Explaining the Explainer: A First Theoretical Analysis of LIME

Damien Garreau, Ulrike von Luxburg

An Analysis of LIME for Text Data

Dina Mardaoui, Damien Garreau

Explaining the Explainer: A First Theoretical Analysis of LIME

Damien Garreau[1,3]
damien.garreau@unice.fr

Ulrike von Luxburg[1,2]
ulrike.luxburg@uni-tuebingen.de

[1]Max Planck Institute for Intelligent Systems, Germany
[2]University of Tübingen, Germany
[3]Université Côte d'Azur, Inria, CNRS, LJAD, France

Abstract

Machine learning is used more and more often for sensitive applications, sometimes replacing humans in critical decision-making processes. As such, interpretability of these algorithms is a pressing need. One popular algorithm to provide interpretability is LIME (Local Interpretable Model-Agnostic Explanation). In this paper, we provide the first theoretical analysis of LIME. We derive closed-form expressions for the coefficients of the interpretable model when the function to explain is linear. The good news is that these coefficients are proportional to the gradient of the function to explain: LIME indeed discovers meaningful features. However, our analysis also reveals that poor choices of parameters can lead LIME to miss important features.

1 Introduction

1.1 Interpretability

The recent advance of machine learning methods is partly due to the widespread use of very complicated models, for instance deep neural networks. As an example, the Inception Network (Szegedy et al., 2015) depends on approximately 23 million parameters. While these models achieve and sometimes surpass human-level performance on certain tasks (image classification being one of the most famous), they are often perceived as *black boxes*, with little understanding of how they make individual predictions.

This lack of understanding is a problem for several reasons. First, it can be a source of catastrophic errors when these models are deployed *in the wild*. For instance, for any safety system recognizing cars in images, we want to be absolutely certain that the algorithm is using features related to cars, and not exploiting some artifacts of the images. Second, this opacity prevents these models from being *socially accepted*. It is important to get a basic understanding of the decision making process to accept it.

Model-agnostic explanation techniques aim to solve this interpretability problem by providing qualitative or quantitative help to understand how black-box algorithms make decisions. Since the global complexity of the black-box models is hard to understand, they often rely on a *local* point of view, and produce an interpretation for a specific instance. In this article, we focus on such an explanation technique: **Local Interpretable Model-Agnostic Explanations** (LIME, Ribeiro et al. (2016)).

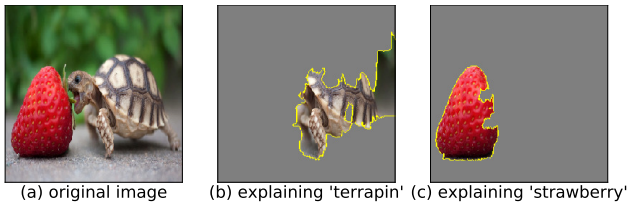

Figure 1: LIME explanation for object identification in images. We used Inception (Szegedy et al., 2015) as a black-box model. Terrapin, a sort of turtle, is the top label predicted for the image in panel (a). Panel (b) shows the results of LIME, explaining how this prediction was made. The highlighted parts of the image are the superpixels with the top coefficients in the surrogate linear model. We ran the same experiment for the 'strawberry' label in panel (c).

1.2 Contributions

Our main goal in this paper is to provide theoretical guarantees for LIME. On the way, we shed light on

Proceedings of the 23rd International Conference on Artificial Intelligence and Statistics (AISTATS) 2020, Palermo, Italy. PMLR: Volume 108.

some interesting behavior of the algorithm in a simple setting. Our analysis is based on the Euclidean version of LIME, called "tabular LIME." Our main results are the following:

(i). When the model to explain is linear, we **compute in closed-form** the average coefficients of the surrogate linear model obtained by `TabularLIME`.
(ii). In particular, these coefficients are **proportional to the partial derivatives of the black-box model** at the instance to explain. This implies that `TabularLIME` indeed highlights important features.
(iii). On the negative side, using the closed-form expressions we show that **it is possible to make some important features disappear** in the interpretation, just by changing a parameter of the method.
(iv). We also compute the local error of the surrogate model, and show that it is **bounded** away from 0 in general.

We explain how `TabularLIME` works in more details in Section 2. In Section 3, we state our main results. They are discussed in Section 4, and we provide an outline of the proof of our main result in Section 5. We conclude in Section 6.

2 LIME: Outline and notation

2.1 Intuition

From now on, we will consider a particular model encoded as a function $f : \mathbb{R}^d \to \mathbb{R}$ and a particular instance $\xi \in \mathbb{R}^d$ to explain. We make no assumptions on this function, *e.g.*, how it might have been learned. We simply consider f as a black-box model giving us predictions for all points of the input space. Our goal will be to explain the decision $f(\xi)$ that this model makes for one particular instance ξ.

As soon as f is too complicated, it is hopeless to try and fit an interpretable model globally, since the interpretable model will be too simple to capture all the complexity of f. Thus a reasonable course of action is to consider a *local* point of view, and to explain f in the neighborhood of some fixed instance ξ. This is the main idea behind LIME: To explain a decision for some fixed input ξ, sample other examples around ξ, use these samples to build a simple interpretable model in the neighborhood of ξ, and use this surrogate model to explain the decision for ξ.

One additional idea that makes a huge difference with other existing methods is to use *discretized* features of smaller dimension d' to build the local model. These new categorical features are easier to interpret, since they are categorical. In the case of images, they are built by using a split of the image ξ into superpixels (Ren and Malik, 2003). See Figure 1 for an example of LIME output in the case of image classification. In this situation, the surrogate model highlights the superpixels of the image that are the most "active" in predicting a given label.

Whereas LIME is most famous for its results on images, it is easier to understand how it operates and to analyze theoretically on **tabular data**. In the case of tabular data, LIME works essentially in the same way, with a main difference: tabular LIME requires a train set, and each feature is discretized according to the empirical quantiles of this training set.

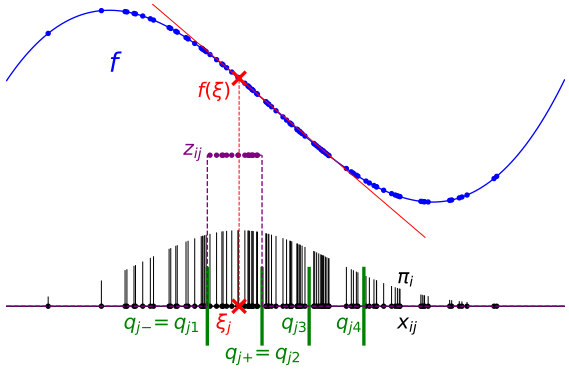

Figure 2: General setting of `TabularLIME` along coordinate j. Given a specific datapoint ξ (in red), we want to build a local model for f (in blue), given new samples $x_1, \dots, x_n$ (in black). Discretizing with respect to the quantiles of the distribution (in green), these new samples are transformed into categorical features z_i (in purple). In the construction of the surrogate model, they are weighted with respect to their proximity with ξ (here exponential weights given by Eq. (2.1), in black). In red, we plotted the tangent line, the best linear approximation one could hope for.

We now describe the general operation of LIME on Euclidean data, which we call `TabularLIME`. We provide synthetic description of `TabularLIME` in Algorithm 1, and we refer to Figure 2 for a depiction of our setting along a given coordinate. Suppose that we want to explain the prediction of the model f at the instance ξ. `TabularLIME` has an intricate way to sample points in a local neighborhood of ξ. First, `TabularLIME` constructs empirical quantiles of the train set on each dimension, for a given number p of bins. These quantile boxes are then used to construct a discrete representation of the data: if ξ_j falls between $\hat{q}_k$ and $\hat{q}_{k+1}$, it receives the value k. We now have a discrete version of ξ, say $(2, 3, \dots)^\top$. The next step is to sample discrete examples in $\{1, \dots, p\}^d$ uniformly at random: for instance, $(1, 3, \dots)^\top$ means that `TabularLIME` sampled an encoding such that the first coordinate falls into

the first quantile box, the second coordinate into the third, etc. `TabularLIME` subsequently un-discretizes these encodings by sampling from a normal distribution truncated to the corresponding quantile boxes, obtaining *new examples* $x_1, \dots, x_n$. For example, for sample $(1, 3, \dots)^\top$ we now sample the first coordinate from a normal distribution restricted to quantile box #1, the second coordinate from quantile box #3, etc. This sampling procedure ensures that we have samples in each part of the space. The next step is to convert these sampled points to binary features, indicating for each coordinate if the new example falls into the same quantile box as ξ. Here, z_i would be $(1, 0, \dots)^\top$. Finally, an interpretable model (say linear) is learned using these binary features.

Algorithm 1 `TabularLIME` for regression

Require: Model f, # of new samples n, instance ξ, bandwidth ν, # of bins p, mean μ, variance σ^2

$q \leftarrow$ `GetQuantiles`(p,μ,σ)
$t \leftarrow$ `Discretize`(ξ,q)
for $i = 1$ to n **do**
  for $j = 1$ to d **do**
    $y_{i,j} \leftarrow$ `SampleUniform`$(\{1, \dots, p\})$
    $(q_\ell, q_u) \leftarrow (q_{j,y_{ij}}, q_{j,y_{ij}+1})$
    $x_{i,j} \leftarrow$ `SampleTruncGaussian`$(q_\ell, q_u, \mu, \sigma)$
    $z_{i,j} \leftarrow \mathbf{1}_{t_j = y_{i,j}}$
  end for
  $\pi_i \leftarrow \exp\left(\frac{-\|x_i - \xi\|^2}{2\nu^2}\right)$
end for
$\widehat{\beta} \leftarrow$ `WeightedLeastSquares`$(z, f(x), \pi)$
return $\widehat{\beta}$

2.2 Implementation choices and notation

LIME is a quite general framework and leaves some freedom to the user regarding each brick of the algorithm. We now discuss each step of `TabularLIME` in more detail, presenting our implementation choices and introducing our notation on the way.

Discretization. As said previously, the first step of `TabularLIME` is to create a partition of the input space using a train set. Intuitively, `TabularLIME` produces *interpretable features* by discretizing each dimension. Formally, given a fixed number of bins p, for each feature j, the empirical quantiles $\hat{q}_{j,0}, \dots, \hat{q}_{j,p}$ are computed. Thus, along each dimension, there is a mapping $\hat{\phi}_j : \mathbb{R} \to \{1, \dots, p\}$ associating each real number to the index of the quantile box it belongs to. For any point $x \in \mathbb{R}^d$, the interpretable features are then defined as a $0-1$ vector corresponding to the discretization of x being the same as the discretization of ξ. Namely, $z_j = \mathbf{1}_{\hat{\phi}_j(x) = \hat{\phi}_j(\xi)}$ for all $1 \leqslant j \leqslant d$. Intuitively, these categorical features correspond to the *absence* or *presence* of interpretable components. The discretization process makes a huge difference with respect to other methods: we lose the obvious link with the gradient of the function, and it is much more complicated to see how the local properties of f influence the result of the LIME algorithm, even in a simple setting. In all our experiments, we took $p = 4$ (quartile discretization, the default setting).

