $g : x \mapsto [x/\min\{1,x\}]\exp(-x^2/168)$ gives $g(x) \leq \sqrt{84}e^{-1/2}$ for all $x \geq 0$. We thus have

$$\mathrm{Var}(D_B) \leq \frac{c_\alpha^2\tau^2}{n} + \frac{12e^{-1/2}\sqrt{84}}{n\alpha^2}\sum_{j=1}^{N}|p(j)-p_0(j)|\min\left\{\tau, |p(j)-p_0(j)|\right\}.$$

Using that $\alpha^2 c_\alpha^2 \leq 5$ for all $\alpha \in (0,1)$, we finally obtain the claim of Proposition 4.4.2,

$$\mathrm{Var}(D_B) \leq \frac{5}{(n\alpha^2)^2} + \frac{67}{n\alpha^2}D_\tau(f).$$

It remains now to prove (4.19) and (4.20). We will use the following concentration inequality which is an application of Bernstein's inequality (see for instance Corollary 2.11 in [11])

$$\mathbb{P}\left(|\widehat{p}_j - p(j)| \geq x\right) \leq 2\exp\left(-\frac{n\alpha^2x^2}{42}\right), \quad \text{for all } 0 < x \leq \frac{1}{\alpha}. \tag{4.21}$$

Let us prove (4.19). Let $j \in [\![1, N]\!]$. We first deal with the case where $p(j) - p_0(j) \geq 2\tau$.

We have

$$\begin{aligned}
\mathrm{Var}\left([\widehat{p}_j - p_0(j)]_{-\tau}^{\tau}\right) &= \mathrm{Var}\left([\widehat{p}_j - p_0(j)]_{-\tau}^{\tau} - \tau\right) \\
&\leq \mathbb{E}\left[\left([\widehat{p}_j - p_0(j)]_{-\tau}^{\tau} - \tau\right)^2\right] \\
&= \mathbb{E}\left[(-2\tau)^2 \mathbb{1}\left(\widehat{p}_j - p_0(j) \leq -\tau\right) + (\widehat{p}_j - p_0(j) - \tau)^2 \mathbb{1}\left(\widehat{p}_j - p_0(j) \in [-\tau, \tau]\right)\right] \\
&\leq 4\tau^2 \mathbb{P}\left(\widehat{p}_j - p_0(j) \leq \tau\right) \\
&= 4\tau^2 \mathbb{P}\left(p(j) - \widehat{p}_j \geq p(j) - p_0(j) - \tau\right) \\
&\leq 4\tau^2 \mathbb{P}\left(|p(j) - \widehat{p}_j| \geq p(j) - p_0(j) - \tau\right)
\end{aligned}$$

Now, if $p(j) - p_0(j) \geq 2\tau$ then we have $0 < p(j) - p_0(j) - \tau \leq p(j) \leq 1 \leq 1/\alpha$ and (4.21) gives

$$\begin{aligned}
\mathrm{Var}\left([\widehat{p}_j - p_0(j)]_{-\tau}^{\tau}\right) &\leq 8\tau^2 \exp\left(-\frac{n\alpha^2 \left\{p(j) - p_0(j) - \tau\right\}^2}{42}\right) \\
&\leq \frac{8}{n\alpha^2} \exp\left(-\frac{n\alpha^2 \left\{p(j) - p_0(j)\right\}^2}{168}\right),
\end{aligned}$$

which ends the proof of (4.19) for the elements $j \in [\![1, N]\!]$ such that $p(j) - p_0(j) \geq 2\tau$. Starting from $\mathrm{Var}\left([\widehat{p}_j - p_0(j)]_{-\tau}^{\tau}\right) = \mathrm{Var}\left([\widehat{p}_j - p_0(j)]_{-\tau}^{\tau} + \tau\right)$, a similar proof gives (4.19) for the elements $j \in [\![1, N]\!]$ such that $p(j) - p_0(j) \leq -2\tau$. It remains to deal with the case $|p(j) - p_0(j)| < 2\tau$. In this case, using that $[\cdot]_{-\tau}^{\tau}$ is Lipschitz continuous with Lipschitz

constant 1 we have

$$\begin{aligned}
\mathrm{Var}\left([\widehat{p}_j - p_0(j)]_{-\tau}^{\tau}\right) &= \mathrm{Var}\left([\widehat{p}_j - p_0(j)]_{-\tau}^{\tau} - [p_j - p_0(j)]_{-\tau}^{\tau}\right) \\
&\leq \mathbb{E}\left[\left([\widehat{p}_j - p_0(j)]_{-\tau}^{\tau} - [p_j - p_0(j)]_{-\tau}^{\tau}\right)^2\right] \\
&\leq \mathbb{E}\left[|\widehat{p}_j - p(j)|^2\right] \\
&= \mathrm{Var}(\widehat{p}_j) \\
&= \frac{1}{n^2}\sum_{i=1}^{n}\mathrm{Var}\left(I(X_i \in B_j)\right) + \frac{4}{n^2\alpha^2}\sum_{i=1}^{n}\mathrm{Var}(W_{ij}) \\
&\leq \frac{9}{n\alpha^2} \\
&= \frac{9}{n\alpha^2}\exp\left(\frac{n\alpha^2\left\{p(j) - p_0(j)\right\}^2}{168}\right)\exp\left(-\frac{n\alpha^2\left\{p(j) - p_0(j)\right\}^2}{168}\right) \\
&\leq \frac{9\exp(1/42)}{n\alpha^2}\exp\left(-\frac{n\alpha^2\left\{p(j) - p_0(j)\right\}^2}{168}\right),
\end{aligned}$$

where the last inequality follows from the assumption $|p(j) - p_0(j)| \leq 2\tau = 2/\sqrt{n\alpha^2}$. This ends the proof of (4.19). We now prove (4.20). For all $i \in [\![1, n+1]\!]$, we will write

$$\begin{aligned}
\mathbb{E}_i\left[\cdot\right] &= \mathbb{E}\left[\cdot \mid X_1, \ldots, X_{i-1}\right], \\
\mathbb{E}_i^j\left[\cdot\right] &= \frac{1}{p(j)}\mathbb{E}\left[\cdot \mathbb{1}(X_i \in B_j) \mid X_1, \ldots, X_{i-1}\right], \\
\mathbb{E}_i^{comp}\left[\cdot\right] &= \frac{1}{p\left(\overline{B}\right)}\mathbb{E}\left[\cdot \mathbb{1}(X_i \in \overline{B}) \mid X_1, \ldots, X_{i-1}\right].
\end{aligned}$$

Observe that

$$\mathbb{E}_i^j\left[P_{j_1}\right] \overset{a.s.}{=} \mathbb{E}_i^{j_2}\left[P_{j_1}\right], \quad \forall j, j_2 \neq j_1, \tag{4.22}$$

and

$$\mathbb{E}_i^{comp}\left[P_{j_1}\right] \overset{a.s.}{=} \mathbb{E}_i^{j_2}\left[P_{j_1}\right], \quad \forall j_2 \neq j_1, \tag{4.23}$$

where we recall that $P_j = [\widehat{p}_j - p_0(j)]_{-\tau}^{\tau}$. Let $j_1, j_2 \in [\![1, N]\!]$, $j_1 \neq j_2$. We have

$$\begin{aligned}
\mathrm{Cov}\left(P_{j_1}, P_{j_2}\right) &= \mathrm{Cov}\left(\mathbb{E}_{n+1}\left[P_{j_1}\right], \mathbb{E}_{n+1}\left[P_{j_2}\right]\right) \\
&= \mathbb{E}\left[\mathbb{E}_{n+1}\left[P_{j_1}\right]\mathbb{E}_{n+1}\left[P_{j_2}\right]\right] - \mathbb{E}\left[P_{j_1}\right]\mathbb{E}\left[P_{j_2}\right] \\
&= \mathbb{E}\left[\sum_{i=1}^{n}\left(\mathbb{E}_{i+1}\left[P_{j_1}\right]\mathbb{E}_{i+1}\left[P_{j_2}\right] - \mathbb{E}_i\left[P_{j_1}\right]\mathbb{E}_i\left[P_{j_2}\right]\right)\right],
\end{aligned}$$

where the sum in the last line is a telescoping sum. We thus have

$$\mathrm{Cov}\left(P_{j_1}, P_{j_2}\right) = \sum_{i=1}^{n} \mathbb{E}\left[\mathbb{E}_{i+1}\left[P_{j_1}\right]\mathbb{E}_{i+1}\left[P_{j_2}\right] - \mathbb{E}_i\left[P_{j_1}\right]\mathbb{E}_i\left[P_{j_2}\right]\right]. \tag{4.24}$$

Now, it holds

$$\begin{aligned}
\mathbb{E}_i\left[P_{j_1}\right] &= \mathbb{E}\left[P_{j_1} \mid X_1, \dots, X_{i-1}\right] \\
&= \mathbb{E}\left[P_{j_1} \cdot \left(\sum_{j=1}^{N} \mathbb{1}(X_i \in B_j) + \mathbb{1}(X_i \in \overline{B})\right) \mid X_1, \dots, X_{i-1}\right] \\
&= \sum_{j=1}^{N} p(j)\mathbb{E}_i^j\left[P_{j_1}\right] + p\left(\overline{B}\right)\mathbb{E}_i^{comp}\left[P_{j_1}\right] \\
&= p(j_1)\mathbb{E}_i^{j_1}\left[P_{j_1}\right] + \sum_{\substack{j=1 \\ j\neq j_1}}^{N} p(j)\mathbb{E}_i^{j_2}\left[P_{j_1}\right] + p\left(\overline{B}\right)\mathbb{E}_i^{j_2}\left[P_{j_1}\right],
\end{aligned}$$

where the last equality follows from (4.22) and (4.23). We thus obtain

$$\mathbb{E}_i\left[P_{j_1}\right] = p(j_1)\mathbb{E}_i^{j_1}\left[P_{j_1}\right] + (1 - p(j_1))\mathbb{E}_i^{j_2}\left[P_{j_1}\right]. \tag{4.25}$$

Similarly, it holds

$$\mathbb{E}_i\left[P_{j_2}\right] = p(j_2)\mathbb{E}_i^{j_2}\left[P_{j_2}\right] + (1 - p(j_2))\mathbb{E}_i^{j_1}\left[P_{j_2}\right]. \tag{4.26}$$

We now compute $\mathbb{E}_{X_i}\left[\mathbb{E}_{i+1}\left[P_{j_1}\right]\mathbb{E}_{i+1}\left[P_{j_2}\right]\right]$. We have

$$\begin{aligned}
&\mathbb{E}_{X_i}\left[\mathbb{E}_{i+1}\left[P_{j_1}\right]\mathbb{E}_{i+1}\left[P_{j_2}\right]\right] \\
&= \int_{\mathbb{R}} f(y_i)\left[\int_{\mathbb{R}^{n-i}} P_{j_1}(X_1, \dots, X_{i-1}, y_i, y_{i+1}, \dots y_n) f(y_{i+1}) \cdots f(y_n) \mathrm{d}y_{i+1} \cdots \mathrm{d}y_n \right. \\
&\qquad \left. \cdot \int_{\mathbb{R}^{n-i}} P_{j_2}(X_1, \dots, X_{i-1}, y_i, y'_{i+1}, \dots y'_n) f(y'_{i+1}) \cdots f(y'_n) \mathrm{d}y'_{i+1} \cdots \mathrm{d}y'_n\right] \mathrm{d}y_i \\
&= \sum_{j=1}^{N} \int_{\mathbb{R}} f(y_i)\mathbb{1}(y_i \in B_j)\left[\int_{\mathbb{R}^{n-i}} P_{j_1}(X_1, \dots, X_{i-1}, y_i, y_{i+1}, \dots y_n) f(y_{i+1}) \cdots f(y_n) \mathrm{d}y_{i+1} \cdots \mathrm{d}y_n \right. \\
&\qquad \left. \cdot \int_{\mathbb{R}^{n-i}} P_{j_2}(X_1, \dots, X_{i-1}, y_i, y'_{i+1}, \dots y'_n) f(y'_{i+1}) \cdots f(y'_n) \mathrm{d}y'_{i+1} \cdots \mathrm{d}y'_n\right] \mathrm{d}y_i \\
&\quad + \int_{\mathbb{R}} f(y_i)\mathbb{1}(y_i \in \overline{B})\left[\int_{\mathbb{R}^{n-i}} P_{j_1}(X_1, \dots, X_{i-1}, y_i, y_{i+1}, \dots y_n) f(y_{i+1}) \cdots f(y_n) \mathrm{d}y_{i+1} \cdots \mathrm{d}y_n \right. \\
&\qquad \left. \cdot \int_{\mathbb{R}^{n-i}} P_{j_2}(X_1, \dots, X_{i-1}, y_i, y'_{i+1}, \dots y'_n) f(y'_{i+1}) \cdots f(y'_n) \mathrm{d}y'_{i+1} \cdots \mathrm{d}y'_n\right] \mathrm{d}y_i
\end{aligned}$$

