An Information-Theoretic Approach to Personalized Explainable Machine Learning

Alexander Jung and Pedro H. J. Nardelli

Abstract—Automated decision making is used routinely throughout our every-day life. Recommender systems decide which jobs, movies, or other user profiles might be interesting to us. Spell checkers help us to make good use of language. Fraud detection systems decide if a credit card transactions should be verified more closely. Many of these decision making systems use machine learning methods that fit complex models to massive datasets. The successful deployment of machine learning (ML) methods to many (critical) application domains crucially depends on its explainability. Indeed, humans have a strong desire to get explanations that resolve the uncertainty about experienced phenomena like the predictions and decisions obtained from ML methods. Explainable ML is challenging since explanations must be tailored (personalized) to individual users with varying backgrounds. Some users might have received university-level education in ML, while other users might have no formal training in linear algebra. Linear regression with few features might be perfectly interpretable for the first group but might be considered a black-box by the latter. We propose a simple probabilistic model for the predictions and user knowledge. This model allows to study explainable ML using information theory. Explaining is here considered as the task of reducing the “surprise” incurred by a prediction. We quantify the effect of an explanation by the conditional mutual information between the explanation and prediction, given the user background.

I. INTRODUCTION

Machine learning (ML) methods compute predictions for quantities of interest based on a statistical analysis of large amounts of historical data [2], [10], [14]. These methods are routinely used to power many services within our everyday-life. ML methods power recommendation systems that decide what job ads or which other user profiles could be interesting to us [17], [26]. Recent breakthroughs in ML, such as in image or text processing [8], also holds the promise of boosting the level of automation in domains which currently rely mainly on human labour or manual design [7].

A key challenge for the successful and ethically sound deployment of ML methods to critical application domains is the (lack of) explainability of its predictions [9], [12], [19], [25]. Explanations of predictions, which are used for decisions that affect humans, are increasingly becoming a legal obligation [25]. Beside legal aspects, it also seems that humans have a basic need for understanding decision making processes [15], [16].

One reason why explainable ML is challenging is that (good) explanations must be tailored to the knowledge of individual users (”explainee”). In general, for a particular prediction, there is no unique explanation that serves equally well a large group of heterogeneous users. Thus, achieving explainable ML would be easier for applications involving a homogenous group of users, like graduate students in a university program.

Large-scale applications as, for instance, recommendation systems for video streaming providers typically involve users with very different backgrounds, which can range from graduate studies in ML-related fields to users with no formal training in linear algebra. While linear models involving few hand-crafted features might be viewed as interpretable for the former group it might be considered a “black-box” for the latter group of users.

This contribution studies explainable ML within information theory by using a probabilistic model for the data and user background. Loosely speaking, we model the effect of providing an explanation for a prediction as a reduction of the “surprise” incurred by a prediction to the user. This qualitative interpretation of explaining a prediction leads naturally to measuring the quantitative effect of explanations via (conditional) mutual information (MI) between the explanation and the prediction, given the user background (see Section II).

Our approach is different from existing work on explainable ML in the sense that we explicitly model the specific knowledge of each individual user. In contrast, most existing methods for explainable ML do not make any assumption about the end-user and her background knowledge.

Explainable ML methods can be roughly divided into two groups. The first group of methods uses models that are considered as intrinsically interpretable, like linear regression or small decision trees. The second group of methods, referred to as model-agnostic methods, probe an ML method by perturbing the features of the data point.

The most straightforward approach to explainable ML methods is to use models that are considered to be intrinsically interpretable. Such methods include linear models, decision trees and artificial neural networks [1], [9], [21]. Explaining the predictions obtained from such intrinsically interpretable models merely amounts to specifying the model parameters, such as the weights \(w_i\) of a linear predictor \(h(x) = \sum_i w_i x_i\), or the feature-wise thresholds used in decision trees [10].

Interpretable models offer an intuitive decomposition of its predictions into a combination of elementary properties of a data point. Defining elementary properties of a data point via the activations of a (deep) neural network renders those models also interpretable (see [21]).

Interpretable models for sequential decision making have been studied in [18], where the authors obtain an explainable multi-
armed bandit model by using the choice for the action space as the explanation. An explanation can be obtained by notifying the user that only previously purchased items are recommended. In contrast to \cite{18}, our approach uses a probabilistic model for the user background to compute personalized explanations that are optimal in a precise (information-theoretic) sense.