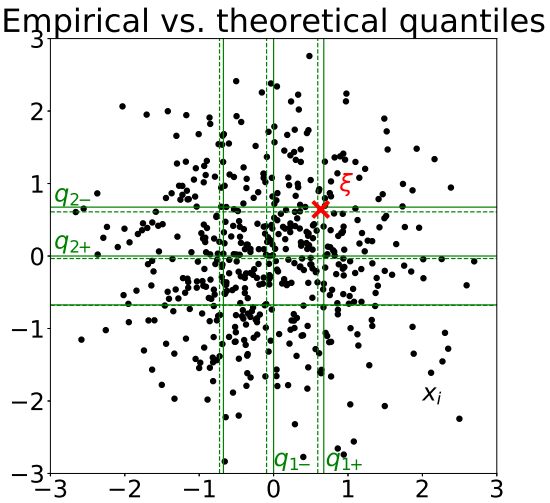

Figure 3: A visualization of the train set in dimension $d = 2$ with $\mu = (0, 0)^\top$, and $\sigma^2 = 1$. The empirical quantiles (dashed green lines) are already very close to the theoretical quantiles (green lines) for $n_{\text{train}} = 500$. The main difference in the procedure appears if ξ (red cross) is chosen at the edge of a quantile box, changing the way all the new samples are encoded. But for a train set containing enough observations and a generic ξ, there is virtually no difference between using the theoretical quantiles and the empirical quantiles.

Sampling strategy. Along with $\hat{\phi}$, `TabularLIME` creates an un-discretization procedure $\hat{\psi} : \{1, \dots, p\} \to \mathbb{R}$. Simply put, given a coordinate j and a bin index k, $\hat{\psi}_j(k)$ samples a truncated Gaussian on the corresponding bin, with parameters computed from the training set. The `TabularLIME` sampling strategy for a new example amounts to (i) sample $y_i \in \{1, \dots, p\}^d$ a random variable such that the y_{ij} are independent samples of the discrete uniform distribution on $\{1, \dots, p\}$, and (ii) apply the un-discretization step, that is, return $\hat{\psi}(y)$. We will denote by $x_1, \dots, x_n \in \mathbb{R}^d$ these new examples, and $z_1, \dots, z_n \in \{0, 1\}^d$ their discretized counterparts. Note that it is possible to take other bin boxes than those given by the empirical quantiles, the y_{ij}s are then sampled according to the frequency observed in the dataset. The sampling step of `TabularLIME` helps to explore the values of the function in the neighborhood of the instance to explain. Thus it is not so important to sample according to the distribution of the data,

and a Gaussian sampling that mimics it is enough.

Assuming that we know the distribution of the train data, it is possible to use the theoretical quantiles instead of the empirical ones. For a large number of examples, they are arbitrary close (see, for instance, Lemma 21.2 in Van der Vaart (2000)). See Figure 3 for an illustration. It is this approach that we will take from now on: we denote the discretization step by ϕ and denote the quantiles by q_{jk} for $1 \leqslant j \leqslant d$ and $0 \leqslant k \leqslant p$ to mark this slight difference. Also note that, for every $1 \leqslant j \leqslant d$, we set $q_{j\pm}$ the quantiles bounding ξ_j, that is, $q_{j-} \leqslant \xi_j < q_{j+}$ (see Figure 2).

Train set. `TabularLIME` requires a train set, which is left free to the user. In spirit, one should sample according to the distribution of the train set used to fit the model f. Nevertheless, this train set is rarely available, and from now on, we choose to consider draws from a $\mathcal{N}\left(\mu, \sigma^2 \mathrm{I}_d\right)$. The parameters of this Gaussian can be estimated from the training data that was used for f if available. Thus, in our setting, along each dimension j, the $(q_{jk})_{0\leqslant k\leqslant p}$ are the (rescaled) quantiles of the normal distribution. In particular, they are identical for all features. A fundamental consequence is that sampling the new examples x_is first and then discretizing **has the same distribution** as sampling first the bin indices y_is and then un-discretizing.

Weights. We choose to give each example the weight

$$\pi_i := \exp\left(\frac{-\|x_i - \xi\|^2}{2\nu^2}\right), \tag{2.1}$$

where $\|\cdot\|$ is the Euclidean norm on $\mathbb{R}^d$ and $\nu > 0$ is a bandwidth parameter. It should be clear that ν is a hard parameter to tune:

- if ν is very large, then **all the examples receive positive weights:** we are trying to build a simple model that captures the complexity of f at a global scale. This cannot work if f is too complicated.
- if ν is too small, then **only examples in the immediate neighborhood of** ξ receive positive weights. Given the discretization step, this amounts to choosing $z_i = (1, \ldots, 1)^\top$ for all i. Thus the linear model built on top would just be a constant fit, missing all the relevant information.

Note that other distances than the Euclidean distance can be used, for instance the cosine distance for text data. The default implementation of LIME uses $\|z_i - t\|$ instead of $\|x_i - \xi\|$, with bandwidth set to $0.75d$. We choose to use the true Euclidean distance between ξ and the new examples as it can be seen as a smoothed version of the distance to z_i and has the same behavior.

Interpretable model. The final step in `TabularLIME` is to build a local interpretable model. Given a class of simple, interpretable models G, `TabularLIME` selects the best of these models by solving

$$\operatorname*{arg\,min}_{g\in G}\left\{L_n(f, g, \pi_\xi) + \Omega\left(g\right)\right\}, \tag{2.2}$$

where L_n is a local loss function evaluated on the new examples $x_1, \ldots, x_n$, and $\Omega : \mathbb{R}^d \to \mathbb{R}$ is a regularizer function. For instance, a natural choice for the local loss function is the weighted squared loss

$$L_n(f, g, \pi) := \frac{1}{n}\sum_{i=1}^{n} \pi_i \left(f(x_i) - g(z_i)\right)^2 . \tag{2.3}$$

We saw in Section 1.1 different possibilities for G. In this paper, we will focus exclusively on the linear models, in our opinion the easiest models to interpret. Namely, we set $g(z_i) = \beta^\top z_i + \beta_0$, with $\beta \in \mathbb{R}^d$ and $\beta_0 \in \mathbb{R}$. To get rid of the intercept β_0, we now use the standard approach to introduce a phantom coordinate 0, and $z, \beta \in \mathbb{R}^{d+1}$ with $z_0 = 1$ and $\beta_0 = \beta_0$. We also stack the z_is together to obtain $Z \in \{0, 1\}^{n\times(d+1)}$.

The regularization term $\Omega(g)$ is added to insure further interpretability of the model by reducing the number of non-zero coefficients in the linear model given by `TabularLIME`. Typically, one uses L^2 regularization (ridge regression is the default setting of LIME) or L^1 regularization (the Lasso). To simplify the analysis, we will set $\Omega = 0$ in the following. We believe that many of the results of Section 3 stay true in a regularized setting, especially the switch-off phenomenon that we are going to describe below: coefficients are even more likely to be set to zero when $\Omega \neq 0$.

In other words, in our case `TabularLIME` performs *weighted linear regression* on the interpretable features z_is, and outputs a vector $\widehat{\beta} \in \mathbb{R}^{d+1}$ such that

$$\widehat{\beta} \in \operatorname*{arg\,min}_{\beta\in\mathbb{R}^{d+1}} \left\{\frac{1}{n}\sum_{i=1}^{n} \pi_i (y_i - \beta^\top z_i)^2\right\} . \tag{2.4}$$

Note that $\widehat{\beta}$ is a random quantity, with randomness coming from the sampling of the new examples $x_1, \ldots, x_n$. It is clear that from a theoretical point of view, a big hurdle for the theoretical analysis is the discretization process (going from the x_is to the z_is).

Regression vs. classification. To conclude, let us note that `TabularLIME` can be used both for regression and classification. Here we focus on the *regression* mode: the outputs of the model are real numbers, and not discrete elements. In some sense, this is a more general setting than the classification case, since the classification mode operates as `TabularLIME` for

regression, but with f chosen as the function that gives the likelihood of belonging to a certain class according to the model.

2.3 Related work

Let us mention a few other model-agnostic methods that share some characteristics with LIME. We refer to Guidotti et al. (2019) for a thorough review.

Shapley values. Following Shapley (1953) the idea is to estimate for each subset of features S the expected prediction difference $\Delta(S)$ when the value of these features are *fixed* to those of the example to explain. The contribution of the jth feature is then set to an average of the contribution of j over all possible coalitions (subgroups of features not containing j). They are used in some recent interpretability work, see Lundberg and Lee (2017) for instance. It is extremely costly to compute, and does not provide much information as soon as the number of features is high. Shapley values share with LIME the idea of quantifying how much a feature contributes to the prediction for a given example.

Gradient methods. Also related to LIME, *gradient-based* methods as in Baehrens et al. (2010) provide local explanations without knowledge of the model. Essentially, these methods compute the partial derivatives of f at a given example. For images, this can yield satisfying plots where, for instance, the contours of the object appear: a *saliency map* (Zeiler and Fergus, 2014). Shrikumar et al. (2016, 2017) propose to use the "input × derivative" product, showing advantages over gradient methods. But in any case, the output of these gradient based methods is not so interpretable since the number of features is so high. LIME gets around this problem by using a local dictionary with much smaller dimensionality than the input space.

3 Theoretical value of the coefficients of the surrogate model

We are now ready to state our main result. Let us denote by $\widehat{\beta}$ the coefficients of the linear surrogate model obtained by `TabularLIME`. In a nutshell, when the underlying model f is linear, we can derive the average value β of the $\widehat{\beta}$ coefficients. In particular, we will see that the β_js are proportional to the partial derivatives $\partial_j f(\xi)$. The exact form of the proportionality coefficients is given in the formal statement below, it essentially depends on the scaling parameters

$$\tilde{\mu} := \frac{\nu^2\mu + \sigma^2\xi}{\nu^2+\sigma^2} \in \mathbb{R}^d \text{ and } \tilde{\sigma} := \frac{\nu^2\sigma^2}{\nu^2+\sigma^2} > 0\,,$$

and the $q_{j\pm}$s, the quantiles left and right of the ξ_js.

Theorem 3.1 (Coefficients of the surrogate model, theoretical values). *Assume that f is of the form $x \mapsto a^\top x + b$, and set*

$$\beta := \begin{pmatrix} f(\tilde{\mu}) + \sum_{j=1}^d \frac{a_j\theta_j}{1-\alpha_j} \\ \frac{-a_1\theta_1}{\alpha_1(1-\alpha_1)} \\ \vdots \\ \frac{-a_d\theta_d}{\alpha_d(1-\alpha_d)} \end{pmatrix} \in \mathbb{R}^{d+1}\,, \tag{3.1}$$

where, for any $1 \leqslant j \leqslant d$, we defined

$$\alpha_j := \left[\frac{1}{2}\mathrm{erf}\left(\frac{x-\tilde{\mu}_j}{\tilde{\sigma}\sqrt{2}}\right)\right]_{q_{j-}}^{q_{j+}},$$

and

$$\theta_j := \left[\frac{\tilde{\sigma}}{\sqrt{2\pi}}\exp\left(\frac{-(x-\tilde{\mu}_j)^2}{2\tilde{\sigma}^2}\right)\right]_{q_{j-}}^{q_{j+}}.$$

Let $\eta \in (0,1)$. Then, with high probability greater than $1-\eta$, it holds that

$$\left\|\widehat{\beta} - \beta\right\| \lesssim \max(\sigma\left\|\nabla f\right\|, f(\tilde{\mu}) + \tilde{\sigma}\left\|\nabla f\right\|)\sqrt{\frac{\log 1/\eta}{n}}\,.$$

A precise statement with the accurate dependencies in the dimension and the constants hidden in the result can be found in the Appendix (Theorem 10.1). Before discussing the consequences of Theorem 3.1 in the next section, remark that since ξ is encoded by $(1,1,\ldots,1)^\top$, the prediction of the local model at ξ, $\hat{f}(\xi)$, is just the sum of the $\widehat{\beta}_j$s. According to Theorem 3.1, $\hat{f}(\xi)$ will be close to this value, with high probability. Thus we also have a statement about the error made by the surrogate model in ξ.