For $j = 1, \dots, N$, let x_j be such that $B_j = [x_j - h, x_j + h]$. Observe that if $y_i \in \mathring{B}_j$ then it holds $\mathbb{1}(y_i \in B_k) = \delta_{j,k} = \mathbb{1}(x_j \in B_k)$ where δ is the Kronecker delta. Observe also that if $y_i \in \overline{B}$ then it holds $\mathbb{1}(y_i \in B_k) = 0 = \mathbb{1}(z \in B_k)$ for some $z \in \overline{B}$. This gives

$$P_k\left(X_1, \dots, X_{i-1}, y_i, y_{i+1}, \dots, y_n\right) \mathbb{1}(y_i \in \mathring{B}_j) = P_k\left(X_1, \dots, X_{i-1}, x_j, y_{i+1}, \dots, y_n\right) \mathbb{1}(y_i \in \mathring{B}_j), \tag{4.27}$$

and

$$P_k\left(X_1, \dots, X_{i-1}, y_i, y_{i+1}, \dots, y_n\right) \mathbb{1}(y_i \in \overline{B}) = P_k\left(X_1, \dots, X_{i-1}, z, y_{i+1}, \dots, y_n\right) \mathbb{1}(y_i \in \overline{B}). \tag{4.28}$$

We thus have

$$\begin{aligned}
&\mathbb{E}_{X_i}\left[\mathbb{E}_{i+1}\left[P_{j_1}\right]\mathbb{E}_{i+1}\left[P_{j_2}\right]\right] \\
&= \sum_{j=1}^{N} p(j) \left[\int_{\mathbb{R}^{n-i}} P_{j_1}(X_1, \dots, X_{i-1}, x_j, y_{i+1}, \dots y_n) f(y_{i+1}) \cdots f(y_n) \mathrm{d}y_{i+1} \cdots \mathrm{d}y_n \right. \\
&\qquad\qquad \left. \cdot \int_{\mathbb{R}^{n-i}} P_{j_2}(X_1, \dots, X_{i-1}, x_j, y'_{i+1}, \dots y'_n) f(y'_{i+1}) \cdots f(y'_n) \mathrm{d}y'_{i+1} \cdots \mathrm{d}y'_n \right] \\
&\quad + p(\overline{B}) \left[\int_{\mathbb{R}^{n-i}} P_{j_1}(X_1, \dots, X_{i-1}, z, y_{i+1}, \dots y_n) f(y_{i+1}) \cdots f(y_n) \mathrm{d}y_{i+1} \cdots \mathrm{d}y_n \right. \\
&\qquad\qquad \left. \cdot \int_{\mathbb{R}^{n-i}} P_{j_2}(X_1, \dots, X_{i-1}, z, y'_{i+1}, \dots y'_n) f(y'_{i+1}) \cdots f(y'_n) \mathrm{d}y'_{i+1} \cdots \mathrm{d}y'_n \right].
\end{aligned}$$

Now, observe that

$$\int_{\mathbb{R}^{n-i}} P_k(X_1, \dots, X_{i-1}, x_j, y_{i+1}, \dots y_n) f(y_{i+1}) \cdots f(y_n) \mathrm{d}y_{i+1} \cdots \mathrm{d}y_n = \mathbb{E}_i^j[P_k]. \tag{4.29}$$

Indeed, it holds

$$\begin{aligned}
\mathbb{E}_i^j[P_k] &= \frac{1}{p(j)} \mathbb{E}\left[P_k \mathbb{1}(X_i \in B_j) \mid X_1, \dots, X_{i-1}\right] \\
&= \frac{1}{p(j)} \int_{\mathbb{R}^{n-i+1}} P_k(X_1, \dots, X_{i-1}, y_i, y_{i+1}, \dots, y_n) \mathbb{1}(y_i \in B_j) f(y_i) f(y_{i+1}) \cdots f(y_n) \mathrm{d}y_i \mathrm{d}y_{i+1} \mathrm{d}y_n \\
&= \int_{\mathbb{R}^{n-i}} P_k(X_1, \dots, X_{i-1}, x_j, y_{i+1}, \dots, y_n) f(y_{i+1}) \cdots f(y_n) \mathrm{d}y_{i+1} \mathrm{d}y_n,
\end{aligned}$$

where the last equality follows from (4.27). Similarly, using (4.28) one can prove that for $z \in \overline{B}$ it holds

$$\int_{\mathbb{R}^{n-i}} P_k(X_1, \dots, X_{i-1}, z, y_{i+1}, \dots y_n) f(y_{i+1}) \cdots f(y_n) \mathrm{d}y_{i+1} \cdots \mathrm{d}y_n = \mathbb{E}_i^{comp}[P_k].$$

We thus have

$$\mathbb{E}_{X_i}\left[\mathbb{E}_{i+1}\left[P_{j_1}\right]\mathbb{E}_{i+1}\left[P_{j_2}\right]\right] = \sum_{j=1}^{N} p(j)\mathbb{E}_i^j[P_{j_1}]\mathbb{E}_i^j[P_{j_2}] + p(\overline{B})\mathbb{E}_i^{comp}[P_{j_1}]\mathbb{E}_i^{comp}[P_{j_2}],$$

and, using (4.22) and (4.23) we finally obtain

$$\begin{aligned}\mathbb{E}_{X_i}\left[\mathbb{E}_{i+1}\left[P_{j_1}\right]\mathbb{E}_{i+1}\left[P_{j_2}\right]\right] &= p(j_1)\mathbb{E}_i^{j_1}\left[P_{j_1}\right]\mathbb{E}_i^{j_1}\left[P_{j_2}\right] + p(j_2)\mathbb{E}_i^{j_2}\left[P_{j_1}\right]\mathbb{E}_i^{j_2}\left[P_{j_2}\right] \\ &\quad + \left(1 - p(j_1) - p(j_2)\right)\mathbb{E}_i^{j_2}\left[P_{j_1}\right]\mathbb{E}_i^{j_1}\left[P_{j_2}\right]. \quad (4.30)\end{aligned}$$

Putting (4.25), (4.26) and (4.30) in (4.24), we obtain

$$\begin{aligned}&\mathrm{Cov}\left(P_{j_1}, P_{j_2}\right) \\ &= \sum_{i=1}^{n} \mathbb{E}\Big[p(j_1)\mathbb{E}_i^{j_1}\left[P_{j_1}\right]\mathbb{E}_i^{j_1}\left[P_{j_2}\right] + p(j_2)\mathbb{E}_i^{j_2}\left[P_{j_1}\right]\mathbb{E}_i^{j_2}\left[P_{j_2}\right] + \left(1 - p(j_1) - p(j_2)\right)\mathbb{E}_i^{j_2}\left[P_{j_1}\right]\mathbb{E}_i^{j_1}\left[P_{j_2}\right] \\ &\qquad + \Big\{p(j_1)\mathbb{E}_i^{j_1}\left[P_{j_1}\right] + \left(1 - p(j_1)\right)\mathbb{E}_i^{j_2}\left[P_{j_1}\right]\Big\}\Big\{p(j_2)\mathbb{E}_i^{j_2}\left[P_{j_2}\right] + \left(1 - p(j_2)\right)\mathbb{E}_i^{j_1}\left[P_{j_2}\right]\Big\}\Big] \\ &= \sum_{i=1}^{n} p(j_1)p(j_2)\mathbb{E}\left[\left(\mathbb{E}_i^{j_1}\left[P_{j_1}\right] - \mathbb{E}_i^{j_2}\left[P_{j_1}\right]\right)\left(\mathbb{E}_i^{j_1}\left[P_{j_2}\right] - \mathbb{E}_i^{j_2}\left[P_{j_2}\right]\right)\right],\end{aligned}$$

and Cauchy-Schwarz inequality gives

$$\left|\mathrm{Cov}(P_{j_1}, P_{j_2})\right| \leq \sum_{i=1}^{n} p(j_1)p(j_2)\sqrt{\mathbb{E}\left[\left(\mathbb{E}_i^{j_1}\left[P_{j_1}\right] - \mathbb{E}_i^{j_2}\left[P_{j_1}\right]\right)^2\right]}\sqrt{\mathbb{E}\left[\left(\mathbb{E}_i^{j_1}\left[P_{j_2}\right] - \mathbb{E}_i^{j_2}\left[P_{j_2}\right]\right)^2\right]}. \quad (4.31)$$

Now, using (4.29) and Jensen's inequality we have

$$\begin{aligned}&\mathbb{E}\left[\left(\mathbb{E}_i^{j_1}\left[P_{j_1}\right] - \mathbb{E}_i^{j_2}\left[P_{j_1}\right]\right)^2\right] \\ &= \mathbb{E}\Big[\Big\{\int_{\mathbb{R}^{n-i}} \left(P_{j_1}(X_1, \ldots, X_{i-1}, x_{j_1}, y_{i+1}, \ldots, y_n) - P_{j_1}(X_1, \ldots, X_{i-1}, x_{j_2}, y_{i+1}, \ldots, y_n)\right) \\ &\qquad\qquad f(y_{i+1}) \cdots f(y_n)\mathrm{d}y_{i+1} \cdots \mathrm{d}y_n\Big\}^2\Big] \\ &\leq \mathbb{E}\Big[\int_{\mathbb{R}^{n-i}} \left\{P_{j_1}(X_1, \ldots, X_{i-1}, x_{j_1}, y_{i+1}, \ldots, y_n) - P_{j_1}(X_1, \ldots, X_{i-1}, x_{j_2}, y_{i+1}, \ldots, y_n)\right\}^2 \\ &\qquad\qquad f(y_{i+1}) \cdots f(y_n)\mathrm{d}y_{i+1} \cdots \mathrm{d}y_n\Big] \\ &= \mathbb{E}\left[\left\{P_{j_1}(X_1, \ldots, X_{i-1}, x_{j_1}, X_{i+1}, \ldots, X_n) - P_{j_1}(X_1, \ldots, X_{i-1}, x_{j_2}, X_{i+1}, \ldots, X_n)\right\}^2\right] \\ &= \mathbb{E}\left[\left(\left[\frac{1}{n} + Y\right]_{-\tau}^{\tau} - [Y]_{-\tau}^{\tau}\right)^2\right],\end{aligned}$$

where

$$Y = \frac{1}{n}\sum_{\substack{k=1\\k\neq i}}^{n} \mathbb{1}(X_k \in B_{j_1}) + \frac{2}{n\alpha}\sum_{k=1}^{n} W_{kj_1} - p_0(j_1).$$

Note that since $[\cdot]_{-\tau}^{\tau}$ is continuous Lipschitz with Lipschitz constant 1, it holds

$$\mathbb{E}\left[\left(\mathbb{E}_i^{j_1}\left[P_{j_1}\right] - \mathbb{E}_i^{j_2}\left[P_{j_1}\right]\right)^2\right] \leq \frac{1}{n^2}.$$

However, we can provide another bound when $|p(j_1) - p_0(j_1)| \geq 2(\tau + 1/n)$. Assume that $p(j_1) - p_0(j_1) \geq 2(\tau + 1/n)$. We have

$$\begin{aligned}
&\mathbb{E}\left[\left(\mathbb{E}_i^{j_1}\left[P_{j_1}\right] - \mathbb{E}_i^{j_2}\left[P_{j_1}\right]\right)^2\right] \\
&\leq \mathbb{E}\left[\left(\left[\frac{1}{n} + Y\right]_{-\tau}^{\tau} - [Y]_{-\tau}^{\tau}\right)^2 \mathbb{1}(Y \leq \tau)\right] + \mathbb{E}\left[\left(\left[\frac{1}{n} + Y\right]_{-\tau}^{\tau} - [Y]_{-\tau}^{\tau}\right)^2 \mathbb{1}(Y > \tau)\right] \\
&\leq \frac{1}{n^2}\mathbb{P}(Y \leq \tau) \\
&= \frac{1}{n^2}\mathbb{P}\left(\frac{1}{n}\sum_{\substack{k=1\\k\neq i}}^{n} \mathbb{1}(X_k \in B_{j_1}) + \frac{2}{n\alpha}\sum_{k=1}^{n} W_{kj_1} - p_0(j_1) \leq \tau\right) \\
&\leq \frac{1}{n^2}\mathbb{P}\left(\frac{1}{n}\sum_{k=1}^{n} \mathbb{1}(X_k \in B_{j_1}) - \frac{1}{n} + \frac{2}{n\alpha}\sum_{k=1}^{n} W_{kj_1} - p_0(j_1) \leq \tau\right) \\
&= \frac{1}{n^2}\mathbb{P}\left(\widehat{p}_{j_1} \leq \tau + \frac{1}{n} + p_0(j_1)\right) \\
&\leq \frac{1}{n^2}\mathbb{P}\left(|\widehat{p}_{j_1} - p(j_1)| \geq p(j_1) - p_0(j_1) - \tau - \frac{1}{n}\right)
\end{aligned}$$

Now, if $p(j_1) - p_0(j_1) \geq 2(\tau + 1/n)$ then we have $0 < p(j_1) - p_0(j_1) - \tau - \frac{1}{n} \leq p(j_1) \leq 1 \leq \frac{1}{\alpha}$ and (4.21) gives

$$\begin{aligned}
\mathbb{E}\left[\left(\mathbb{E}_i^{j_1}\left[P_{j_1}\right] - \mathbb{E}_i^{j_2}\left[P_{j_1}\right]\right)^2\right] &\leq \frac{2}{n^2}\exp\left(-\frac{n\alpha^2\left(p(j_1) - p_0(j_1) - \tau - 1/n\right)^2}{42}\right) \\
&\leq \frac{2}{n^2}\exp\left(-\frac{n\alpha^2\left(p(j_1) - p_0(j_1)\right)^2}{168}\right).
\end{aligned}$$

One can prove the same result if $p(j_1) - p_0(j_1) \leq -2(\tau + 1/n)$, and similar bounds with j_1 replaced by j_2 hold for $\mathbb{E}\left[\left(\mathbb{E}_i^{j_1}\left[P_{j_2}\right] - \mathbb{E}_i^{j_2}\left[P_{j_2}\right]\right)^2\right]$. We can now conclude.
If $j_1 \neq j_2$ are such that $|p(j_1) - p_0(j_1)| \geq 2(\tau + 1/n)$ and $|p(j_2) - p_0(j_2)| \geq 2(\tau + 1/n)$

then (4.31) gives

$$|\mathrm{Cov}\left(P_{j_1}, P_{j_2}\right)| \leq \frac{2p(j_1)p(j_2)}{n} \exp\left(-\frac{n\alpha^2\left[(p(j_1)-p_0(j_1))^2+(p(j_2)-p_0(j_2))^2\right]}{336}\right).$$

If $j_1 \neq j_2$ are such that $|p(j_1)-p_0(j_1)| < 2(\tau+1/n)$ and $|p(j_2)-p_0(j_2)| \geq 2(\tau+1/n)$ then (4.31) gives

$$\begin{aligned}
&|\mathrm{Cov}\left(P_{j_1}, P_{j_2}\right)| \\
&\leq \frac{\sqrt{2}p(j_1)p(j_2)}{n} \exp\left(-\frac{n\alpha^2(p(j_2)-p_0(j_2))^2}{336}\right) \\
&= \frac{\sqrt{2}p(j_1)p(j_2)}{n} \exp\left(-\frac{n\alpha^2\left[(p(j_1)-p_0(j_1))^2+(p(j_2)-p_0(j_2))^2\right]}{336}\right) \exp\left(\frac{n\alpha^2(p(j_1)-p_0(j_1))^2}{336}\right) \\
&\leq \frac{\sqrt{2}\exp(1/21)p(j_1)p(j_2)}{n} \exp\left(-\frac{n\alpha^2\left[(p(j_1)-p_0(j_1))^2+(p(j_2)-p_0(j_2))^2\right]}{336}\right),
\end{aligned}$$

since $|p(j_1)-p_0(j_1)| < 2(\tau+1/n) \leq 4/\sqrt{n\alpha^2}$. The same result holds if $j_1 \neq j_2$ are such that $|p(j_1)-p_0(j_1)| \geq 2(\tau+1/n)$ and $|p(j_2)-p_0(j_2)| < 2(\tau+1/n)$. Finally, if $j_1 \neq j_2$ are such that $|p(j_1)-p_0(j_1)| < 2(\tau+1/n)$ and $|p(j_2)-p_0(j_2)| < 2(\tau+1/n)$, then (4.31) gives

$$\begin{aligned}
|\mathrm{Cov}\left(P_{j_1}, P_{j_2}\right)| &\leq \frac{p(j_1)p(j_2)}{n} \\
&\leq \frac{p(j_1)p(j_2)}{n} \exp\left(\frac{2}{21}\right) \exp\left(-\frac{n\alpha^2\left[(p(j_1)-p_0(j_1))^2+(p(j_2)-p_0(j_2))^2\right]}{336}\right),
\end{aligned}$$

which ends the proof of (4.20). □

4.7.3 Proof of Theorem 4.4.3

The outline of the proof is similar to that of Theorem 4.3.4 : we first prove that the choice of t_1 and t_2 in (4.10) yields $\mathbb{P}_{Q^n_{f_0}}(\Phi = 1) \leq \gamma/2$ and we then exhibit $\rho_1, \rho_2 > 0$ such that

$$\begin{cases}
\int_B |f-f_0| \geq \rho_1 \Rightarrow \mathbb{P}_{Q^n_f}(D_B < t_1) \leq \gamma/2 \\
\int_{\bar{B}} |f-f_0| \geq \rho_2 \Rightarrow \mathbb{P}_{Q^n_f}(T_B < t_2) \leq \gamma/2.
\end{cases}$$

The quantity $\rho_1+\rho_2$ will then provide an upper bound on $\mathcal{E}_{n,\alpha}(f_0,\gamma)$.

We have already seen in the proof of the upper bound in the non-interactive scenario

that the choice $t_2 = \sqrt{20/(n\alpha^2\gamma)}$ gives $\mathbb{P}_{Q^n_{f_0}}(T_B \geq t_2) \leq \gamma/4$. Moreover, Chebychev's inequality and Proposition 4.4.2 yield

$$\begin{aligned}\mathbb{P}_{Q^n_{f_0}}(D_B \geq t_1) = \mathbb{P}_{Q^n_{f_0}}(D_B - \mathbb{E}_{Q^n_{f_0}}[D_B] \geq t_1) &\leq \mathbb{P}_{Q^n_{f_0}}\left(|D_B - \mathbb{E}_{Q^n_{f_0}}[D_B]| \geq t_1\right) \\ &\leq \frac{\mathrm{Var}_{Qf_0^n}(D_B)}{t_1^2} \\ &\leq \frac{5}{(n\alpha^2)^2 t_1^2} \\ &\leq \frac{\gamma}{4}\end{aligned}$$

for $t_1 = 2\sqrt{5}/(n\alpha^2\sqrt{\gamma})$. We thus have

$$\mathbb{P}_{Q^n_{f_0}}(\Phi = 1) \leq \mathbb{P}_{Q^n_{f_0}}(D_B \geq t_1) + \mathbb{P}_{Q^n_{f_0}}(T_B \geq t_2) \leq \frac{\gamma}{2}.$$

We have seen in the proof of Theorem 4.3.4 (upper bound in the non-interactive scenario) that if we set

$$\rho_2 = 2\int_{\bar{B}} f_0 + \left(1 + \frac{1}{\sqrt{2}}\right) t_2,$$

then we have

$$\int_{\bar{B}} |f - f_0| \geq \rho_2 \implies \mathbb{P}_{Q^n_f}(T_B < t_2) \leq \frac{\gamma}{2}.$$

It remains now to exhibit ρ_1 such that $\int_B |f - f_0| \geq \rho_1$ implies $\mathbb{P}_{Q^n_f}(D_B < t_1) \leq \gamma/2$. Chebychev's inequality gives

$$\begin{aligned}\mathbb{P}_{Q^n_f}(D_B < t_1) = \mathbb{P}_{Q^n_f}\left(\mathbb{E}_{Q^n_f}[D_B] - D_B > \mathbb{E}_{Q^n_f}[D_B] - t_1\right) &\leq \frac{\mathrm{Var}_{Qf^n}(D_B)}{\left(\mathbb{E}_{Q^n_f}[D_B] - t_1\right)^2} \\ &\leq \frac{\frac{5}{(n\alpha^2)^2}}{\left(\mathbb{E}_{Q^n_f}[D_B] - t_1\right)^2} + \frac{\frac{67 D_\tau(f)}{n\alpha^2}}{\left(\mathbb{E}_{Q^n_f}[D_B] - t_1\right)^2},\end{aligned}$$

if $\mathbb{E}_{Q^n_f}[D_B] - t_1 > 0$. Now, observe that if $D_\tau(f) \geq 12(t_1 + 6\tau/\sqrt{n})$, Proposition 4.4.2 implies

$$\mathbb{E}_{Q^n_f}[D_B] - t_1 \geq \frac{1}{6} D_\tau(f) - \frac{6\tau}{\sqrt{n}} - t_1 \geq t_1 + \frac{6\tau}{\sqrt{n}} \geq t_1,$$

and

$$\mathbb{E}_{Q_f^n}[D_B] - t_1 \geq \frac{1}{6}D_\tau(f) - \left(\frac{6\tau}{\sqrt{n}} + t_1\right) \geq \frac{1}{6}D_\tau(f) - \frac{1}{12}D_\tau(f) = \frac{1}{12}D_\tau(f).$$

Thus, if $D_\tau(f) \geq 12(t_1 + 6\tau/\sqrt{n})$ we obtain

$$\mathbb{P}_{Q_f^n}(D_B < t_1) \leq \frac{5}{(n\alpha^2)^2 t_1^2} + \frac{144 \times 67}{n\alpha^2 D_\tau(f)} = \frac{\gamma}{4} + \frac{9648}{n\alpha^2 D_\tau(f)}.$$

Thus, if $D_\tau(f)$ satisfies

$$D_\tau(f) \geq \frac{C_\gamma}{n\alpha^2}, \quad \text{with } C_\gamma = \max\left\{\frac{24\sqrt{5}+72}{\sqrt{\gamma}}, \frac{9648 \times 4}{\gamma}\right\}$$

then we have $\mathbb{P}_{Q_f^n}(D_B < t_1) \leq \gamma/2$. We now exhibit ρ_1 such that $\int_B |f - f_0| \geq \rho_1$ implies $D_\tau(f) \geq C_\gamma/(n\alpha^2)$. To this aim, we will use the following facts

i) $D_\tau(f) \geq \min\left\{\sum_{j=1}^N |p(j) - p_0(j)|^2, \tau\sqrt{\sum_{j=1}^N |p(j) - p_0(j)|^2}\right\}$,

ii) $\sum_{j=1}^N |p(j) - p_0(j)|^2 \geq \frac{C_\gamma^2}{n\alpha^2} \Rightarrow \min\left\{\sum_{j=1}^N |p(j) - p_0(j)|^2, \tau\sqrt{\sum_{j=1}^N |p(j) - p_0(j)|^2}\right\} \geq \frac{C_\gamma}{n\alpha^2}$,

iii) $\left(\int_B |f - f_0|\right)^2 \leq 4(L + L_0)^2|B|^2h^{2\beta} + |B|/(2h)\sum_{j=1}^N |p(j) - p_0(j)|^2$.