Corollary 3.1 (Local error of the surrogate model). *Let $\eta \in (0,1)$. Then, under the assumptions of Theorem 3.1, with probability greater than $1-\eta$, it holds that*

$$\left|\hat{f}(\xi) - f(\tilde{\mu}) + \sum_{j=1}^d \frac{a_j\theta_j}{\alpha_j}\right| \leqslant$$

$$\leqslant \max(\sigma\left\|\nabla f\right\|, f(\tilde{\mu}) + \tilde{\sigma}\left\|\nabla f\right\|)\sqrt{\frac{\log 1/\eta}{n}}\,,$$

with hidden constants depending on d and the α_js.

Obviously the goal of `TabularLIME` is not to produce a very accurate model, but to provide interpretability. The error of the local model can be seen as a hint about how reliable the interpretation might be.

4 Consequences of our main results

We now discuss the consequences of Theorem 3.1 and Corollary 3.1.

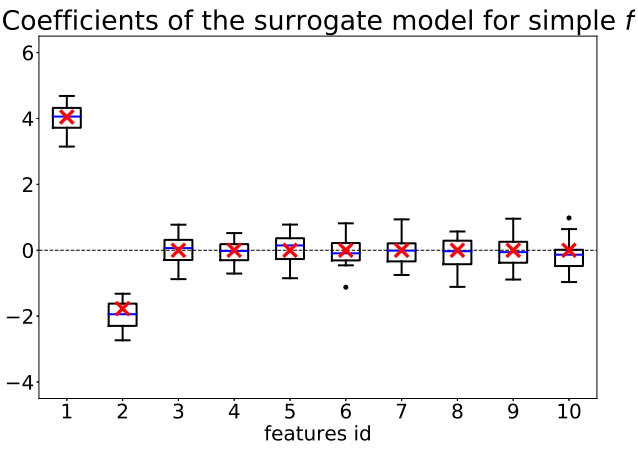

Figure 4: Example where the true underlying black box model only depends on *two* features: $f(x) = 10x_1 - 10x_2$. For each of the 10 features, we plot the values of the $\widehat{\beta}_j$s obtained by `TabularLIME`. The blue line shows the median over all experiments, the red cross the β_j theoretical value according to our theorem. The boxplots contain values between first and third quartiles, the whiskers are 1.5 times the interquartile ranges, and the black dots mark values outside this range. To produce the figure, we made 20 repetitions of the experiment, with $n = 10^4$ examples and $\nu = 1$. We see that `TabularLIME` finds nonzero coefficients exactly for the first two coordinates, up to noise coming from the sampling. This is the result that one would hope to achieve, and also the result predicted by our theory.

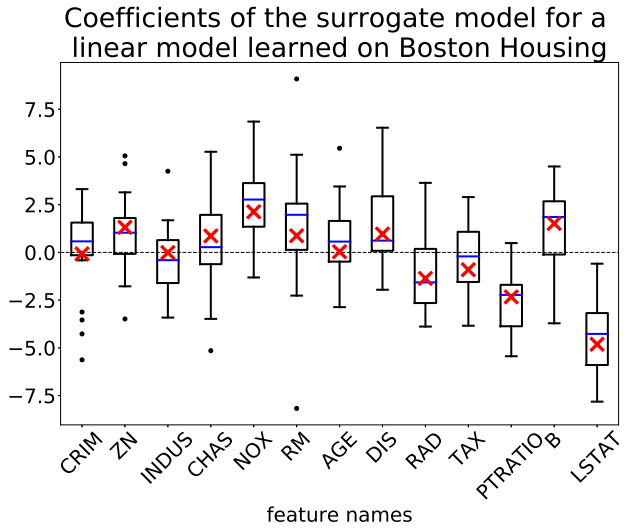

Figure 5: Values of the coefficients obtained by `TabularLIME` on each coordinate in dimension $d = 13$ for a linear model trained on the Boston housing dataset (Harrison Jr. and Rubinfeld, 1978). The β_js are concentrated around the red crosses, which denote the β_js, the theoretical values predicted by Theorem 3.1. To produce the figure, we ran 20 experiments with $n = 10^3$ new samples generated for each run and we set $\nu = 1$.

Dependency in the partial derivatives. A first consequence of Theorem 3.1 is that the coefficients of the linear model given by `TabularLIME` are approximately **proportional to the partial derivatives of** f at ξ, with constant depending on our assumptions. An interesting follow-up is that, if f depends only on a few features, then the partial derivatives in the other coordinates are zero, and the coefficients given by `TabularLIME` for these coordinates will be 0 as well. For instance, if $f(x) = 10x_1 - 10x_2$ as in Figure 4, then $\beta_1 \simeq 11.4$, $\beta_2 \simeq -4.1$, and $\beta_j = 0$ for all $j \geqslant 3$. In a simple setting, we thus showed that `TabularLIME` does not produce interpretations with additional erroneous feature dependencies. Indeed, when the number of samples is high, the coordinates which do not influence the prediction will have a coefficient close to the theoretical value 0 in the surrogate linear model. For a bandwidth not too large, this dependency in the partial derivatives seems to hold to some extent for more general functions. See for instance Figure 6, where we demonstrate this phenomenon for a kernel regressor.

Robustness of the explanations. Theorem 3.1 means that, for large n, `TabularLIME` outputs coefficients that are very close to β with high probability, where β is a vector that can be computed explicitly as per Eq. (3.1). Still without looking too closely at the values of β, this is already interesting and hints that there is some robustness in the interpretations provided by `TabularLIME`: given enough samples, the explanation will not jump from one feature to the other. This is a desirable property for any interpretable method, since the user does not want explanations to change randomly with different runs of the algorithm. We illustrate this phenomenon in Figure 5.

Influence of the bandwidth. Unfortunately, Theorem 3.1 does not provide directly a founded way to pick ν, which would for instance minimize the variance for a given level of noise. The quest for a founded heuristic is still open. However, we gain some interesting insights on the role of ν. Namely, for fixed ξ, μ, and σ, the multiplicative constants $\theta_j/(\alpha_j(1-\alpha_j))$ appearing in Eq. (3.1) depend essentially on ν.

Without looking too much into these constants, one can already see that they regulate the magnitude of the coefficients of the surrogate model in a non-trivial way. For instance, in the experiment depicted in Figure 4, the partial derivative of f along the two first coordinate has the same magnitude, whereas the interpretable coefficient is much larger for the first coordinate than the second. Thus we believe that the value of the coefficients in the obtained linear model should not be taken too much into account.

More disturbing, it is possible to artificially (or by

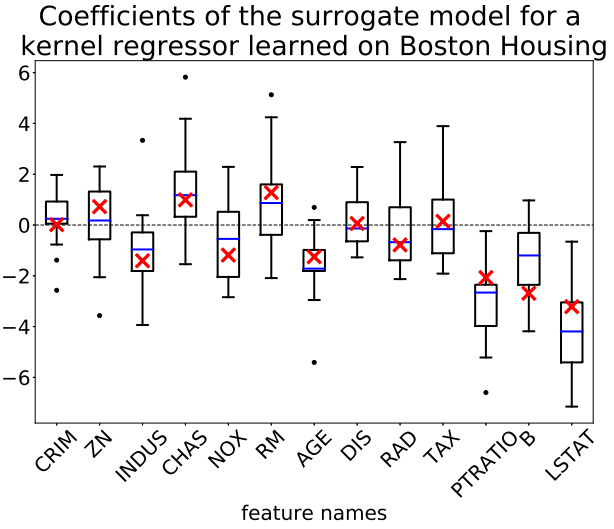

Figure 6: Values of the coefficients obtained by `TabularLIME` on each coordinate. We used the same settings as in Figure 5, but this time we train a *kernel ridge* regressor on the Boston Housing dataset—a nonlinear function. For the ridge regression, we used the Gaussian kernel with scale parameter set to 5 and default regularization constant ($\alpha = 1$). We then estimated the partial derivatives of f at ξ and reported the corresponding β_js in red. For the chosen bandwidth (we took $\nu = 1$), the experiments seem to roughly agree with our theory.

accident) put θ_j to zero, therefore **forgetting** about feature j in the explanation, whereas it could play an important role in the prediction. To see why, we have to return to the definition of the θ_js: since $q_{j-} < q_{j+}$ by construction, to have $\theta_j = 0$ is possible only if

$$V_{\text{crit}} := \sigma^2 \frac{2\xi_j - q_{j-} - q_{j+}}{-2\mu_j + q_{j-} + q_{j+}} > 0\,, \qquad (4.1)$$

and ν^2 is set to V_{crit}. We demonstrate this switching-off phenomenon in Figure 7. An interesting take is that ν not only decides at which scale the explanation is made, but also the magnitude of the coefficients in the interpretable model, even for small changes of ν.

Error of the surrogate model. A simple consequence of Corollary 3.1 is that, unless some cancellation happens between in the term $f(\tilde{\mu}) - \sum_j \frac{a_j \theta_j}{\alpha_j}$, **the local error of the surrogate model is bounded away from zero**. For instance, as soon as $\tilde{\mu} \neq \mu$, it is the general situation. Therefore, the surrogate model produced by `TabularLIME` is not *accurate* in general. We show some experimental results in Figure 8.

Finally, we discuss briefly the limitations of Theorem 3.1.

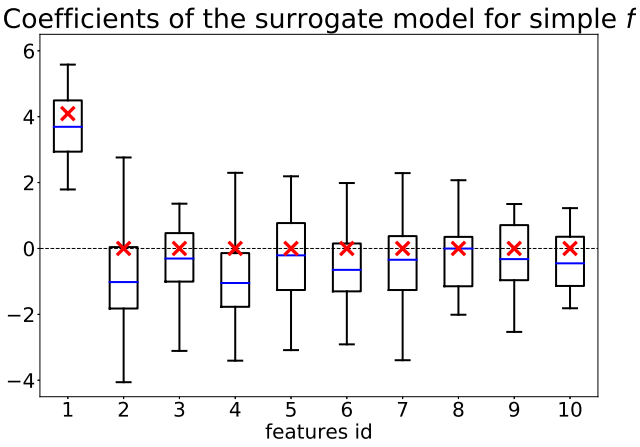

Figure 7: Values of the coefficients given by LIME. In this experiment, we took exactly the same setting as in Figure 4, but this time set the bandwidth to $\nu = 0.53$ instead of 1. In that case, the second feature is switched-off by `TabularLIME`. Note that it is not the case that ν is too small and that we are in a degenerated case: `TabularLIME` still puts a nonzero coefficient on the first coordinate.

Linearity of f. The linearity of f is a quite restrictive assumption, but we think that it is useful to consider for two reasons.

First, the weighted nature of the procedure means that `TabularLIME` is not considering examples that are too far away from ξ with respect to the scaling parameter ν. Thus it is truly a *local* assumption on f, that could be replaced by a boundedness assumption on the Hessian of f in the neighborhood of ξ, at the price of more technicalities and assuming that ν is not too large. See, in particular, Lemma 11.3 in the Appendix, after which we discuss an extension of the proof when f is linear with a second degree perturbative term. We show in Figure 6 how our theoretical predictions behave for a non-linear function (a kernel ridge regressor).

Second, our main concern is to know whether `TabularLIME` operates correctly in a simple setting, and not to provide bounds for the most general f possible. Indeed, if we can already show imperfect behavior for `TabularLIME` when f is linear as seen earlier, our guess is that such behavior will only worsen for more complicated f.