We admit for now these three facts and conclude the proof of our upper bound. If we have

$$\left(\int_B |f - f_0|\right)^2 \geq 4(L + L_0)^2|B|^2h^{2\beta} + \frac{|B|}{2h}\frac{C_\gamma^2}{n\alpha^2}$$

then iii) implies

$$\sum_{j=1}^N |p(j) - p_0(j)|^2 \geq \frac{C_\gamma^2}{n\alpha^2},$$

and ii) combined with i) yield $D_\tau(f) \geq C_\gamma/(n\alpha^2)$ and thus $\mathbb{P}_{Q_f^n}(D_B < t_1) \leq \gamma/2$. We can then take

$$\rho_1 = \sqrt{4(L + L_0)^2|B|^2h^{2\beta} + \frac{|B|}{2h}\frac{C_\gamma^2}{n\alpha^2}}.$$

For all $f \in H(\beta, L)$ satisfying $\|f - f_0\|_1 \geq \rho_1 + \rho_2$ it holds

$$\mathbb{P}_{Q_{f_0}^n}(\Phi = 1) + \mathbb{P}_{Q_f^n}(\Phi = 0) \leq \frac{\gamma}{2} + \min\left\{\mathbb{P}_{Q_f^n}(D_B < t_1), \mathbb{P}_{Q_f^n}(T_B < t_2)\right\} \leq \frac{\gamma}{2} + \frac{\gamma}{2} = \gamma,$$

since $\|f - f_0\|_1 \geq \rho_1 + \rho_2$ implies $\int_B |f - f_0| \geq \rho_1$ or $\int_{\bar{B}} |f - f_0| \geq \rho_2$. Consequently, we have

$$\begin{aligned}\mathcal{E}_{n,\alpha}(f_0, \gamma) \leq \rho_1 + \rho_2 &= \sqrt{4(L + L_0)^2 |B|^2 h^{2\beta} + \frac{|B|}{2h} \frac{C_\gamma^2}{n\alpha^2}} + 2 \int_{\bar{B}} f_0 + \left(1 + \frac{1}{\sqrt{2}}\right) t_2 \\ &\leq C(L, L_0, \gamma) \left[|B| h^\beta + \sqrt{\frac{|B|}{hn\alpha^2}} + \int_{\bar{B}} f_0 + \frac{1}{\sqrt{n\alpha^2}} \right].\end{aligned}$$

The choice $h \asymp |B|^{-\frac{1}{2\beta+1}} (n\alpha^2)^{-\frac{1}{2\beta+1}}$ yields

$$\mathcal{E}_{n,\alpha}(f_0, \gamma) \leq C \left[|B|^{\frac{\beta+1}{2\beta+1}} (n\alpha^2)^{-\frac{\beta}{2\beta+1}} + \int_{\bar{B}} f_0 + \frac{1}{\sqrt{n\alpha^2}} \right],$$

which ends the proof of Theorem 4.4.3. It remains to prove i), ii) and iii). Let's start with the proof of i). If $\tau \geq \sqrt{\sum_{j=1}^N |p(j) - p_0(j)|^2}$, then $\tau \geq |p(j) - p_0(j)|$ for all j, and we thus have

$$D_\tau(f) = \sum_{j=1}^N |p(j) - p_0(j)|^2 = \min \left\{ \sum_{j=1}^N |p(j) - p_0(j)|^2, \tau \sqrt{\sum_{j=1}^N |p(j) - p_0(j)|^2} \right\}.$$

We now deal with the case $\tau < \sqrt{\sum_{j=1}^N |p(j) - p_0(j)|^2}$. In this case, we can write

$$\begin{aligned}&D_\tau(f) - \tau \sqrt{\sum_{j=1}^N |p(j) - p_0(j)|^2} \\ &\quad = \sum_{j=1}^N |p(j) - p_0(j)| \min\{|p(j) - p_0(j)|, \tau\} - \tau \frac{\sum_{j=1}^N |p(j) - p_0(j)|^2}{\sqrt{\sum_{k=1}^N |p(k) - p_0(k)|^2}} \\ &\quad = \sum_{j=1}^N |p(j) - p_0(j)| \underbrace{\left[\min\{|p(j) - p_0(j)|, \tau\} - \frac{\tau |p(j) - p_0(j)|}{\sqrt{\sum_{k=1}^N |p(k) - p_0(k)|^2}} \right]}_{=: A_j},\end{aligned}$$

and $A_j \geq 0$ for all j. Indeed, if j is such that $|p(j) - p_0(j)| < \tau$ it holds

$$A_j = |p(j) - p_0(j)| \left[1 - \frac{\tau}{\sqrt{\sum_{k=1}^N |p(k) - p_0(k)|^2}} \right] \geq 0,$$

and if j is such that $|p(j) - p_0(j)| \geq \tau$ it holds

$$A_j = \tau \left[1 - \frac{|p(j) - p_0(j)|}{\sqrt{\sum_{k=1}^N |p(k) - p_0(k)|^2}} \right] \geq 0.$$

Thus, if $\tau < \sqrt{\sum_{j=1}^N |p(j) - p_0(j)|^2}$ we have

$$D_\tau(f) \geq \tau \sqrt{\sum_{j=1}^N |p(j) - p_0(j)|^2} = \min \left\{ \sum_{j=1}^N |p(j) - p_0(j)|^2, \tau \sqrt{\sum_{j=1}^N |p(j) - p_0(j)|^2} \right\},$$

which end the proof of i). We now prove ii). Assume that $\sum_{j=1}^N |p(j) - p_0(j)|^2 \geq C_\gamma^2/(n\alpha^2)$. It holds $C_\gamma^2 \geq C_\gamma$ since $C_\gamma \geq 1$ and we thus have $\sum_{j=1}^N |p(j) - p_0(j)|^2 \geq C_\gamma/(n\alpha^2)$. It also holds

$$\tau \sqrt{\sum_{j=1}^N |p(j) - p_0(j)|^2} \geq \tau \cdot \frac{C_\gamma}{\sqrt{n\alpha^2}} = \frac{C_\gamma}{n\alpha^2},$$

yielding ii). Finally, Cauchy-Schwarz inequality yields

$$\begin{aligned} \left(\int_B |f - f_0| \right)^2 &\leq |B| \int_B |f - f_0|^2 \\ &\leq |B| \cdot \left| \int_B |f - f_0|^2 - \frac{1}{2h} \sum_{j=1}^N \left(p(j) - p_0(j) \right)^2 \right| + \frac{|B|}{2h} \sum_{j=1}^N \left(p(j) - p_0(j) \right)^2. \end{aligned}$$

Now, observe that

$$\left| \int_B |f - f_0|^2 - \frac{1}{2h} \sum_{j=1}^N \left(p(j) - p_0(j) \right)^2 \right| = \left| \sum_{j=1}^N \int_{B_j} \left[(f - f_0)(x) - \frac{p(j) - p_0(j)}{2h} \right]^2 \mathrm{d}x \right|,$$

and observe also that for $x \in B_j$ it holds

$$\begin{aligned}\left|(f-f_0)(x) - \frac{p(j)-p_0(j)}{2h}\right| &= \left|\frac{1}{2h}\int_{B_j}[(f-f_0)(x)-(f-f_0)(u)]\mathrm{d}u\right| \\ &\leq \frac{1}{2h}\int_{B_j}\left[|f(x)-f(u)|+|f_0(x)-f_0(u)|\right]\mathrm{d}u \\ &\leq \frac{L+L_0}{2h}\int_{B_j}|x-u|^\beta \mathrm{d}u \\ &\leq \frac{L+L_0}{2h}\int_{B_j}(2h)^\beta \mathrm{d}u \\ &\leq 2(L+L_0)h^\beta.\end{aligned}$$

This gives

$$\left|\int_B |f-f_0|^2 - \frac{1}{2h}\sum_{j=1}^N (p(j)-p_0(j))^2\right| \leq \sum_{j=1}^N \int_{B_j} 4(L+L_0)^2 h^{2\beta} = 4(L+L_0)^2|B|h^{2\beta},$$

which yields iii).

4.7.4 Proof of Theorem 4.4.4

Let $B \subset \mathbb{R}$ be a nonempty compact set, and let $(B_j)_{j=1,\dots,N}$ be a partition of B, $h>0$ be the bandwidth and $(x_1,\dots,x_N)$ be the centering points, that is $B_j = [x_j - h, x_j + h]$ for all $j \in [\![1,N]\!]$. Let $\psi : [-1,1] \to \mathbb{R}$ be such that $\psi \in H(\beta, L)$, $\int \psi = 0$ and $\int \psi^2 = 1$. For $j \in [\![1,N]\!]$, define

$$\psi_j : t \in \mathbb{R} \mapsto \frac{1}{\sqrt{h}}\psi\left(\frac{t-x_j}{h}\right).$$

Note that the support of ψ_j is B_j, $\int \psi_j = 0$ and $(\psi_j)_{j=1,\dots,N}$ is an orthonormal family.

For $\delta > 0$ and $\nu \in \mathcal{V}_N = \{-1,1\}^N$, define the functions

$$f_\nu : x \in \mathbb{R} \mapsto f_0(x) + \delta \sum_{j=1}^N \nu_j \psi_j(x),$$

The following lemma shows that for δ properly chosen, for all $\nu \in \mathcal{V}_N$, f_ν is a density belonging to $H(\beta, L)$ and f_ν is sufficiently far away from f_0 in a L_1 sense.

Lemma 4.7.1. *If the parameter δ appearing in the definition of f_ν satisfies*

$$\delta \leq \sqrt{h} \cdot \min\left\{ \frac{C_0(B)}{\|\psi\|_\infty}, \frac{1}{2}\left(1 - \frac{L_0}{L}\right) h^\beta \right\},$$

where $C_0(B) := \min\{f_0(x) : x \in B\}$, then we have

i) $f_\nu \geq 0$ *and* $\int f_\nu = 1$, *for all* $\nu \in \mathcal{V}_N$,

ii) $f_\nu \in H(\beta, L)$, *for all* $\nu \in \mathcal{V}_N$,

iii) $\|f_\nu - f_0\|_1 = C_1 \delta N \sqrt{h}$, *for all* $\nu \in \mathcal{V}_N$, *with* $C_1 = \int_{-1}^1 |\psi|$.

Proof. We first prove *i)*. Since $\int \psi_j = 0$ for all $j = 1, \ldots, n$, it holds $\int f_\nu = \int f_0 = 1$ for all ν. Since $\mathrm{Supp}(\psi_k) = B_k$ for all $k = 1, \ldots, N$, it holds $f_\nu \equiv f_0$ on B^c and thus f_ν is non-negative on B^c. Now, for $x \in B_j$ it holds for all $\nu \in \mathcal{V}_N$

$$f_\nu(x) = f_0(x) + \delta \nu_j \psi_j(x) \geq C_0(B) - \delta \|\psi_j\|_\infty \geq C_0(B) - \frac{\delta \|\psi\|_\infty}{\sqrt{h}} \geq 0,$$

since $\delta \leq C_0(B)\sqrt{h}/\|\psi\|_\infty$ Thus, f_ν is non-negative on $\mathbb{R}$ for all $\nu \in \mathcal{V}_N$.

To prove *ii)*, we have to show that $|f_\nu(x) - f_\nu(y)| \leq L|x-y|^\beta$, for all $\nu \in \mathcal{V}_N$, for all $x, y \in \mathbb{R}$. Since $f_\nu \equiv f_0$ on B^c and $f_0 \in H(\beta, L_0)$, this result is trivial for $x, y \in B^c$. If $x \in B_l$ and $y \in B_k$ it holds

$$\begin{aligned}
|f_\nu(x) - f_\nu(y)| &\leq |f_0(x) - f_0(y)| + |\delta \nu_l \psi_l(x) - \delta \nu_k \psi_k(y)| \\
&\leq L_0|x-y|^\beta + |\delta \nu_l \psi_l(x) - \delta \nu_l \psi_l(y)| + |\delta \nu_k \psi_k(x) - \delta \nu_k \psi_k(y)| \\
&\leq L_0|x-y|^\beta + \frac{\delta}{\sqrt{h}} \left| \psi\left(\frac{x - x_l}{h}\right) - \psi\left(\frac{y - x_l}{h}\right) \right| \\
&\qquad + \frac{\delta}{\sqrt{h}} \left| \psi\left(\frac{x - x_k}{h}\right) - \psi\left(\frac{y - x_k}{h}\right) \right| \\
&\leq L_0|x-y|^\beta + \frac{\delta}{h^{\beta+1/2}} \cdot L|x-y|^\beta + \frac{\delta}{h^{\beta+1/2}} \cdot L|x-y|^\beta \\
&= \left(\frac{L_0}{L} + \frac{2\delta}{h^{\beta+1/2}} \right) L|x-y|^\beta \\
&\leq L|x-y|^\beta
\end{aligned}$$

where we have used $\psi \in H(\beta, L)$ and $\delta \leq \frac{h^{\beta+1/2}}{2}\left(1 - \frac{L_0}{L}\right)$. Thus, it holds $|f_\nu(x) - f_\nu(y)| \leq L|x-y|^\beta$ for all $\nu \in \mathcal{V}_N$, $x \in B_l$ and $y \in B_k$. The case $x \in B^c$ and $y \in B_k$ can be handled in a similar way, which ends the proof of *ii)*.

We now prove *iii*). It holds

$$\int_{\mathbb{R}} |f_\nu - f_0| = \int_{\mathbb{R}} \left| \delta \sum_{j=1}^{N} \nu_j \psi_j(x) \right| \mathrm{d}x = \sum_{k=1}^{N} \int_{B_k} |\delta \nu_k \psi_k(x)| \, \mathrm{d}x = \delta N \sqrt{h} \int_{-1}^{1} |\psi|.$$

□

For a privacy mechanism $Q \in \mathcal{Q}_\alpha$, we denote by $Q^n_{f_0}$ (respectively $Q^n_{f_\nu}$) the distribution of $(Z_1, \dots, Z_n)$ when the X_i's are distributed according to f_0 (respectively to f_ν). We set $\bar{Q}^n = 1/2^N \sum_{\nu \in \mathcal{V}_N} Q^n_{f_\nu}$. If δ is chosen such that $\delta \leq \sqrt{h} \cdot \min \left\{ \frac{C_0(B)}{\|\psi\|_\infty}, \frac{1}{2} \left(1 - \frac{L_0}{L}\right) h^\beta \right\}$, setting $\rho^\star = C_1 \delta N \sqrt{h}$, we deduce from the above lemma that if

$$\mathrm{KL}(Q^n_{f_0}, \bar{Q}^n) \leq 2(1-\gamma)^2 \text{ for all } Q \in \mathcal{Q}_\alpha, \tag{4.32}$$

then it holds

$$\inf_{Q \in \mathcal{Q}_\alpha} \inf_{\phi \in \Phi_Q} \sup_{f \in H_1(\rho^\star)} \left\{ \mathbb{P}_{Q^n_{f_0}}(\phi = 1) + \mathbb{P}_{Q^n_f}(\phi = 0) \right\} \geq \gamma,$$

where $H_1(\rho^\star) := \{ f \in H(\beta, L) : f \geq 0, \int f = 1, \|f - f_0\|_1 \geq \rho^\star \}$, and consequently $\mathcal{E}_{n,\alpha}(f_0, \gamma) \geq \rho^\star$. Indeed, if (4.32) holds, then we have

$$\begin{aligned}
&\inf_{Q \in \mathcal{Q}_\alpha} \inf_{\phi \in \Phi_Q} \sup_{f \in H_1(\rho^\star)} \left\{ \mathbb{P}_{Q^n_{f_0}}(\phi = 1) + \mathbb{P}_{Q^n_f}(\phi = 0) \right\} \\
&\qquad \geq \inf_{Q \in \mathcal{Q}_\alpha} \inf_{\phi \in \Phi_Q} \left(\mathbb{P}_{Q^n_{f_0}}(\phi = 1) + \frac{1}{2^N} \sum_{\nu \in \mathcal{V}_N} \mathbb{P}_{Q^n_{f_\nu}}(\phi = 0) \right) \\
&\qquad = \inf_{Q \in \mathcal{Q}_\alpha} \inf_{\phi \in \Phi_Q} \left(1 - \left[\mathbb{P}_{Q^n_{f_0}}(\phi = 0) - \mathbb{P}_{\bar{Q}^n}(\phi = 0) \right] \right) \\
&\qquad \geq \inf_{Q \in \mathcal{Q}_\alpha} \left[1 - \mathrm{TV}(Q^n_{f_0}, \bar{Q}^n) \right] \\
&\qquad \geq \inf_{Q \in \mathcal{Q}_\alpha} \left[1 - \sqrt{\frac{\mathrm{KL}(Q^n_{f_0}, \bar{Q}^n)}{2}} \right] \\
&\qquad \geq \gamma,
\end{aligned}$$

where the second to last inequality follows from Pinsker's inequality. We now prove that (4.32) holds under an extra assumption on δ. Fix a privacy mechanism $Q \in \mathcal{Q}_\alpha$. The conditionnal distribution of Z_i given $Z_1, \dots, Z_{i-1}$ when X_i is distributed according to f_0 or f_ν will be denoted by $\mathcal{L}^{(0)}_{Z_i | z_{1:(i-1)}}(dz_i) = \int_{\mathbb{R}} Q_i(dz_i \mid x_i, z_{1:(i-1)}) f_0(x_i) dx_i$ and $\mathcal{L}^{(\nu)}_{Z_i | z_{1:(i-1)}}(dz_i) = \int_{\mathbb{R}} Q_i(dz_i \mid x_i, z_{1:(i-1)}) f_\nu(x_i) dx_i$ respectively. The joint distribution of

$Z_1, \dots, Z_i$ when $X_1, \dots, X_i$ are i.i.d. from f_0 will be denoted by

$$\mathcal{L}^{(0)}_{Z_1,\dots,Z_i}(dz_{1:i}) = \mathcal{L}^{(0)}_{Z_i|z_{1:(i-1)}}(dz_i) \cdots \mathcal{L}^{(0)}_{Z_2|z_1}(dz_2)\mathcal{L}^{(0)}_{Z_1}(dz_1).$$

The convexity and tensorization of the Kullback-Leibler divergence give

$$\begin{aligned}\mathrm{KL}(Q^n_{f_0}, \bar{Q}^n) &\leq \frac{1}{2^N}\sum_{\nu\in\mathcal{V}} \mathrm{KL}(Q^n_{f_0}, Q^n_{f_\nu}) \\ &= \frac{1}{2^N}\sum_{\nu\in\mathcal{V}}\sum_{i=1}^{n}\int_{\mathcal{Z}^{i-1}} \mathrm{KL}\left(\mathcal{L}^{(0)}_{Z_i|z_{1:(i-1)}}, \mathcal{L}^{(\nu)}_{Z_i|z_{1:(i-1)}}\right)\mathcal{L}^{(0)}_{Z_1,\dots,Z_{i-1}}(dz_{1:(i-1)}).\end{aligned}$$

According to lemma B.3 in [15], there exists a probability measure $\mu_{z_{1:(i-1)}}$ on $\mathcal{Z}$ and a family of $\mu_{z_{1:(i-1)}}$-densities $z_i \mapsto q_i(\cdot \mid x_i, z_{1:(i-1)})$ of $Q_i(\cdot \mid x_i, z_{1:(i-1)})$, $x_i \in \mathbb{R}$ such that

$$e^{-\alpha} \leq q_i(z_i \mid x_i, z_{1:(i-1)}) \leq e^{\alpha}, \quad \forall z_i \in \mathcal{Z}, \forall x_i \in \mathbb{R}.$$

We can thus write $\mathcal{L}^{(0)}_{Z_i|z_{1:(i-1)}}(dz_i) = m^{(0)}_i(z_i \mid z_{1:(i-1)})d\mu_{z_{1:(i-1)}}(z_i)$, and $\mathcal{L}^{(\nu)}_{Z_i|z_{1:(i-1)}}(dz_i) = m^{(\nu)}_i(z_i \mid z_{1:(i-1)})d\mu_{z_{1:(i-1)}}(z_i)$ with $m^{(0)}_i(z_i \mid z_{1:(i-1)}) = \int_{\mathbb{R}} q_i(z_i \mid x_i, z_{1:(i-1)})f_0(x_i)\mathrm{d}x_i$ and $m^{(\nu)}_i(z_i \mid z_{1:(i-1)}) = \int_{\mathbb{R}} q_i(z_i \mid x_i, z_{1:(i-1)})f_\nu(x_i)\mathrm{d}x_i$. Bounding the Kullback-Leibler divergence by the χ^2-divergence, we have

$$\begin{aligned}&\mathrm{KL}\left(\mathcal{L}^{(0)}_{Z_i|z_{1:(i-1)}}, \mathcal{L}^{(\nu)}_{Z_i|z_{1:(i-1)}}\right) \\ &\leq \int_{\mathcal{Z}}\left(\frac{d\mathcal{L}^{(0)}_{Z_i|z_{1:(i-1)}}}{d\mathcal{L}^{(\nu)}_{Z_i|z_{1:(i-1)}}} - 1\right)^2 \mathcal{L}^{(\nu)}_{Z_i|z_{1:(i-1)}}(dz_i) \\ &= \int_{\mathcal{Z}}\left(\frac{m^{(0)}_i(z_i \mid z_{1:i-1}) - m^{(\nu)}_i(z_i \mid z_{1:i-1})}{m^{(\nu)}_i(z_i \mid z_{1:i-1})}\right)^2 m^{(\nu)}_i(z_i \mid z_{1:i-1})d\mu_{z_{1:(i-1)}}(z_i) \\ &= \int_{\mathcal{Z}}\left(\frac{\int_{\mathbb{R}} q_i(z_i \mid x, z_{1:i-1})\,(f_0(x) - f_\nu(x))\,dx}{m^{(\nu)}_i(z_i \mid z_{1:i-1})}\right)^2 m^{(\nu)}_i(z_i \mid z_{1:i-1})d\mu_{z_{1:(i-1)}}(z_i) \\ &= \int_{\mathcal{Z}}\left[\int_{\mathbb{R}}\left(\frac{q_i(z_i \mid x, z_{1:i-1})}{m^{(\nu)}_i(z_i \mid z_{1:i-1})} - e^{-2\alpha}\right)(f_0(x) - f_\nu(x))\,dx\right]^2 m^{(\nu)}_i(z_i \mid z_{1:i-1})d\mu_{z_{1:(i-1)}}(z_i),\end{aligned}$$

since $\int_{\mathbb{R}}(f_0 - f_\nu) = 0$. Recall that q_i satisfies $e^{-\alpha} \leq q_i(z_i \mid x, z_{1:(i-1)}) \leq e^{\alpha}$. Thus, we have