Sampling strategy. In our derivation, we use the theoretical quantiles of the Gaussian distribution along each axis, and not prescribed quantiles. We believe that the proof could eventually be adapted, but that the result would loose in clarity. Indeed, the computations for a truncated Gaussian distribution are far more convoluted than for a Gaussian distribution. For instance, in the proof of Lemma 8.1 in the Appendix, some complicated quantities depending on the prescribed

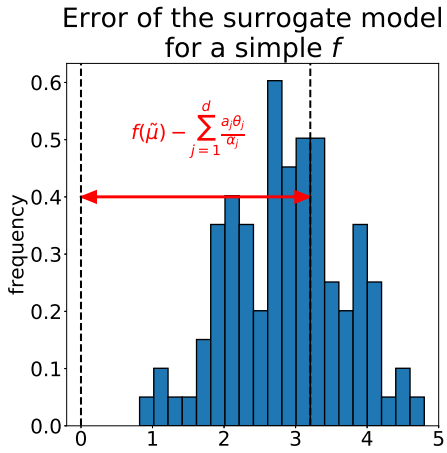

Figure 8: Histogram of the errors $\hat{f}(\xi) - f(\xi)$. The setting is the same as in Figure 4, but we repeated the experiment 100 times. The red double arrow marks the value given by Corollary 3.1 around which the local error concentrate. With high probability, the error of the surrogate model is bounded away from 0.

quantiles would appear when computing $\mathbb{E}[\pi_i z_{ik}]$.

5 Proof of Theorem 3.1

In this section, we explain how Theorem 3.1 is obtained. All formal statements and proofs are in the Appendix.

Outline. The main idea underlying the proof is to realize that $\widehat{\beta}$ is the solution of a weighted least squares problem. Denote by $\Pi \in \mathbb{R}^{n\times n}$ the diagonal matrix such that $\Pi_{ii} = \pi_i$ (the *weight matrix*), and set $f(x) \in \mathbb{R}^{d+1}$ the response vector. Then, taking the gradient of Eq. (5.1), one obtains the key equation

$$(Z^\top \Pi Z)\widehat{\beta} = Z^\top \Pi f(x)\,. \tag{5.1}$$

Let us define $\widehat{\Sigma} := \frac{1}{n} Z^\top \Pi Z$ and $\widehat{\Gamma} := \frac{1}{n} Z^\top \Pi f(x)$, as well as their population counterparts $\Sigma := \mathbb{E}[\widehat{\Sigma}]$ and $\Gamma := \mathbb{E}[\widehat{\Gamma}]$. Intuitively, if we can show that $\widehat{\Sigma}$ and $\widehat{\Gamma}$ are close to Σ and Γ, assuming that Σ is invertible, then we can show that $\widehat{\beta}$ is close to $\beta := \Sigma^{-1}\Gamma$.

The main difficulties in the proof come from the **non-linear** nature of the new features z_i, introducing tractable but challenging integrals. Fortunately, the Gaussian sampling of LIME allows us to overcome these challenges (at the price of heavy computations).

Covariance matrix. The first part of our analysis is thus concerned with the study of the empirical covariance matrix $\widehat{\Sigma}$. Perhaps surprisingly, it is possible to compute the population version of $\widehat{\Sigma}$:

$$\Sigma = C_d \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_d \\ \alpha_1 & \alpha_1 & & \alpha_i\alpha_j \\ \vdots & & \ddots & \\ \alpha_d & \alpha_i\alpha_j & & \alpha_d \end{pmatrix},$$

where the α_js were defined in Section 3, and C_d is a scaling constant that does not appear in the final result (see Lemma 8.1).

Since the α_js are always distinct from 0 and 1, the special structure of Σ makes it possible to invert it in closed-form. We show in Lemma 8.2 that

$$C_d^{-1} \begin{pmatrix} 1 + \sum_{j=1}^d \frac{\alpha_j}{1-\alpha_j} & \frac{-1}{1-\alpha_1} & \cdots & \frac{-1}{1-\alpha_d} \\ \frac{-1}{1-\alpha_1} & \frac{1}{\alpha_1(1-\alpha_1)} & & 0 \\ \vdots & & \ddots & \\ \frac{-1}{1-\alpha_d} & 0 & & \frac{1}{\alpha_d(1-\alpha_d)} \end{pmatrix}.$$

We then achieve control of $\left\|\widehat{\Sigma}^{-1} - \Sigma^{-1}\right\|_{\text{op}}$ *via* standard concentration inequalities, since the new samples are Gaussian and the binary features are *bounded* (see Proposition 8.1).

Right-hand side of Eq. (5.1)**.** Again, despite the non-linear nature of the new features, it is possible to compute the expected version of $\widehat{\Gamma}$ in our setting. In this case, we show in Lemma 9.1 that

$$\Gamma = C_d \begin{pmatrix} f(\tilde{\mu}) \\ \alpha_1 f(\tilde{\mu}) - a_1\theta_1 \\ \vdots \\ \alpha_d f(\tilde{\mu}) - a_d\theta_d \end{pmatrix},$$

where the θ_js were defined in Section 3. They play an analogous role to the α_js but, as noted before, they are signed quantities. As with the analysis of the covariance matrix, since the weights and the new features are bounded, it is possible to show a concentration result for $\widehat{\Gamma}$ (see Lemma 9.3).

Concluding the proof. We can now conclude, first upper bounding $\left\|\widehat{\beta} - \Sigma^{-1}\Gamma\right\|$ by

$$\left\|\widehat{\Sigma}^{-1}\right\|_{\text{op}} \left\|\widehat{\Gamma} - \Gamma\right\| + \left\|\widehat{\Sigma}^{-1} - \Sigma^{-1}\right\|_{\text{op}} \|\Gamma\|\,,$$

and then controlling each of these terms using the previous concentration results. The expression of β is simply obtained by multiplying Σ^{-1} and Γ.

6 Conclusion and future directions

In this paper we provide the first theoretical analysis of LIME, with some good news (LIME discovers interesting features) and bad news (LIME might forget

some important features and the surrogate model is not faithful). All our theoretical results are verified by simulations.

For future work, we would like to complement these results in various directions: Our main goal is to extend the current proof to any function by replacing f by its Taylor expansion at ξ. On a more technical side, we would like to extend our proof to other distance functions (*e.g.*, distances between the z_is and ξ, which is the default setting of LIME), to non-isotropic sampling of the x_is (that is, σ not constant across the dimensions), and to ridge regression.

Acknowledgements

The authors would like to thank Christophe Biernacki for getting them interested in the topic, as well as Leena Chennuru Vankadara for her careful proofreading. This work has been supported by the German Research Foundation through the Institutional Strategy of the University of Tübingen (DFG, ZUK 63), the Cluster of Excellence "Machine Learning—New Perspectives for Science" (EXC 2064/1 number 390727645), and the BMBF Tuebingen AI Center (FKZ: 01IS18039A).

Bibliography

D. Baehrens, T. Schroeter, S. Harmeling, M. Kawanabe, K. Hansen, and K.-R. Müller. How to explain individual classification decisions. *Journal of Machine Learning Research*, 11(6):1803–1831, 2010.

S. Boucheron, G. Lugosi, and P. Massart. *Concentration inequalities: A nonasymptotic theory of independence*. Oxford University Press, 2013.

R. Guidotti, A. Monreale, S. Ruggieri, F. Turini, F. Giannotti, and D. Pedreschi. A survey of methods for explaining black box models. *ACM Computing Surveys*, 51(5):93, 2019.

D. Harrison Jr. and D. L. Rubinfeld. Hedonic housing prices and the demand for clean air. *Journal of environmental economics and management*, 5(1):81–102, 1978.

S. M. Lundberg and S.-I. Lee. A unified approach to interpreting model predictions. In *NeurIPS*, 2017.

D. P. O'Leary and G. W. Stewart. Computing the eigenvalues and eigenvectors of arrowhead matrices. *Journal of Computational Physics*, 90:497–505, 1996.

X. Ren and J. Malik. Learning a classification model for segmentation. In *ICCV*, 2003.

M. T. Ribeiro, S. Singh, and C. Guestrin. Why should I trust you? explaining the predictions of any classifier. In *SIGKDD*, 2016.

L. S. Shapley. A value for n-person games. *Contributions to the Theory of Games*, 2(28):307–317, 1953.

A. Shrikumar, P. Greenside, A. Shcherbina, and A. Kundaje. Not just a black box: Learning important features through propagating activation differences. *arXiv preprint arXiv:1605.01713*, 2016.

A. Shrikumar, P. Greenside, and A. Kundaje. Learning important features through propagating activation differences. In *ICML*, 2017.

C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich. Going deeper with convolutions. In *CVPR*, 2015.

A. W. Van der Vaart. *Asymptotic Statistics*. Cambridge University Press, 2000.

M. J. Wainwright. *High-dimensional statistics: a non-asymptotic viewpoint*. Cambridge University Press, 2019.

H. Weyl. Das asymptotische Verteilungsgesetz der Eigenwerte linearer partieller Differentialgleichungen (mit einer Anwendung auf die Theorie der Hohlraumstrahlung). *Mathematische Annalen*, 71(4):441–479, 1912.

M. D. Zeiler and R. Fergus. Visualizing and understanding convolutional networks. In *ECCV*, pages 818–833, 2014.

Supplementary material for:

Explaining the Explainer: A First Theoretical Analysis of LIME

In this supplementary material, we provide the proof of Theorem 3.1 of the main paper. It is a simplified version of Theorem 10.1. We first recall our setting in Section 7. Then, following Section 5 of the main paper, we study the covariance matrix in Section 8, and the right-hand side of the key equation (5.1) in Section 9. Finally, we state and prove Theorem 10.1 in Section 10. Some technical results (mainly Gaussian integrals computation) and external concentration results are collected in Section 11.

7 Setting

Let us recall briefly the main assumptions under which we prove Theorem 3.1. Recall that they are discussed in details in Section 2.2 of the main paper.

H1 (Linear f). The black-box model can be written $a^\top x + b$, with $a \in \mathbb{R}^d$ and $b \in \mathbb{R}$ fixed.

H2 (Gaussian sampling). The random variables $x_1, \dots, x_n$ are i.i.d. $\mathcal{N}\left(\mu, \sigma^2 \mathrm{I}_d\right)$.

Also recall that, for any $1 \leqslant i \leqslant n$, we set the weights to

$$\pi_i := \exp\left(\frac{-\left\|x_i - \xi\right\|^2}{2\nu^2}\right). \tag{7.1}$$

We will need the following scaling constant:

$$C_d := \left(\frac{\nu^2}{\nu^2 + \sigma^2}\right)^{d/2} \cdot \exp\left(\frac{-\left\|\xi - \mu\right\|^2}{2(\nu^2 + \sigma^2)}\right), \tag{7.2}$$

which does not play any role in the final result. One can check that $C_d \to 1$ when $\nu \gg \sigma$, regardless of the dimension.

Finally, for any $1 \leqslant j \leqslant d$, recall that we defined

$$\alpha_j := \left[\frac{1}{2}\mathrm{erf}\left(\frac{x - \tilde{\mu}_j}{\tilde{\sigma}\sqrt{2}}\right)\right]_{q_{j-}}^{q_{j+}}, \tag{7.3}$$

and

$$\theta_j := \left[\frac{\tilde{\sigma}}{\sqrt{2\pi}} \exp\left(\frac{-(x - \tilde{\mu}_j)^2}{2\tilde{\sigma}^2}\right)\right]_{q_{j-}}^{q_{j+}}, \tag{7.4}$$

where $q_{j\pm}$ are the quantile boundaries of ξ_j. These coefficients are discussed in Section 5 of the main paper. Note that all the expected values are taken with respect to the randomness on the $x_1, \dots, x_n$.