$e^\alpha = \int e^\alpha f_\nu \geq m_i^{(\nu)}(z_i \mid z_{1:(i-1)}) \geq e^{-\alpha} \int f_\nu = e^{-\alpha}$, and therefore

$$0 \leq g_{i,z_{1:i}}(x) := \frac{q_i(z_i \mid x, z_{1:(i-1)})}{m_i^{(\nu)}(z_i \mid z_{1:(i-1)})} - e^{-2\alpha} \leq z_\alpha = e^{2\alpha} - e^{-2\alpha}.$$

Thus,

$$\begin{aligned}
&\frac{1}{2^N} \sum_{\nu \in \mathcal{V}_N} \left[\int_{\mathbb{R}} \left(\frac{q_i(z_i \mid x, z_{1:i-1})}{m_i^{(\nu)}(z_i \mid z_{1:i-1})} - e^{-2\alpha} \right) (f_0(x) - f_\nu(x))\, dx \right]^2 m_i^{(\nu)}(z_i \mid z_{1:i-1}) \\
&\leq e^\alpha \delta^2 \frac{1}{2^N} \sum_{\nu \in \mathcal{V}_N} \left[\sum_{k=1}^N \nu_k \int_{\mathbb{R}} g_{i,z_{1:i}}(x) \psi_k(x) dx \right]^2 \\
&= e\delta^2 \sum_{k=1}^N \left[\int_{\mathbb{R}} g_{i,z_{1:i}}(x) \psi_k(x) dx \right]^2 \\
&\leq e\delta^2 z_\alpha^2 \sum_{k=1}^N \|\psi_k\|_1^2 \\
&\leq e\delta^2 z_\alpha^2 N h C_1^2 \\
&= \frac{e}{2} C_1^2 \delta^2 z_\alpha^2 |B|,
\end{aligned}$$

where we recall that $C_1 = \int |\psi|$. We thus obtain

$$\mathrm{KL}(Q_{f_0}^n, \bar{Q}^n) \leq \frac{e}{2} C_1^2 \delta^2 n z_\alpha^2 |B|,$$

and (4.32) holds as soon as

$$\delta \leq \sqrt{\frac{4(1-\gamma)^2}{e C_1^2 n z_\alpha^2 |B|}}.$$

Finally, taking $\delta = \min\left\{ \sqrt{h} \cdot \min\left\{ \frac{C_0(B)}{\|\psi\|_\infty}, \frac{1}{2}\left(1 - \frac{L_0}{L}\right) h^\beta \right\}, \sqrt{\frac{4(1-\gamma)^2}{e C_1^2 n z_\alpha^2 |B|}} \right\}$, we obtain

$$\mathcal{E}_{n,\alpha}(f_0, \gamma) \geq C(\psi, \gamma) \min\left\{ |B| \min\left\{ \frac{C_0(B)}{\|\psi\|_\infty}, \frac{1}{2}\left(1 - \frac{L_0}{L}\right) h^\beta \right\}, \frac{\sqrt{|B|}}{\sqrt{h}\sqrt{n z_\alpha^2}} \right\}.$$

If B is chosen such that $C_0(B) = \min\{f_0(x), x \in B\} \geq C h^\beta$, then the bound becomes

$$\mathcal{E}_{n,\alpha}(f_0, \gamma) \geq C(\psi, \gamma, L, L_0) \min\left\{ |B| h^\beta, \frac{\sqrt{|B|}}{\sqrt{h}\sqrt{n z_\alpha^2}} \right\},$$

and the choice $h \asymp |B|^{-1/(2\beta+1)}(nz_\alpha^2)^{-1/(2\beta+1)}$ yields

$$\mathcal{E}_{n,\alpha}(f_0,\gamma) \geq C(\psi,\gamma,L,L_0)|B|^{\frac{\beta+1}{2\beta+1}}(nz_\alpha^2)^{-\frac{\beta}{2\beta+1}}.$$

Note that with this choice of h, the condition $C_0(B) \geq Ch^\beta$ becomes $|B|^{\beta/(2\beta+1)}C_0(B) \geq C(nz_\alpha^2)^{-\beta/(2\beta+1)}$.

4.8 Appendix : Proofs of Section 4.5

4.8.1 Example 4.5.2

We first prove the result for the non-interactive case. Take

$$B = [a,T], \quad \text{with} \quad T = (n\alpha^2)^{\frac{2\beta}{k(4\beta+3)+3\beta+3}}.$$

Note that $T > a$ for n large enough. Theorem 4.3.4 gives

$$\begin{aligned}
\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) &\lesssim \max\left\{(T-a)^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}}, \left(\frac{a}{T}\right)^k\right\} \\
&\lesssim \max\left\{T^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}}, T^{-k}\right\} \\
&= (n\alpha^2)^{-\frac{2k\beta}{k(4\beta+3)+3\beta+3}}.
\end{aligned}$$

To obtain the lower bound, we first check that condition (4.7) in Theorem 4.3.5 is satisfied. Since $T \to +\infty$ as $n \to \infty$, it holds for n large enough

$$\begin{aligned}
|B|^{\frac{\beta}{4\beta+3}}C_0(B) &= (T-a)^{\frac{\beta}{4\beta+3}}\frac{ka^k}{T^{k+1}} \\
&= ka^kT^{\frac{\beta}{4\beta+3}-(k+1)}\left(1-\frac{a}{T}\right)^{\frac{\beta}{4\beta+3}} \\
&\gtrsim T^{\frac{\beta-(k+1)(4\beta+3)}{4\beta+3}} \\
&\gtrsim C(n\alpha^2)^{-\frac{2\beta}{4\beta+3}}.
\end{aligned}$$

Condition (4.7) is thus satisfied and Theorem 4.3.5 thus yields for n large enough

$$\begin{aligned}\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) &\gtrsim \left[\log\left(C(T-a)^{\frac{4\beta+4}{4\beta+3}}(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1}(T-a)^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}}\\ &\gtrsim \left[\log\left(CT^{\frac{4\beta+4}{4\beta+3}}(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1}T^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}}\\ &\gtrsim \left[\log\left(C(n\alpha^2)^{\frac{4\beta+4}{4\beta+3}\cdot\frac{2\beta}{k(4\beta+3)+3\beta+3}+\frac{2}{4\beta+3}}\right)\right]^{-1}(n\alpha^2)^{-\frac{2k\beta}{k(4\beta+3)+3\beta+3}}.\end{aligned}$$

The proof in the interactive scenario follows the same lines at the exception of the choice of T which should be taken as

$$T = (n\alpha^2)^{\frac{\beta}{k(2\beta+1)+\beta+1}}.$$

4.8.2 Example 4.5.3

We first prove the result for the non-interactive case. Take

$$B = [0,T], \quad \text{with} \quad T = \frac{1}{\lambda}\cdot\frac{2\beta}{4\beta+3}\log(n\alpha^2).$$

Theorem 4.3.4 gives

$$\begin{aligned}\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) &\lesssim \max\left\{T^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}}, \exp(-\lambda T)\right\}\\ &\lesssim \max\left\{\log(n\alpha^2)^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}}, (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}\right\}\\ &\lesssim \log(n\alpha^2)^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}}.\end{aligned}$$

Now, observe that

$$|B|^{\frac{\beta}{4\beta+3}}C_0(B) = T^{\frac{\beta}{4\beta+3}}\cdot\lambda\exp(-\lambda T) = \lambda T^{\frac{\beta}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}} \gtrsim (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}.$$

Thus, condition (4.7) is satisfied and Theorem 4.3.5 yields

$$\begin{aligned}\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) &\gtrsim \left[\log\left(CT^{\frac{4\beta+4}{4\beta+3}}(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1}T^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}}\\ &\gtrsim \left[\log\left(C\log(n\alpha^2)^{\frac{4\beta+4}{4\beta+3}}(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1}\log(n\alpha^2)^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}}.\end{aligned}$$

The proof in the interactive scenario follows the same lines at the exception of the choice of T which should be taken as

$$T = \frac{1}{\lambda} \cdot \frac{\beta}{2\beta+1} \log(n\alpha^2).$$

4.8.3 Example 4.5.4

We first prove the result for the non-interactive case. Take

$$B = [-T, T], \quad \text{with} \quad T = \sqrt{\frac{4\beta}{4\beta+3} \log(n\alpha^2)}.$$

Theorem 4.3.4 gives

$$\begin{aligned}
\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0, \gamma) &\lesssim \max\left\{ (2T)^{\frac{3\beta+3}{4\beta+3}} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}, \frac{2}{\sqrt{2\pi}} \int_T^{+\infty} e^{-x^2/2} dx \right\} \\
&\lesssim \max\left\{ T^{\frac{3\beta+3}{4\beta+3}} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}, \frac{1}{T} \exp\left(-\frac{T^2}{2}\right) \right\} \\
&\lesssim \max\left\{ \log(n\alpha^2)^{\frac{3\beta+3}{2(4\beta+3)}} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}, (n\alpha^2)^{-\frac{2\beta}{4\beta+3}} \right\} \\
&\lesssim \log(n\alpha^2)^{\frac{3\beta+3}{2(4\beta+3)}} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}.
\end{aligned}$$

Now, observe that

$$|B|^{\frac{\beta}{4\beta+3}} C_0(B) = (2T)^{\frac{\beta}{4\beta+3}} \cdot \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{T^2}{2}\right) \gtrsim (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}.$$

Thus, condition (4.7) is satisfied and Theorem 4.3.5 yields

$$\begin{aligned}
\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0, \gamma) &\gtrsim \left[\log\left(C (2T)^{\frac{4\beta+4}{4\beta+3}} (n\alpha^2)^{\frac{2}{4\beta+3}} \right) \right]^{-1} (2T)^{\frac{3\beta+3}{4\beta+3}} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}} \\
&\gtrsim \left[\log\left(C \log(n\alpha^2)^{\frac{4\beta+4}{2(4\beta+3)}} (n\alpha^2)^{\frac{2}{4\beta+3}} \right) \right]^{-1} \log(n\alpha^2)^{\frac{3\beta+3}{2(4\beta+3)}} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}
\end{aligned}$$

The proof in the interactive scenario follows the same lines at the exception of the choice of T which should be taken as

$$T = \sqrt{\frac{2\beta}{2\beta+1} \log(n\alpha^2)}.$$

4.8.4 Example 4.5.5

We first prove the result for the non-interactive case. Take

$$B = [-T, T], \quad \text{with} \quad T = (n\alpha^2)^{\frac{2\beta}{7\beta+6}}.$$

Theorem 4.3.4 gives

$$\begin{aligned}\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0, \gamma) &\lesssim \max\left\{(2T)^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}}, \frac{2}{\pi a}\int_T^{+\infty}\frac{a^2}{a^2+x^2}dx\right\} \\ &\lesssim \max\left\{T^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}}, \arctan\left(\frac{a}{T}\right)\right\}.\end{aligned}$$

Since $T \to \infty$ as $n \to \infty$, we have $\arctan(a/T) \sim_{n\to\infty} a/T$ and thus $\arctan(a/T) \leq 2(a/T)$ for n large enough. This gives for n large enough

$$\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0, \gamma) \lesssim \max\left\{T^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}}, \frac{1}{T}\right\} = (n\alpha^2)^{-\frac{2\beta}{7\beta+6}}$$

Now, observe that for n large enough it holds

$$|B|^{\frac{\beta}{4\beta+3}}C_0(B) = (2T)^{\frac{\beta}{4\beta+3}} \cdot \frac{1}{\pi a}\frac{a^2}{T^2+a^2} \gtrsim T^{\frac{\beta}{4\beta+3}} \cdot \frac{1}{T^2} = (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}.$$

Thus, condition (4.7) is satisfied and Theorem 4.3.5 yields

$$\begin{aligned}\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0, \gamma) &\gtrsim \left[\log\left(C(2T)^{\frac{4\beta+4}{4\beta+3}}(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1}(2T)^{\frac{3\beta+3}{4\beta+3}}(n\alpha^2)^{-\frac{2\beta}{4\beta+3}} \\ &\gtrsim \left[\log\left(C(n\alpha^2)^{\frac{4\beta+4}{4\beta+3}\cdot\frac{2\beta}{7\beta+6}+\frac{2}{4\beta+3}}\right)\right]^{-1}(n\alpha^2)^{-\frac{2\beta}{7\beta+6}}.\end{aligned}$$

The proof in the interactive scenario follows the same lines at the exception of the choice of T which should be taken as

$$T = (n\alpha^2)^{\frac{\beta}{3\beta+2}}.$$

4.8.5 Example 4.5.6

We first prove the result for the non-interactive case. The upper bound is straightforward taking $B = [0, 2/\sqrt{L_0}]$. For the lower bound, take

$$B = \left[T, \frac{2}{\sqrt{L_0}} - T\right], \quad \text{with} \quad T = (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}.$$

Note that for n large enough it holds $T < 1/(2\sqrt{L_0})$ and we thus have

$$|B|^{\frac{\beta}{4\beta+3}} C_0(B) = \left(\frac{2}{\sqrt{L_0}} - 2T\right)^{\frac{\beta}{4\beta+3}} \cdot L_0 T \gtrsim T = (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}.$$

Thus, condition (4.7) is satisfied and Theorem 4.3.5 yields

$$\begin{aligned}\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0, \gamma) &\gtrsim \left[\log\left(C\left(\frac{2}{\sqrt{L_0}} - 2T\right)^{\frac{4\beta+4}{4\beta+3}} (n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1} \left(\frac{2}{\sqrt{L_0}} - 2T\right)^{\frac{3\beta+3}{4\beta+3}} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}} \\ &\gtrsim \left[\log\left(C(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}\end{aligned}$$

The proof in the interactive scenario follows the same lines at the exception of the choice of T for the lower bound which should be taken as

$$T = (n\alpha^2)^{-\frac{\beta}{2\beta+1}}.$$

4.8.6 Example 4.5.7

Let $a \geq 1$, $b \geq 1$ with $a > 1$ or $b > 1$. We first prove the result for the non-interactive case. The upper bound is straightforward taking $B = [0, 1]$. For the lower bound, we need to distinguish different cases.

Case 1 : $a > 1, b = 1$. In this case f_0 is strictly non-decreasing on $[0, 1]$ and $f_0(0) = 0$. In order that f_0 is bounded from below by a strictly positive quantity, we thus take B of the form $B = [T_1, 1]$ with $0 < T_1 < 1$. We choose

$$T_1 = (n\alpha^2)^{-\frac{2\beta}{(a-1)(4\beta+3)}}.$$

Observe that that for n large enough we have

$$|B|^{\frac{\beta}{4\beta+3}} C_0(B) = [1-T_1]^{\frac{\beta}{4\beta+3}} \cdot \frac{1}{B(a,1)} T_1^{a-1} \gtrsim T_1^{a-1} = (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}$$

Thus, condition (4.7) is satisfied and Theorem 4.3.5 yields for n large enough

$$\begin{aligned}\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) &\gtrsim \left[\log\left(C\,[1-T_1]^{\frac{4\beta+4}{4\beta+3}}\,(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1} [1-T_1]^{\frac{3\beta+3}{4\beta+3}}\,(n\alpha^2)^{-\frac{2\beta}{4\beta+3}} \\ &\gtrsim \left[\log\left(C(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}.\end{aligned}$$

Case 2 : $a = 1, b > 1$. In this case f_0 is strictly non-increasing on $[0,1]$ and $f_0(1) = 0$. In order that f_0 is bounded from below by a strictly positive quantity, we thus take B of the form $B = [0, 1-T_2]$ with $0 < T_2 < 1$. We choose

$$T_2 = (n\alpha^2)^{-\frac{2\beta}{(b-1)(4\beta+3)}}.$$

Observe that that for n large enough we have

$$|B|^{\frac{\beta}{4\beta+3}} C_0(B) = [1-T_2]^{\frac{\beta}{4\beta+3}} \cdot \frac{1}{B(1,b)} T_2^{b-1} \gtrsim T_2^{b-1} = (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}$$

Thus, condition (4.7) is satisfied and Theorem 4.3.5 yields for n large enough

$$\begin{aligned}\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) &\gtrsim \left[\log\left(C\,[1-T_2]^{\frac{4\beta+4}{4\beta+3}}\,(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1} [1-T_2]^{\frac{3\beta+3}{4\beta+3}}\,(n\alpha^2)^{-\frac{2\beta}{4\beta+3}} \\ &\gtrsim \left[\log\left(C(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}.\end{aligned}$$

Case 3 : $a > 1, b > 1$. In this case, f_0 is non-decreasing on $[0, (a-1)/(a+b-2)]$, non-increasing on $[(a-1)/(a+b-2), 1]$ and $f_0(0) = f_0(1) = 0$. In order that f_0 is bounded from below by a strictly positive quantity, we thus take B of the form $B = [T_3, 1-T_4]$ and we choose

$$T_3 = (n\alpha^2)^{-\frac{2\beta}{(a-1)(4\beta+3)}}, \quad T_4 = (n\alpha^2)^{-\frac{2\beta}{(b-1)(4\beta+3)}}.$$

Observe that for n large enough it holds

$$0 < T_3 < \frac{a-1}{a+b-2} < 1 - T_4 < 1.$$

Observe that for n large enough we have

$$\begin{aligned}|B|^{\frac{\beta}{4\beta+3}} C_0(B) &= [1-(T_3+T_4)]^{\frac{\beta}{4\beta+3}} \cdot \frac{1}{B(a,b)} \min\left\{T_3^{a-1}(1-T_3)^{b-1}, (1-T_4)^{a-1}T_4^{b-1}\right\} \\ &\gtrsim \min\left\{T_3^{a-1}, T_4^{b-1}\right\} \\ &\gtrsim (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}.\end{aligned}$$

Thus, condition (4.7) is satisfied and Theorem 4.3.5 yields for n large enough

$$\begin{aligned}\mathcal{E}^{\mathrm{NI}}_{n,\alpha}(f_0,\gamma) &\gtrsim \left[\log\left(C\left[1-(T_3+T_4)\right]^{\frac{4\beta+4}{4\beta+3}}(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1} [1-(T_3+T_4)]^{\frac{3\beta+3}{4\beta+3}} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}} \\ &\gtrsim \left[\log\left(C(n\alpha^2)^{\frac{2}{4\beta+3}}\right)\right]^{-1} (n\alpha^2)^{-\frac{2\beta}{4\beta+3}}\end{aligned}$$

The proof in the interactive scenario follows the same lines at the exception of the choice of T_1 and T_2 which should be taken as

$$T_1 = T_3 = (n\alpha^2)^{-\frac{\beta}{(a-1)(2\beta+1)}}, \quad T_2 = T_4 = (n\alpha^2)^{-\frac{\beta}{(b-1)(2\beta+1)}}.$$

Bibliography

[1] J. Acharya, C. L. Canonne, C. Freitag, and H. Tyagi. Test without Trust: Optimal Locally Private Distribution Testing. *arXiv e-prints*, art. arXiv:1808.02174, Aug. 2018.

[2] J. Acharya, Z. Sun, and H. Zhang. Differentially private testing of identity and closeness of discrete distributions. In *Advances in Neural Information Processing Systems*, pages 6878–6891, 2018.

[3] J. Acharya, C. L. Canonne, C. Freitag, and H. Tyagi. Test without trust: Optimal locally private distribution testing. In *Proceedings of Machine Learning Research*, volume 89, pages 2067–2076, 2019.

[4] M. Aliakbarpour, I. Diakonikolas, and R. Rubinfeld. Differentially private identity and equivalence testing of discrete distributions. In *International Conference on Machine Learning*, pages 169–178, 2018.

[5] M. Avella-Medina and V.-E. Brunel. Differentially private sub-gaussian location estimators. *arXiv preprint arXiv:1906.11923*, 2019.

[6] M. Bafna and J. Ullman. The price of selection in differential privacy. In *Conference on Learning Theory (COLT)*, 2007.

[7] S. Balakrishnan and L. Wasserman. Hypothesis testing for densities and high-dimensional multinomials: Sharp local minimax rates. *Annals of Statistics*, 47(4): 1893–1927, 2019.

[8] B. Barak, K. Chaudhuri, C. Dwork, S. Kale, F. McSherry, and K. Talwar. Privacy, accuracy, and consistency too: a holistic solution to contingency table release. In *Proceedings of the twenty-sixth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, pages 273–282, 2007.

[9] M. Barbaro and T. Zeller. A Face Is Exposed for AOL Searcher No. 4417749. *The New York Times*, Aug. 2006. URL https://www.nytimes.com/2006/08/09/technology/09aol.html.

[10] T. Berrett and C. Butucea. Locally private non-asymptotic testing of discrete distributions is faster using interactive mechanisms. *33, NeurIPS*, 2020.

[11] S. Boucheron, G. Lugosi, and P. Massart. *Concentration inequalities: A nonasymptotic theory of independence*. Oxford university press, 2013.

[12] C. Butucea, M. Ndaoud, N. A. Stepanova, and A. B. Tsybakov. Variable selection with Hamming loss. *The Annals of Statistics*, 46(5):1837–1875, 2018.

[13] C. Butucea, A. Dubois, M. Kroll, and A. Saumard. Local differential privacy: Elbow effect in optimal density estimation and adaptation over besov ellipsoids. *Bernoulli*, 26(3):1727–1764, 2020.

[14] C. Butucea, A. Dubois, and A. Saumard. Sharp phase transitions for exact support recovery under local differential privacy. *arXiv preprint arXiv:2011.14881*, 2020.

[15] C. Butucea, A. Rohde, and L. Steinberger. Interactive versus non-interactive locally differentially private estimation: Two elbows for the quadratic functional. *arXiv preprint arXiv:2003.04773*, 2020.

[16] B. Cai, C. Daskalakis, and G. Kamath. Priv'it: private and sample efficient identity testing. In *Proceedings of the 34th International Conference on Machine Learning-Volume 70*, pages 635–644, 2017.

[17] T. T. Cai, Y. Wang, and L. Zhang. The cost of privacy: Optimal rates of convergence for parameter estimation with differential privacy. *arXiv preprint arXiv:1902.04495*, 2019.

[18] J. Chhor and A. Carpentier. Sharp local minimax rates for goodness-of-fit testing in large random graphs, multivariate poisson families and multinomials. *arXiv preprint arXiv:2012.13766*, 2020.

[19] I. Diakonikolas and D. M. Kane. A new approach for testing properties of discrete distributions. In *2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 685–694. IEEE, 2016.

[20] Differential Privacy Team, Apple. Learning with privacy at scale. Technical report, Apple, 2017.

[21] B. Ding, J. Kulkarni, and S. Yekhanin. Collecting telemetry data privately. In *Advances in Neural Information Processing Systems*, pages 3571–3580, 2017.

[22] J. Dong, A. Roth, and W. J. Su. Gaussian differential privacy. *arXiv preprint arXiv:1905.02383*, 2019.

[23] D. L. Donoho and R. C. Liu. Geometrizing rates of convergence. II, III. *Ann. Statist.*, 19(2):633–667, 668–701, 1991.

[24] D. L. Donoho, I. M. Johnstone, G. Kerkyacharian, and D. Picard. Density estimation by wavelet thresholding. *Ann. Statist.*, 24(2):508–539, 1996.

[25] A. Dubois, T. Berrett, and C. Butucea. Goodness of fit testing for hölder continuous densities under local differential privacy. *Submitted*, 2021.