8 Covariance matrix

In this section, we state and prove the intermediate results used to control the covariance matrix $\widehat{\Sigma}$. The goal of this section is to obtain the control of $\left\|\widehat{\Sigma}^{-1} - \Sigma^{-1}\right\|_{\mathrm{op}}$ in probability. Intuitively, if this quantity is small enough, then we can inverse Eq. (5.1) and make very precise statements about $\widehat{\beta}$.

We first show that it is possible to compute the expected covariance matrix in closed form. Without this result, a concentration result would still hold, but it would be much harder to gain precise insights on the β_js.

Lemma 8.1 (Expected covariance matrix). *Under Assumption 2, the expected value of $\widehat{\Sigma}$ is given by*

$$\Sigma := C_d \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_d \\ \alpha_1 & \alpha_1 & & \alpha_i\alpha_j \\ \vdots & & \ddots & \\ \alpha_d & \alpha_i\alpha_j & & \alpha_d \end{pmatrix}.$$

Proof. Elementary computations yield

$$\widehat{\Sigma} = \frac{1}{n} \begin{pmatrix} \sum_{i=1}^n \pi_i & \sum_{i=1}^n \pi_i z_{i1} & \cdots & \sum_{i=1}^n \pi_i z_{id} \\ \sum_{i=1}^n \pi_i z_{i1} & \sum_{i=1}^n \pi_i z_{i1} & & \sum_{i=1}^n \pi_i z_{ik} z_{i\ell} \\ \vdots & & \ddots & \\ \sum_{i=1}^n \pi_i z_{id} & \sum_{i=1}^n \pi_i z_{ik} z_{i\ell} & & \sum_{i=1}^n \pi_i z_{id} \end{pmatrix}.$$

Reading the coefficients of this matrix, we have essentially three computations to complete: $\mathbb{E}[\pi_i]$, $\mathbb{E}[\pi_i z_{ik}]$, and $\mathbb{E}[\pi_i z_{ik} z_{i\ell}]$.

Computation of $\mathbb{E}[\pi_i]$. Since the x_is are Gaussian (Assumption 2) and using the definition of the weights (Eq. (7.1)), we can write

$$\mathbb{E}[\pi_i] = \int_{\mathbb{R}^d} \exp\left(\frac{-\|x_i - \xi\|^2}{2\nu^2}\right) \exp\left(\frac{-\|x_i - \mu\|^2}{2\sigma^2}\right) \frac{\mathrm{d}x_{i1} \cdots x_{id}}{(2\pi\sigma^2)^{d/2}}.$$

By independence across coordinates, the last display amounts to

$$\prod_{j=1}^d \int_{-\infty}^{+\infty} \exp\left(\frac{-(x-\xi_j)^2}{2\nu^2} + \frac{-(x-\mu_j)^2}{2\sigma^2}\right) \frac{\mathrm{d}x}{\sigma\sqrt{2\pi}}.$$

We then apply Lemma 11.1 to each of the integrals within the product to obtain

$$\prod_{j=1}^d \frac{\nu}{\sqrt{\nu^2+\sigma^2}} \cdot \exp\left(\frac{-(\xi_j-\mu_j)^2}{2(\nu^2+\sigma^2)}\right) = \frac{\nu^d}{(\nu^2+\sigma^2)^{d/2}} \cdot \exp\left(\frac{-\|\xi-\mu\|^2}{2(\nu^2+\sigma^2)}\right).$$

We recognize the definition of the scaling constant (Eq. (7.2)): we have proved that $\mathbb{E}[\pi_i] = C_d$.

Computation of $\mathbb{E}[\pi_i z_{ik}]$. Since the x_is are Gaussian (Assumption 2) and using the definition of the weights (Eq. (7.1)),

$$\mathbb{E}[\pi_i] = \int_{\mathbb{R}^d} \exp\left(\frac{-\|x_i - \xi\|^2}{2\nu^2}\right) \exp\left(\frac{-\|x_i - \mu\|^2}{2\sigma^2}\right) \mathbf{1}_{\phi(x_i)_k = \phi(\xi)_k} \frac{\mathrm{d}x_{i1} \cdots x_{id}}{(2\pi\sigma^2)^{d/2}}.$$

By independence across coordinates, the last display amounts to

$$\int_{q_{k-}}^{q_{k+}} \exp\left(\frac{-(x-\xi_k)^2}{2\nu^2} + \frac{-(x-\mu_k)^2}{2\sigma^2}\right) \frac{\mathrm{d}x}{\sigma\sqrt{2\pi}} \cdot \prod_{\substack{j=1 \\ j\neq k}}^d \int_{-\infty}^{+\infty} \exp\left(\frac{-(x-\xi_j)^2}{2\nu^2} + \frac{-(x-\mu_j)^2}{2\sigma^2}\right) \frac{\mathrm{d}x}{\sigma\sqrt{2\pi}}.$$

Using Lemma 11.1, we obtain

$$\frac{\nu^d}{(\nu^2+\sigma^2)^{d/2}} \cdot \exp\left(\frac{-\|\xi-\mu\|^2}{2(\nu^2+\sigma^2)}\right) \cdot \left[\frac{1}{2}\mathrm{erf}\left(\frac{\nu^2(x-\mu_k)+\sigma^2(x-\xi_k)}{\nu\sigma\sqrt{2(\nu^2+\sigma^2)}}\right)\right]_{q_{k-}}^{q_{k+}}.$$

We recognize the definition of the scaling constant (Eq. (7.2)) and of the α_k coefficient (Eq. (7.3)): we have proved that $\mathbb{E}[\pi_i z_{ik}] = C_d \alpha_k$.

Computation of $\mathbb{E}[\pi_i z_{ik} z_{i\ell}]$. Since the x_is are Gaussian (Assumption 2) and using the definition of the weights (Eq. (7.1)),

$$\mathbb{E}[\pi_i z_{ik} z_{i\ell}] = \int_{\mathbb{R}^d} \exp\left(\frac{-\|x_i-\xi\|^2}{2\nu^2}\right)\exp\left(\frac{-\|x_i-\mu\|^2}{2\sigma^2}\right)\mathbf{1}_{\phi(x_i)_k=\phi(\xi)_k}\mathbf{1}_{\phi(x_i)_\ell=\phi(\xi)_\ell}\frac{\mathrm{d}x_{i1}\cdots\mathrm{d}x_{id}}{(2\pi\sigma^2)^{d/2}}\,.$$

By independence across coordinates, the last display amounts to

$$\prod_{\substack{j=1\\ j\neq k,\ell}}^{d}\int_{-\infty}^{+\infty}\exp\left(\frac{-(x-\xi_j)^2}{2\nu^2}+\frac{-(x-\mu_j)^2}{2\sigma^2}\right)\frac{\mathrm{d}x}{\sigma\sqrt{2\pi}}\cdot\int_{q_{k-}}^{q_{k+}}\exp\left(\frac{-(x-\xi_k)^2}{2\nu^2}+\frac{-(x-\mu_k)^2}{2\sigma^2}\right)\frac{\mathrm{d}x}{\sigma\sqrt{2\pi}}$$
$$\cdot\int_{q_{\ell-}}^{q_{\ell+}}\exp\left(\frac{-(x-\xi_\ell)^2}{2\nu^2}+\frac{-(x-\mu_\ell)^2}{2\sigma^2}\right)\frac{\mathrm{d}x}{\sigma\sqrt{2\pi}}\,.$$

Using Lemma 11.1, we obtain

$$\frac{\nu^d}{(\nu^2+\sigma^2)^{d/2}}\cdot\exp\left(\frac{-\|\xi-\mu\|^2}{2(\nu^2+\sigma^2)}\right)\cdot\left[\frac{1}{2}\mathrm{erf}\left(\frac{\nu^2(x-\mu_k)+\sigma^2(x-\xi_k)}{\nu\sigma\sqrt{2(\nu^2+\sigma^2)}}\right)\right]_{q_{k-}}^{q_{k+}}$$
$$\cdot\left[\frac{1}{2}\mathrm{erf}\left(\frac{\nu^2(x-\mu_\ell)+\sigma^2(x-\xi_\ell)}{\nu\sigma\sqrt{2(\nu^2+\sigma^2)}}\right)\right]_{q_{\ell-}}^{q_{\ell+}}\,.$$

We recognize the definition of the scaling constant (Eq. (7.2)) and of the alphas (Eq. (7.3)): we have proved that $\mathbb{E}[\pi_i z_{ik} z_{i\ell}] = C_d\alpha_k\alpha_\ell$. □

As it turns out, we show that it is possible to invert Σ in closed-form, therefore simplifying tremendously our quest for control of $\left\|\widehat{\Sigma}^{-1}-\Sigma^{-1}\right\|_{\mathrm{op}}$. Indeed, in most cases, even if concentration could be shown, one would not have a precise idea of the coefficients of Σ^{-1}.

Lemma 8.2 (Inverse of the covariance matrix). *If $\alpha_j \neq 0,1$ for any $j\in\{1,\dots,d\}$, then Σ is invertible, and*

$$\Sigma^{-1} = C_d^{-1}\begin{pmatrix} 1+\sum_{j=1}^d\frac{\alpha_j}{1-\alpha_j} & \frac{-1}{1-\alpha_1} & \cdots & \frac{-1}{1-\alpha_d}\\ \frac{-1}{1-\alpha_1} & \frac{1}{\alpha_1(1-\alpha_1)} & & 0\\ \vdots & & \ddots & \\ \frac{-1}{1-\alpha_d} & 0 & & \frac{1}{\alpha_d(1-\alpha_d)}\end{pmatrix}.$$

Proof. Define $\alpha\in\mathbb{R}^d$ the vector of the α_js. Set $A:=1$, $B:=\alpha^\top$, $C:=\alpha$, and

$$D := \begin{pmatrix}\alpha_1 & & \alpha_j\alpha_k\\ & \ddots & \\ \alpha_j\alpha_k & & \alpha_d\end{pmatrix}.$$

Then Σ is a block matrix that can be written $\Sigma = C_d\begin{bmatrix}A & B\\ C & D\end{bmatrix}$. We notice that

$$D - CA^{-1}B = \mathrm{Diag}\left(\alpha_1(1-\alpha_1),\dots,\alpha_d(1-\alpha_d)\right)\,.$$

Note that, since erf is an increasing function, the α_js are always distinct from 0 and 1. Thus $D-CA^{-1}B$ is an invertible matrix, and we can use the block matrix inversion formula to obtain the claimed result. □

As a direct consequence of the computation of Σ^{-1}, we can control its largest eigenvalue.

Lemma 8.3 (Control of $\left\|\Sigma^{-1}\right\|_{\mathrm{op}}$). *We have the following bound on the operator norm of the inverse covariance matrix:*

$$\left\|\Sigma^{-1}\right\|_{op} \leqslant \frac{3dA_d}{C_d}\,,$$

where $A_d := \max_{1\leqslant j\leqslant d}\frac{1}{\alpha_j(1-\alpha_j)}$.

Proof. We control the operator norm of Σ^{-1} by its Frobenius norm: Namely,

$$\begin{aligned}\left\|\Sigma^{-1}\right\|_{\mathrm{op}}^2 &\leqslant \left\|\Sigma^{-1}\right\|_{\mathrm{F}}^2 \\ &= C_d^{-2}\left[\left(1+\sum\frac{\alpha_j}{1-\alpha_j}\right)^2+\sum\frac{1}{(1-\alpha_j)^2}+\sum\frac{1}{\alpha_j(1-\alpha_j)}\right] \\ \left\|\Sigma^{-1}\right\|_{\mathrm{op}}^2 &\leqslant 6C_d^{-2}d^2\left(\max\frac{1}{\alpha_j(1-\alpha_j)}\right)^2,\end{aligned}$$

where we used $\alpha_j \in (0,1)$ in the last step of the derivation. □

Remark 8.1. Better bounds can without doubt be obtained. A step in this direction is to notice that $S := C_d\Sigma^{-1}$ is an arrowhead matrix (O'Leary and Stewart, 1996). Thus the eigenvalues of S are solutions of the secular equation

$$1+\sum_{j=1}^{d}\frac{\alpha_j}{1-\alpha_j}-\lambda+\sum_{j=1}^{d}\frac{\alpha_j}{(1-\alpha_j)(1-\lambda\alpha_j(1-\alpha_j))}=0\,.$$

Further study of this equation could yield an improved statement for Lemma 8.3.

We now show that the empirical covariance matrix concentrates around Σ. It is interesting to see that the non-linear nature of the new coordinates (the z_{ij}s) calls for complicated computations but allows us to use simple concentration tools since they are, in essence, Bernoulli random variables.

Lemma 8.4 (Concentration of the empirical covariance matrix). *Let $\widehat{\Sigma}$ and Σ be defined as before. Then, for every $t>0$,*

$$\mathbb{P}\left(\left\|\widehat{\Sigma}-\Sigma\right\|_{op}\geqslant t\right)\leqslant 4d^2\exp(-2nt^2)\,.$$

Proof. Recall that $\|\cdot\|_{\mathrm{op}} \leqslant \|\cdot\|_{\mathrm{F}}$: it suffices to show the result for the Frobenius norm. Next, we notice that the summands appearing in the entries of $\widehat{\Sigma}$, $X_i^{(1)} := \pi_i$, $X_i^{(2,k)} := \pi_i z_{ik}$, and $X_i^{(3,k,\ell)} := \pi_i z_{ik} z_{i\ell}$, are all bounded. Indeed, by the definition of the weights and the definition of the new features, they all take values in $[0,1]$. Moreover, for given k,ℓ, they are independent random variables. Thus we can apply Hoeffding's inequality (Theorem 11.1) to $X_i^{(1)}$, $X_i^{(2,k)}$, and $X_i^{(3,k,\ell)}$. For any given $t>0$, we obtain

$$\begin{cases}\mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^n(\pi_i-\mathbb{E}\left[\pi_i\right])\right|\geqslant t\right)\leqslant 2\exp(-2nt^2)\\ \mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^n(\pi_i z_{ik}-\mathbb{E}\left[\pi_i\right])\right|\geqslant t\right)\leqslant 2\exp(-2nt^2)\\ \mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^n(\pi_i z_{ik}z_{i\ell}-\mathbb{E}\left[\pi_i\right])\right|\geqslant t\right)\leqslant 2\exp(-2nt^2)\end{cases}$$

We conclude by a union bound on the $(d+1)^2 \leqslant 2d^2$ entries of the matrix. □

As a consequence of the two preceding lemmas, we can control the largest eigenvalue of Σ^{-1}.

Lemma 8.5 (Control of $\left\|\widehat{\Sigma}^{-1}\right\|_{\mathbf{op}}$). *For every $t\in\left(0,\frac{C_d}{6dA_d}\right]$, with probability greater than $1-4d^2\exp(-2nt^2)$,*

$$\left\|\widehat{\Sigma}^{-1}\right\|_{op}\leqslant\frac{6dA_d}{C_d}\,.$$

Proof. Let $t\in(0,C_d/(6dA_d)]$. According to Lemma 8.3, $\lambda_{\max}(\Sigma^{-1})\leqslant 3dA_d/C_d$. We deduce that

$$\lambda_{\min}(\Sigma)\geqslant\frac{C_d}{3dA_d}\,.$$

Now let us use Lemma 8.4 with this t: there is an event Ω, which has probability greater than $1-4d^2\exp(-2nt^2)$, such that $\left\|\widehat{\Sigma}-\Sigma\right\|_{\mathrm{op}}\leqslant t$. According to Weyl's inequality (Weyl, 1912), on this event,

$$\left|\lambda_{\min}(\widehat{\Sigma})-\lambda_{\min}(\Sigma)\right|\leqslant\left\|\widehat{\Sigma}-\Sigma\right\|_{\mathrm{op}}\leqslant t\,.$$

In particular,

$$\lambda_{\min}(\widehat{\Sigma}) \geqslant \lambda_{\min}(\Sigma) - t \geqslant \frac{C_d}{6dA_d}\,.$$

Finally, we deduce that

$$\left\|\widehat{\Sigma}^{-1}\right\|_{\mathrm{op}} \leqslant \frac{6dA_d}{C_d}\,.$$

□

We can now state and prove the main result of this section, controlling the operator norm of $\widehat{\Sigma} - \Sigma$ with high probability.

Proposition 8.1 (Control of $\left\|\widehat{\Sigma}^{-1} - \Sigma^{-1}\right\|_{\mathbf{op}}$). *For every $t \in \left(0, \frac{3dA_d}{C_d}\right]$, we have*

$$\mathbb{P}\left(\left\|\widehat{\Sigma}^{-1} - \Sigma^{-1}\right\|_{op} \geqslant t\right) \leqslant 8d^2 \exp\left(\frac{-C_d^4 n t^2}{162 d^4 A_d^4}\right)\,.$$

Remark 8.2. Proposition 8.1 is the key tool to invert Eq. (5.1) and gain precise control over $\widehat{\beta}$. In the regime that we consider, the dimension d as well as the number of bins p are *fixed*, and d, C_d, and A_d are essentially numerical constants. We did not optimize these constant with respect to d, since the main message is to consider the behavior for a large number of new examples ($n \to +\infty$).

Proof. We notice that, assuming that $\widehat{\Sigma}$ is invertible, $\widehat{\Sigma}^{-1} - \Sigma^{-1} = \widehat{\Sigma}^{-1}(\Sigma - \widehat{\Sigma})\Sigma^{-1}$. Since $\|\cdot\|_{\mathrm{op}}$ is sub-multiplicative, we just have to control each term individually. Lemma 8.3 gives us

$$\left\|\Sigma^{-1}\right\|_{\mathrm{op}} \leqslant \frac{3dA_d}{C_d}\,.$$

Next, set $t_1 := \frac{C_d^2 t}{18 d^2 A_d^2}$. According to Lemma 8.4, with probability greater than $1 - 4d^2\exp(-2nt_1^2)$,

$$\left\|\widehat{\Sigma} - \Sigma\right\|_{\mathrm{op}} \leqslant t_1\,.$$

Finally, set $t_2 := t_1$. It is easy to check that $t_2 \leqslant C_d/(6dA_d)$. Thus we can use Lemma 8.5: with probability greater than $1 - 4d^2\exp(-2nt_1^2)$,

$$\left\|\widehat{\Sigma}^{-1}\right\|_{\mathrm{op}} \leqslant \frac{6dA_d}{C_d}\,.$$

By the union bound, with probability greater than $1 - 8d^2\exp\left(\frac{-C_d^4 n t^2}{162 d^4 A_d^4}\right)$,

$$\begin{aligned}\left\|\widehat{\Sigma}^{-1} - \widehat{\Sigma}\right\|_{\mathrm{op}} &\leqslant \left\|\Sigma^{-1}\right\|_{\mathrm{op}} \cdot \left\|\widehat{\Sigma} - \Sigma\right\|_{\mathrm{op}} \cdot \left\|\widehat{\Sigma}^{-1}\right\|_{\mathrm{op}} \\ &\leqslant \frac{3dA_d}{C_d} \cdot t_1 \cdot \frac{6dA_d}{C_d} = t\,.\end{aligned}$$

□

9 Right-hand side of Eq. (5.1)

In this section, we state and prove the results in relation to $\widehat{\Gamma}$. We begin with the computation of Γ, the expected value of $\widehat{\Gamma}$.

Lemma 9.1 (Computation of Γ). *Under Assumption 2 and 1, the expected value of $\widehat{\Gamma}$ is given by*

$$\Gamma = C_d \begin{pmatrix} f(\tilde{\mu}) \\ \alpha_1 f(\tilde{\mu}) - a_1\theta_1 \\ \vdots \\ \alpha_d f(\tilde{\mu}) - a_d\theta_d \end{pmatrix},$$

where the θ_js are defined by

$$\theta_j := \left[\frac{\tilde{\sigma}}{\sqrt{2\pi}} \exp\left(\frac{-(x-\tilde{\mu}_j)^2}{2\tilde{\sigma}^2} \right) \right]_{q_{j-}}^{q_{j+}} .$$

Proof. Given the expression of $\widehat{\Gamma}$, we have essentially two computations to manage: $\mathbb{E}\left[\pi_i f(x_i)\right]$ and $\mathbb{E}\left[\pi_i z_{ij} f(x_i)\right]$.

Computation of $\mathbb{E}\left[\pi_i f(x_i)\right]$. Under Assumption 1, by linearity of the integral,

$$\mathbb{E}\left[\pi_i f(x_i)\right] = \mathbb{E}\left[\pi_i (a^\top + b)\right] = b\mathbb{E}\left[\pi_i\right] + \sum_{j=1}^{d} a_j \mathbb{E}\left[\pi_i x_{ij}\right] . \tag{9.1}$$

Now we have already seen in the proof of Lemma 8.1 that $\mathbb{E}\left[\pi_i\right] = C_d$. Thus we can focus on the computation of $\mathbb{E}\left[\pi_i x_{ij}\right]$ for fixed i, j. Under Assumption 2, we have

$$\mathbb{E}\left[\pi_i x_{ij}\right] = \int_{\mathbb{R}^d} x_j \cdot \exp\left(\frac{-\left\|x-\xi\right\|^2}{2\nu^2} + \frac{-\left\|x-\mu\right\|^2}{2\sigma^2} \right) \frac{\mathrm{d}x_1 \cdots \mathrm{d}x_d}{(2\pi\sigma^2)^{d/2}} .$$

By independence, the last display amounts to

$$\int_{-\infty}^{+\infty} x \cdot \exp\left(\frac{-(x-\xi_j)^2}{2\nu^2} + \frac{-(x-\mu_j)^2}{2\sigma^2} \right) \frac{\mathrm{d}x}{\sigma\sqrt{2\pi}} \cdot \prod_{k \neq j} \int_{-\infty}^{+\infty} \exp\left(\frac{-(x-\xi_k)^2}{2\nu^2} + \frac{-(x-\mu_k)^2}{2\sigma^2} \right) \frac{\mathrm{d}x}{\sigma\sqrt{2\pi}} .$$

A straightforward application of Lemmas 11.1 and 11.2 yields

$$\mathbb{E}\left[\pi_i x_{ij}\right] = C_d \cdot \frac{\nu^2\mu_j + \sigma^2\xi_j}{\nu^2 + \sigma^2} .$$

Back to Eq. (9.1), we have shown that

$$\mathbb{E}\left[\pi_i f(x_i)\right] = C_d b + \sum_{j=1}^{d} a_j \cdot C_d \frac{\nu^2\mu_j + \sigma^2\xi_j}{\nu^2 + \sigma^2} = C_d f(\tilde{\mu}) .$$

Computation of $\mathbb{E}\left[\pi_i z_{ij} f(x_i)\right]$. Under Assumption 1, by linearity of the integral,

$$\mathbb{E}\left[\pi_i z_{ij} f(x_i)\right] = b\mathbb{E}\left[\pi_i z_{ij}\right] + \sum_{k=1}^{d} a_k \cdot \mathbb{E}\left[\pi_i z_{ij} x_{ik}\right] . \tag{9.2}$$