[26] J. C. Duchi and R. Rogers. Lower bounds for locally private estimation via communication complexity. In *Proceedings of the Thirty-Second Conference on Learning Theory*, volume 99 of *Proceedings of Machine Learning Research*, pages 1161–1191, 2019.

[27] J. C. Duchi and F. Ruan. The right complexity measure in locally private estimation: It is not the Fisher information. *arXiv preprint arXiv:1806.05756*, 2018.

[28] J. C. Duchi, M. I. Jordan, and M. J. Wainwright. Local privacy and statistical minimax rates. In *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, pages 429–438, 2013.

[29] J. C. Duchi, M. I. Jordan, and M. J. Wainwright. Local privacy and minimax bounds: Sharp rates for probability estimation. In *Advances in Neural Information Processing Systems*, pages 1529–1537, 2013.

[30] J. C. Duchi, M. I. Jordan, and M. J. Wainwright. Minimax optimal procedures for locally private estimation. *Journal of the American Statistical Association*, 113(521): 182–201, 2018.

[31] C. Dwork and A. Roth. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, 9(3-4):211–407, 2013.

[32] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor. Our data, ourselves: Privacy via distributed noise generation. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 486–503. Springer, 2006.

[33] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography conference*, pages 265–284. Springer, 2006.

[34] C. Dwork, G. N. Rothblum, and S. Vadhan. Boosting and differential privacy. In *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, pages 51–60. IEEE, 2010.

[35] Ú. Erlingsson, V. Pihur, and A. Korolova. Rappor: Randomized aggregatable privacy-preserving ordinal response. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, pages 1054–1067, 2014.

[36] M. Gaboardi and R. Rogers. Local private hypothesis testing: Chi-square tests. In *International Conference on Machine Learning*, pages 1626–1635, 2018.

[37] M. Gaboardi, H. Lim, R. Rogers, and S. Vadhan. Differentially private chi-squared hypothesis testing: Goodness of fit and independence testing. In *International conference on machine learning*, pages 2111–2120, 2016.

[38] E. Giné and R. Nickl. *Mathematical foundations of infinite-dimensional statistical models*. Cambridge Series in Statistical and Probabilistic Mathematics, [40]. Cambridge University Press, New York, 2016.

[39] K. Hafner. And if You Liked the Movie, a Netflix Contest May Reward You Handsomely. *The New York Times*, Oct. 2006. URL https://www.nytimes.com/2006/10/02/technology/02netflix.html.

[40] R. Hall, A. Rinaldo, and L. Wasserman. Differential privacy for functions and functional data. *Journal of Machine Learning Research*, 14:703–727, 2013.

[41] W. Härdle, G. Kerkyacharian, D. Picard, and A. Tsybakov. *Wavelets, approximation, and statistical applications*, volume 129 of *Lecture Notes in Statistics*. Springer-Verlag, New York, 1998.

[42] F. Hirsch and G. Lacombe. *Eléments d'analyse fonctionnelle: cours et exercices avec réponses*. Dunod, 2009.

[43] M. Joseph, J. Mao, S. Neel, and A. Roth. The role of interactivity in local differential privacy. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 94–105. IEEE, 2019.

[44] P. Kairouz, S. Oh, and P. Viswanath. Extremal mechanisms for local differential privacy. In *Advances in neural information processing systems*, pages 2879–2887, 2014.

[45] P. Kairouz, S. Oh, and P. Viswanath. Extremal mechanisms for local differential privacy. *The Journal of Machine Learning Research*, 17(1):492–542, 2016.

[46] P. Kairouz, S. Oh, and P. Viswanath. The composition theorem for differential privacy. *IEEE Transactions on Information Theory*, 63(6):4037–4049, 2017.

[47] S. P. Kasiviswanathan, H. K. Lee, K. Nissim, S. Raskhodnikova, and A. Smith. What can we learn privately? *SIAM Journal on Computing*, 40(3):793–826, 2011.

[48] G. Kerkyacharian, P. Petrushev, D. Picard, and T. Willer. Needlet algorithms for estimation in inverse problems. *Electronic Journal of Statistics*, 1:30–76, 2007.

[49] D. Kifer, A. Smith, and A. Thakurta. Private convex empirical risk minimization and high-dimensional regression. In *Conference on Learning Theory*, pages 25–1. JMLR Workshop and Conference Proceedings, 2012.

[50] M. Kroll. Pointwise adaptive kernel density estimation under local approximate differential privacy. *arXiv preprint arXiv:1907.06233*, 2019.

[51] J. Lam-Weil, B. Laurent, and J.-M. Loubes. Minimax optimal goodness-of-fit testing for densities and multinomials under a local differential privacy constraint. *arXiv preprint arXiv:2002.04254*, 2020.

[52] E. L. Lehmann and J. P. Romano. *Testing statistical hypotheses*. Springer Science & Business Media, 2006.

[53] F. McSherry and K. Talwar. Mechanism design via differential privacy. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*, pages 94–103. IEEE, 2007.

[54] I. Mironov. Rényi differential privacy. In *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, pages 263–275. IEEE, 2017.

[55] J. Murtagh and S. Vadhan. The complexity of computing the optimal composition of differential privacy. In *Theory of Cryptography Conference*, pages 157–175. Springer, 2016.

[56] A. Narayanan and V. Shmatikov. Robust de-anonymization of large sparse datasets. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pages 111–125. IEEE, 2008.

[57] M. Ndaoud. Sharp optimal recovery in the two component gaussian mixture model. *arXiv preprint arXiv:1812.08078*, 2018.

[58] M. Ndaoud and A. B. Tsybakov. Optimal variable selection and adaptive noisy compressed sensing. *IEEE Transactions on Information Theory*, 66(4):2517–2532, 2020.

[59] Netflix. Netflix Prize: Review Rules. URL https://web.archive.org/web/20100106185508/http://www.netflixprize.com//rules.

[60] K. Nissim, S. Raskhodnikova, and A. Smith. Smooth sensitivity and sampling in private data analysis. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 75–84, 2007.

[61] V. V. Petrov. *Limit theorems of probability theory: Sequences of independent random variables*, volume 4 of *Oxford Studies in Probability*. The Clarendon Press, Oxford University Press, New York, 1995.

[62] R. Rogers and D. Kifer. A new class of private chi-square hypothesis tests. In *Artificial Intelligence and Statistics*, pages 991–1000, 2017.

[63] A. Rohde and L. Steinberger. Geometrizing rates of convergence under local differential privacy constraints. *Annals of Statistics*, 48(5):2646–2670, 2020.

[64] R. J. Serfling. *Approximation theorems of mathematical statistics*. John Wiley & Sons, 1980.

[65] O. Sheffet. Locally private hypothesis testing. In *International Conference on Machine Learning*, pages 4605–4614. PMLR, 2018.

[66] A. Smith. Differential privacy and the secrecy of the sample. URL https://adamdsmith.wordpress.com/2009/09/02/sample-secrecy/.

[67] A. Smith. Efficient, differentially private point estimators. *arXiv preprint arXiv:0809.4794*, 2008.

[68] A. Smith. Privacy-preserving statistical estimation with optimal convergence rates. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 813–822, 2011.

[69] V. Spokoiny. Adaptive hypothesis testing using wavelets. *The Annals of Statistics*, 24(6):2477 – 2498, 1996.

[70] T. Steinke and J. Ullman. Tight lower bounds for differentially private selection. In *58th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*. 2017.

[71] L. Sweeney. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570, 2002.

[72] A. B. Tsybakov. *Introduction to nonparametric estimation*. Springer Series in Statistics. Springer, New York, 2009.

[73] J. Ullman. Cs7880: Rigorous approaches to data privacy, spring 2017. URL http://www.ccs.neu.edu/home/jullman/cs7880s17/HW1sol.pdf.

[74] J. Ullman. Tight lower bounds for locally differentially private selection. *arXiv preprint arXiv:1802.02638*, 2018.

[75] G. Valiant and P. Valiant. An automatic inequality prover and instance optimal identity testing. *SIAM Journal on Computing*, 46(1):429–455, 2017.

[76] M. J. Wainwright. *High-dimensional statistics: A non-asymptotic viewpoint*, volume 48 of *Cambridge Series in Statistical and Probabilistic Mathematics*. Cambridge University Press, Cambridge, 2019.

[77] Y. Wang, J. Lee, and D. Kifer. Revisiting differentially private hypothesis tests for categorical data. *arXiv preprint arXiv:1511.03376*, 2015.

[78] Y.-X. Wang, B. Balle, and S. P. Kasiviswanathan. Subsampled rényi differential privacy and analytical moments accountant. In *The 22nd International Conference on Artificial Intelligence and Statistics*, pages 1226–1235. PMLR, 2019.

[79] S. L. Warner. Randomized response: A survey technique for eliminating evasive answer bias. *Journal of the American Statistical Association*, 60(309):63–69, 1965.

[80] L. Wasserman and S. Zhou. A statistical framework for differential privacy. *Journal of the American Statistical Association*, 105(489):375–389, 2010.

[81] M. Ye and A. Barg. Asymptotically optimal private estimation under mean square loss. *arXiv preprint arXiv:1708.00059*, 2017.

[82] M. Ye and A. Barg. Optimal schemes for discrete distribution estimation under locally differential privacy. *IEEE Transactions on Information Theory*, 64(8):5662–5676, 2018.

[83] B. Yu. Assouad, fano, and le cam. In *Festschrift for Lucien Le Cam*, pages 423–435. Springer, 1997.

UNIVERSITE BRETAGNE LOIRE / MATHSTIC

ENSAI École nationale de la statistique et de l'analyse de l'information

Titre : Problèmes d'estimation, de sélection de variables et de tests sous contraintes de confidentialité différentielle locale

Mot clés : confidentialité différentielle locale, estimation d'une densité, identification du support, tests d'adéquation, transition de phase, vitesses minimax

Résumé : La notion de confidentialité différentielle a été introduite pour permettre de réaliser des analyses statistiques tout en fournissant des garanties de protection des données personnelles analysées. Dans cette thèse, on s'intéresse à trois problèmes d'inférence statistique sous contraintes de confidentialité différentialle locale.
Dans un premier temps, on s'intéresse à l'estimation non-paramétrique d'une densité de probabilité. Nous étudions le risque minimax $\mathbb{L}^r$ sur les ellipsoïdes de Besov $\mathcal{B}^s_{pq}(L)$, et nous intéressons à la question de l'adaptation au paramètre de régularité.
On s'intéresse ensuite à l'identification du support de l'espérance d'une variable aléatoire suivant une loi normale d-dimensionnelle. Sous des hypothèses de sparsité, nous étudions le risque minimax lié à la distance de Hamming, et en déduisons des conditions nécessaires et suffisantes pour que l'identification du support soit possible.
Enfin, nous étudions un problème de test d'adéquation pour des densités Höldériennes dont le support n'est pas supposé borné.
Pour chaque problème, nous mettons en évidence l'influence des contraintes de confidentialité sur les vitesses minimax.

Title: Estimation, variable selection and testing problems under local differential privacy constraints

Keywords: local differential privacy, density estimation, support recovery, goodness-of-fit testing, phase transition, minimax rates

Abstract: The notion of differential privacy has been introduced to enable statistical analyses to be carried out while protecting the privacy of the individuals whose data are analysed. In this thesis, three problems of statistical inference under local differential privacy constraints are considered.
First, we address the problem of nonparametric density estimation. We study the minimax risk over Besov ellipsoids $\mathcal{B}^s_{pq}(L)$ under the $\mathbb{L}^r$-risk, and we investigate adaptation to the regularity parameter.
We then consider the problem of identifying the support of the expectation of a d-dimensional gaussian random variable. Under sparsity assumptions, we study the minimax risk for the Hamming loss, and obtain necessary and sufficient conditions for support recovery to be possible.
Finally, we address a goodness-of-fit testing problem for Hölder continuous densities.
For each problem, we quantify how the local differential privacy constraints affect the classical minimax rates.