We have already computed $\mathbb{E}\left[\pi_i z_{ij}\right]$ in the proof of Lemma 8.1 and found that

$$\mathbb{E}\left[\pi_i z_{ij}\right] = C_d \alpha_j .$$

Regarding the computation of $\mathbb{E}\left[\pi_i z_{ij} x_{ik}\right]$, there are essentially two cases to consider depending whether $k = \ell$ or not. Let us first consider the case $k = j$. Then we obtain

$$\mathbb{E}\left[\pi_i z_{ij} x_{ik}\right] = \int_{\mathbb{R}^d} x_j \exp\left(\frac{-\left\|x-\xi\right\|^2}{2\nu^2} + \frac{-\left\|x-\mu\right\|^2}{2\sigma^2} \right) \mathbf{1}_{\phi(x)_j = \phi(\xi)_j} \frac{\mathrm{d}x_1 \cdots \mathrm{d}x_d}{(2\pi\sigma^2)^{d/2}} .$$

By independence, the last display amounts to

$$\int_{q_{j-}}^{q_{j+}} x \cdot \exp\left(\frac{-(x-\xi_j)^2}{2\nu^2} + \frac{-(x-\mu_j)^2}{2\sigma^2} \right) \frac{\mathrm{d}x}{\sigma\sqrt{2\pi}} \cdot \prod_{k \neq j} \int_{-\infty}^{+\infty} \exp\left(\frac{-(x-\xi_k)^2}{2\nu^2} + \frac{-(x-\mu_k)^2}{2\sigma^2} \right) \frac{\mathrm{d}x}{\sigma\sqrt{2\pi}} .$$

According to Lemma 11.2 and the definition of α_j and θ_j (Eqs. (7.3) and (7.3)), we have

$$\mathbb{E}\left[\pi_i z_{ij} x_{ij}\right] = C_d \frac{\sigma^2\xi_j + \nu^2\mu_j}{\nu^2 + \sigma^2} \alpha_j - C_d \theta_j .$$

Now if $k \neq j$, by independence, $\mathbb{E}\left[\pi_i z_{ij} x_{ik}\right]$ splits in three parts:

$$\mathbb{E}\left[\pi_i z_{ij} x_{ik}\right] = \int_{-\infty}^{+\infty} x \cdot \exp\left(\frac{-(x-\xi_k)^2}{2\nu^2} + \frac{-(x-\mu_k)^2}{2\sigma^2}\right) \frac{\mathrm{d}x}{\sigma\sqrt{2\pi}} \cdot \int_{q_{j-}}^{q_{j+}} \exp\left(\frac{-(x-\xi_j)^2}{2\nu^2} + \frac{-(x-\mu_j)^2}{2\sigma^2}\right) \frac{\mathrm{d}x}{\sigma\sqrt{2\pi}} \cdot \\ \cdot \prod_{\ell \neq j,k} \int_{-\infty}^{+\infty} \exp\left(\frac{-(x-\xi_k)^2}{2\nu^2} + \frac{-(x-\mu_k)^2}{2\sigma^2}\right) \frac{\mathrm{d}x}{\sigma\sqrt{2\pi}} .$$

Lemma 11.1 and 11.2 yield

$$\mathbb{E}\left[\pi_i z_{ij} x_{ik}\right] = C_d \cdot \frac{\sigma^2 \xi_k + \nu^2 \mu_k}{\nu^2 + \sigma^2} \cdot \alpha_j .$$

In definitive, plugging these results into Eq. (9.2) gives

$$\begin{aligned}\mathbb{E}\left[\pi_i z_{ij} f(x_i)\right] &= C_d \alpha_j b + a_j \left(C_d \frac{\sigma^2 \xi_j + \nu^2 \mu_j}{\nu^2 + \sigma^2} \alpha_j - C_d \theta_j\right) + \sum_{k \neq j} a_k \cdot C_d \frac{\sigma^2 \xi_k + \nu^2 \mu_k}{\nu^2 + \sigma^2} \alpha_j \\ &= C_d \alpha_j f(\tilde{\mu}) - C_d a_j \theta_j .\end{aligned}$$

□

As a consequence of Lemma 9.1, we can control $\|\Gamma\|$.

Lemma 9.2 (Control of $\|\Gamma\|$). *Under Assumptions 2 and 1, it holds that*

$$\|\Gamma\|^2 \leqslant C_d^2 \left(3df(\tilde{\mu})^2 + d\tilde{\sigma}^2 \|\nabla f\|^2\right) .$$

Proof. According to Lemma 9.1, we have

$$\|\Gamma\|^2 = C_d^2 \left(f(\tilde{\mu})^2 + \sum_{j=1}^{d} (\alpha_j f(\tilde{\mu}) - a_j \theta_j)^2\right) .$$

Successively using $(x-y)^2 \leqslant 2(x^2+y^2)$, $\alpha_j \in [0,1]$ and $\theta_j \in [-\tilde{\sigma}/\sqrt{2\pi}, \tilde{\sigma}/\sqrt{2\pi}]$, we write

$$\begin{aligned}\|\Gamma\|^2 &\leqslant C_d^2 \left(f(\tilde{\mu})^2 + \sum_{j=1}^{d} 2(\alpha_j^2 f(\tilde{\mu})^2 + a_j^2 \theta_j^2)\right) \\ &\leqslant C_d^2 \left(3df(\tilde{\mu})^2 + d\tilde{\sigma}^2 \|a\|^2\right) ,\end{aligned}$$

which concludes the proof. □

Finally, we conclude this section with a concentration result for $\widehat{\Gamma}$.

Lemma 9.3 (Concentration of $\left\|\widehat{\Gamma}\right\|$). *Under Assumptions 2 and 1, for any $t > 0$, we have*

$$\mathbb{P}\left(\left\|\widehat{\Gamma} - \Gamma\right\| > t\right) \leqslant 4d \exp\left(\frac{-nt^2}{2\|\nabla f\|^2 \sigma^2}\right) .$$

Proof. Since the x_i are Gaussian with variance σ^2 (Assumption 2), the random variable $a^\top x_i + b$ is Gaussian with variance $\|a\|^2 \sigma^2$, and the $X_i^{(1)} := \pi_i x_i$ are sub-Gaussian with parameter $\|a\|^2 \sigma^2$. They are also independent, thus we can apply Theorem 11.2 to the $X_i^{(1)}$:

$$\mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^{n} \pi_i f(x_i) - \mathbb{E}\left[\pi_i f(x_i)\right]\right| > t\right) \leqslant 2\exp\left(\frac{-nt^2}{2\|a\|^2 \sigma^2}\right) .$$

Furthermore, the z_{ij} are $\{0,1\}$-valued. Thus the random variables $X_i^{(j)} := \pi_i z_{ij} f(x_i)$ are also sub-Gaussian with parameter $\|a\|^2 \sigma^2$. We use Hoeffding's inequality (Theorem 11.2) again, to obtain, for any j,

$$\mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^{n} \pi_i z_{ij} f(x_i) - \mathbb{E}\left[\pi_i z_{ij} f(x_i)\right]\right| > t\right) \leqslant 2\exp\left(\frac{-nt^2}{2\|a\|^2 \sigma^2}\right).$$

By the union bound,

$$\mathbb{P}\left(\left\|\widehat{\Gamma} - \Gamma\right\| > t\right) \leqslant 2(d+1)\exp\left(\frac{-nt^2}{2\|a\|^2 \sigma^2}\right).$$

We deduce the result since $d \geqslant 1$. □

10 Proof of the main result

In this section, we state and prove our main result, Theorem 10.1. It is a more precise version than Theorem 3.1 in the main paper.

Theorem 10.1 (Concentration of $\widehat{\beta}$). *Let $\eta \in (0,1)$ and $\varepsilon > 0$. Take*

$$n \geqslant \max\left(\frac{288\|\nabla f\|^2 \sigma^2 d^2 A_d^2}{\varepsilon^2 C_d^2}\log\frac{12d}{\eta}, \frac{18 d^2 A_d^2}{C_d^2}\log\frac{24d^2}{\eta}, \frac{648 d^5 A_d^4 (3f(\tilde{\mu})^2 + \tilde{\sigma}^2\|\nabla f\|^2)}{C_d^2 \varepsilon^2}\log\frac{24d^2}{\eta}\right).$$

Then, under assumptions 2 and 1,

$$\left\|\widehat{\beta} - \Sigma^{-1}\Gamma\right\| \leqslant \varepsilon,$$

with probability greater than $1-\eta$.

Proof. The main idea of the proof is to notice that

$$\begin{aligned}\left\|\widehat{\beta} - \Sigma^{-1}\Gamma\right\| &= \left\|\widehat{\Sigma}^{-1}\widehat{\Gamma} - \Sigma^{-1}\Gamma\right\| \\ &\leqslant \left\|\widehat{\Sigma}^{-1}(\widehat{\Gamma} - \Gamma)\right\| + \left\|(\widehat{\Sigma}^{-1} - \Sigma^{-1})\Gamma\right\|,\end{aligned}$$

and then to control these two terms using the results of Section 8 and 9.

Control of $\left\|\widehat{\Sigma}^{-1}(\widehat{\Gamma} - \Gamma)\right\|$. We use the upper bound $\left\|\widehat{\Sigma}^{-1}(\widehat{\Gamma} - \Gamma)\right\| \leqslant \left\|\widehat{\Sigma}^{-1}\right\|_{\text{op}} \cdot \left\|\widehat{\Gamma} - \Gamma\right\|$. We then achieve control of the operator norm of the empirical covariance matrix in probability with Lemma 8.5, and control of the norm of $\widehat{\Gamma} - \Gamma$ in probability with Lemma 9.3. Set

$$t_1 := \frac{C_d}{6dA_d} \quad \text{and} \quad n_1 := \frac{18d^2}{C_d^2}\log\frac{12d^2}{\eta}.$$

According to Lemma 8.5, for any $n \geqslant n_1$, there is an event Ω_1^n which has probability greater than $1 - 4d^2\exp(-2nt_1^2)$ such that

$$\left\|\widehat{\Sigma}^{-1}\right\|_{\text{op}} \leqslant \frac{6dA_d}{C_d}$$

on this event. It is easy to check that $4d^2\exp(-2n_1 t_1^2) = \eta/3$, thus Ω_1^n has probability greater than $1 - \eta/3$. Now set

$$t_2 := \frac{\varepsilon C_d}{12dA_d} \quad \text{and} \quad n_2 := \frac{288\|a\|^2\sigma^2 d^2 A_d^2}{\varepsilon^2 C_d^2}\log\frac{12d}{\eta}.$$

According to Lemma 9.3, for any $n \geqslant n_2$, there exists an event Ω_2^n which has probability greater than $1 - 4d\exp\left(\frac{-nt_2^2}{2\|a\|^2\sigma^2}\right)$ such that $\left\|\widehat{\Gamma} - \Gamma\right\| \leqslant t_2$ on that event. One can check that

$$4d\exp\left(\frac{-n_2 t_2^2}{2\|a\|^2\sigma^2}\right) = \frac{\eta}{3},$$

thus Ω_2^n has probability greater than $1-\eta/3$. On the event $\Omega_1^n \cap \Omega_2^n$, we have

$$\left\|\widehat{\Sigma}^{-1}(\widehat{\Gamma}-\Gamma)\right\| \leqslant \left\|\widehat{\Sigma}^{-1}\right\|_{\mathrm{op}} \cdot \left\|\widehat{\Gamma}-\Gamma\right\| \leqslant \frac{6dA_d}{C_d} \cdot t_2 \leqslant \frac{\varepsilon}{2},$$

by definition of t_2.

Control of $\left\|(\widehat{\Sigma}^{-1}-\Sigma^{-1})\Gamma\right\|$. We use the upper bound $\left\|(\widehat{\Sigma}^{-1}-\Sigma^{-1})\Gamma\right\| \leqslant \left\|\widehat{\Sigma}^{-1}-\Sigma^{-1}\right\|_{\mathrm{op}} \cdot \|\Gamma\|$. We then achieve control of $\left\|\widehat{\Sigma}^{-1}-\Sigma^{-1}\right\|_{\mathrm{op}}$ in probability with Proposition 8.1, whereas we can bound the norm of Γ almost surely with Lemma 9.2. If $\|\Gamma\|=0$, then there is nothing to prove. Otherwise, set

$$t_3 := \min\left(\frac{\varepsilon}{2\|\Gamma\|}, \frac{3dA_d}{C_d}\right), \; n_3 := \frac{18d^2A_d^2}{C_d^2}\log\frac{24d^2}{\eta}, \quad \text{and} \quad n_4 := \frac{648d^5A_d^4(3f(\tilde{\mu})^2+\tilde{\sigma}^2\|a\|^2)}{C_d^2\varepsilon^2}\log\frac{24d^2}{\eta}.$$

According to Proposition 8.1, for any $n \geqslant \max(n_3, n_4)$, there is an event Ω_3^n which has probability greater than $1-8d^2\exp\left(\frac{-C_d^3nt_3^2}{162d^2A_d^4}\right)$ such that

$$\left\|\widehat{\Sigma}^{-1}-\Sigma^{-1}\right\|_{\mathrm{op}} \leqslant t_3$$

on this event. With the help of Lemma 9.2, one can check that

$$\max\left(8d^2\exp\left(\frac{-C_d^3n_3t_3^2}{162d^2A_d^4}\right), 8d^2\exp\left(\frac{-C_d^3n_4t_3^2}{162d^2A_d^4}\right)\right) \leqslant \frac{\eta}{3}.$$

Therefore, Ω_3^n has probability greater than $\eta/3$ and, on this event,

$$\left\|(\widehat{\Sigma}^{-1}-\Sigma^{-1})\Gamma\right\| \leqslant \left\|\widehat{\Sigma}^{-1}-\Sigma^{-1}\right\|_{\mathrm{op}} \cdot \|\Gamma\| \leqslant t_3 \cdot \|\Gamma\| \leqslant \frac{\varepsilon}{2}.$$

Conclusion. Set $n \geqslant \max(n_i, i=1\dots4)$. Define $\Omega^n := \Omega_1^n \cap \Omega_2^n \cap \Omega_3^n$, where the Ω_i^n are defined as before. According to the previous reasoning, on the event Ω^n,

$$\begin{aligned}\left\|\widehat{\beta}-\Sigma^{-1}\Gamma\right\| &= \left\|\widehat{\Sigma}^{-1}\widehat{\Gamma}-\Sigma^{-1}\Gamma\right\| \\ &\leqslant \left\|\widehat{\Sigma}^{-1}(\widehat{\Gamma}-\Gamma)\right\| + \left\|(\widehat{\Sigma}^{-1}-\Sigma^{-1})\Gamma\right\| \\ &\leqslant \frac{\varepsilon}{2}+\frac{\varepsilon}{2} = \varepsilon.\end{aligned}$$

Moreover, the union bound gives $\mathbb{P}(\Omega^n) \geqslant 1-\eta$. We conclude by noticing that n_1 is always smaller than n_3, thus we just have to require $n \geqslant \max(n_2, n_3, n_4)$, as in the statement of our result. □

11 Technical lemmas

11.1 Gaussian integrals

In this section, we collect some Gaussian integral computations that are needed in our derivations. We provide succinct proof, since essentially any modern computer algebra system will provide these formulas. Our first result is for zero-th order Gaussian integral.

Lemma 11.1 (Gaussian integral, 0-th order). *Let ξ, μ be real numbers, and ν, σ be positive real numbers. Then, it holds that*

$$\int \exp\left(\frac{-(x-\xi)^2}{2\nu^2}+\frac{-(x-\mu)^2}{2\sigma^2}\right)\frac{\mathrm{d}x}{\sigma\sqrt{2\pi}} = \frac{\nu}{\sqrt{\nu^2+\sigma^2}}\cdot\exp\left(\frac{-(\xi-\mu)^2}{2(\nu^2+\sigma^2)}\right)\cdot\frac{1}{2}\mathrm{erf}\left(\frac{\nu^2(x-\mu)+\sigma^2(x-\xi)}{\nu\sigma\sqrt{2(\nu^2+\sigma^2)}}\right).$$

In particular,

$$\int_{-\infty}^{+\infty} \exp\left(\frac{-(x-\xi)^2}{2\nu^2}+\frac{-(x-\mu)^2}{2\sigma^2}\right)\frac{\mathrm{d}x}{\sigma\sqrt{2\pi}} = \frac{\nu}{\sqrt{\nu^2+\sigma^2}}\cdot\exp\left(\frac{-(\xi-\mu)^2}{2(\nu^2+\sigma^2)}\right).$$

Proof. For any reals a, b, and c, it holds that

$$\int \mathrm{e}^{-ax^2+bx+c}\,\mathrm{d}x = \sqrt{\frac{\pi}{a}} \cdot \mathrm{e}^{\frac{b^2}{4a}+c} \cdot \frac{1}{2}\mathrm{erf}\left(\frac{2ax-b}{2\sqrt{a}}\right).$$

We apply this formula with $a = \frac{1}{2\nu^2} + \frac{1}{2\sigma^2}$, $b = \frac{\xi}{\nu^2} + \frac{\mu}{\sigma^2}$, and $c = -\left(\frac{\xi^2}{2\nu^2} + \frac{\mu^2}{\sigma^2}\right)$. We then notice that $b^2/(4a) + c = \frac{-(\xi-\mu)^2}{2(\nu^2+\sigma^2)}$ and

$$\frac{2ax-b}{2\sqrt{a}} = \frac{\nu^2(x-\mu)+\sigma^2(x-\xi)}{\nu\sigma\sqrt{2(\nu^2+\sigma^2)}}.$$

□

Remark 11.1. We often replace $\frac{\nu^2(x-\mu)+\sigma^2(x-\xi)}{\nu\sigma\sqrt{2(\nu^2+\sigma^2)}}$ by the more readable $(x-\tilde{\mu})/(\tilde{\sigma}\sqrt{2})$ in the main text of the paper.

Since f is assumed to be linear in most of the paper, we need first order computations as well:

Lemma 11.2 (Gaussian integral, 1st order). *Let ξ, μ be real numbers, and ν, σ be positive numbers. Then it holds that*

$$\int x \cdot \exp\left(\frac{-(x-\xi)^2}{2\nu^2} + \frac{-(x-\mu)^2}{2\sigma^2}\right)\frac{\mathrm{d}x}{\sigma\sqrt{2\pi}} = \frac{\nu}{\sqrt{\nu^2+\sigma^2}} \cdot \exp\left(\frac{-(\xi-\mu)^2}{2(\nu^2+\sigma^2)}\right) \cdot \left[\frac{\sigma^2\xi+\nu^2\mu}{\nu^2+\sigma^2} \cdot \frac{1}{2}\mathrm{erf}\left(\frac{\nu^2(x-\mu)+\sigma^2(x-\xi)}{\nu\sigma\sqrt{2(\nu^2+\sigma^2)}}\right) - \frac{\nu\sigma}{\sqrt{2\pi}\sqrt{\nu^2+\sigma^2}} \cdot \exp\left(-\left(\frac{\nu^2(x-\mu)+\sigma^2(x-\xi)}{\nu\sigma\sqrt{2(\nu^2+\sigma^2)}}\right)^2\right)\right].$$

In particular,

$$\int_{-\infty}^{+\infty} x \cdot \exp\left(\frac{-(x-\xi)^2}{2\nu^2} + \frac{-(x-\mu)^2}{2\sigma^2}\right)\frac{\mathrm{d}x}{\sigma\sqrt{2\pi}} = \frac{\sigma^2\xi+\nu^2\mu}{\nu^2+\sigma^2} \cdot \frac{\nu}{\sqrt{\nu^2+\sigma^2}} \cdot \exp\left(\frac{-(\xi-\mu)^2}{2(\nu^2+\sigma^2)}\right).$$

Proof. For any a, b, c with $a > 0$, it holds that

$$\int x \cdot \mathrm{e}^{-ax^2+bx+c}\,\mathrm{d}x = \frac{\sqrt{\pi}b}{4a^{3/2}}\mathrm{e}^{b^2/(4a)+c}\mathrm{erf}\left(\frac{2ax-b}{2\sqrt{a}}\right) - \frac{1}{2a}\mathrm{e}^{-ax^2+bx+c}.$$

□

Finally we want to mention the following result.

Lemma 11.3 (Gaussian integral, 2nd order). *Let ξ, μ be real numbers, and ν, σ be positive real numbers. Then, it holds that*

$$\int_{-\infty}^{+\infty} x^2 \cdot \exp\left(\frac{-(x-\xi)^2}{2\nu^2} + \frac{-(x-\mu)^2}{2\sigma^2}\right)\frac{\mathrm{d}x}{\sigma\sqrt{2\pi}} = \frac{(\sigma^2\xi+\nu^2\mu)^2+\nu^2\sigma^2(\nu^2+\sigma^2)}{(\nu^2+\sigma^2)^2} \cdot \frac{\nu}{\sqrt{\nu^2+\sigma^2}} \cdot \exp\left(\frac{-(\xi-\mu)^2}{2(\nu^2+\sigma^2)}\right).$$

Remark 11.2. As a consequence of Lemma 11.3, it would be possible to further our analysis by adding second degree terms to f. Indeed, quantities depending on $\|x_i - \xi\|$, which would have to be computed to extend the proofs of Lemmas 9.1 and 9.3, can be computed with this lemma. For instance, one can show that

$$\mathbb{E}\left[\pi_i \|x_i-\xi\|^2\right] = C_d \cdot \left[\frac{\nu^4}{(\nu^2+\sigma^2)^2}\|\xi-\mu\|^2 + \frac{\nu^2\sigma^2 d}{\nu^2+\sigma^2}\right].$$

Proof. We use the fact that

$$\int x^2 \cdot \mathrm{e}^{-ax^2+bx+c}\,\mathrm{d}x = \frac{\sqrt{\pi}(2a+b^2)}{8a^{5/2}}\mathrm{e}^{\frac{b^2}{4a}+c} \cdot \mathrm{erf}\left(\frac{2ax-b}{2\sqrt{a}}\right) - \frac{ax+b}{4a^2} \cdot \mathrm{e}^{-ax^2+bx+c}.$$

□

11.2 Concentration results

In this section we collect some concentration results used throughout our proofs. Note that we use rather use the two-sided version of these results.

Theorem 11.1 (Hoeffding's inequality). *Let $X_1, \dots, X_n$ be independent random variables such that X_i takes its values in $[a_i, b_i]$ almost surely for all $i \leqslant n$. Then for every $t > 0$,*

$$\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^{n}(X_i - \mathbb{E}[X_i]) \geqslant t\right) \leqslant \exp\left(\frac{-2t^2n^2}{\sum_{i=1}^{n}(b_i - a_i)^2}\right).$$

Proof. This is Theorem 2.8 in Boucheron et al. (2013) in our notation. □

Theorem 11.2 (Hoeffding's inequality for sub-Gaussian random variables). *Let $X_1, \dots, X_n$ be independent random variables such that X_i is sub-Gaussian with parameter $s^2 > 0$. Then, for every $t > 0$,*

$$\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^{n}X_i - \mathbb{E}[X_i] > t\right) \leqslant \exp\left(\frac{-nt^2}{2s^2}\right).$$

Proof. This is Proposition 2.1 in Wainwright (2019). □