A second group of explainable ML, referred to as model agnostic methods, is based on constructing explanations by probing a predictor as a black box \cite{9, 24}. These methods aim at locally approximating black box models by simpler and interpretable models, such as linear models or shallow decision trees \cite{24}.

Our approach is also model agnostic as it only requires the statistical distributions of the model prediction. However, in contrast to most model agnostic explainable ML, we do not use local approximations to explain a black box method. Instead, we use a probabilistic model for the predictions and user knowledge.

We frame explainable ML within a probabilistic model for ML predictions and user knowledge. This allows to capture the act of explaining a prediction using information-theoretic concepts. The act of explaining provides the user additional information about the prediction delivered by some (arbitrary) ML method.

Information theory has already been used for learning optimal explanations \cite{3}. In a similar spirit, we also use MI to guide the learning of instance-wise explanations. However, in contrast to \cite{3}, we also model the effect of the user background on the information provided by an explanation. In a nutshell, while \cite{3} uses unconditional MI between explanations and predictions, we use the conditional MI given the user knowledge (see Section III).

Outline and Contribution. In Section II we propose a simple probabilistic model for the features, prediction and user summary of a data point. This probabilistic model allows to quantify the effect of explanations via the conditional between the explanation and the model prediction, given the user background.

Our main contribution is the formulation of an information-theoretic concept of optimal personalized explanations. As discussed in Section III, we construct (information-theoretically) optimal personalized explanations by maximizing the conditional MI between explanation and predictions, when conditioning on the user summary of a data point. To the best of our knowledge, we present the first information-theoretic approach to personalized explainable ML.

A simple algorithm for computing optimal explanation given the model predictions and user summaries based on i.i.d. samples is presented in Section IV. The proposed algorithm allows to construct personalized explanations that are optimal in an information-theoretic sense.

II. Problem Setup

We consider a supervised ML problem involving data points with features $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ and label $y \in \mathbb{R}$. Given some labelled training data

$$ (x^{(1)}, y^{(1)}), (x^{(2)}, y^{(2)}), \ldots, (x^{(m)}, y^{(m)}) $$

ML methods typically learn a predictor (map)

$$ h(\cdot) : \mathbb{R}^n \rightarrow \mathbb{R} : x \mapsto \hat{y} = h(x) $$

by requiring $\hat{y}^{(i)} \approx y^{(i)}$ \cite{2, 10, 14}.

After learning a predictor $\hat{y} = h(x)$, it is applied to new data points yielding the prediction $\hat{y} = h(x)$. In may application, the prediction $\hat{y}$ is then delivered to a human user. The user can be the subscriber of a streaming service \cite{6}, a dermatologist \cite{5} or a city planner \cite{27}.

Each user has typically some conception or model for the relation between features $x$ and label $y$ of a data point. Based on the user background, she has some understanding of a data point with features $x$.

Our approach to explainable ML is based on modelling the user understanding of a data point by some summary $u \in \mathbb{R}$. The summary is obtained by a (stochastic) map from the features $x$ of a data point. We will focus on summaries being obtained by a deterministic map

$$ u(\cdot) : \mathbb{R}^n \rightarrow \mathbb{R} : x \mapsto u := u(x). $$

However, our approach also covers stochastic maps characterized by a conditional probability distribution $p(u|x)$.

The (user-specific) quantity $u$ represents the understanding of the specific properties of the data point given the user knowledge (modelling assumptions). We interpret $u$ as a “summary” of the data point based on its features $x$ and the intrinsic modelling assumptions of the user.

Let us illustrate the concept of the user summary $u$ as a means to represent user knowledge (or background) by two particular choices for $u$. First, the user summary could be the prediction obtained from a simplified model, such as linear regression using few features that the user anticipates as being relevant. Another example for a user summary $u$ could be a higher-level feature, such as eye spacing in facial pictures \cite{13}.

We formalize the act of explaining a prediction $\hat{y} = h(x)$ as presenting some additional quantity $e$ to the user. This “explanation” $e$ can be any quantity that helps the user to understand the prediction $\hat{y}$, given her understanding $u$ of the data point. Loosely speaking, the explanation $e$ contributes to resolving the uncertainty of the user $u$ about the prediction $\hat{y}$ \cite{15}.

For the sake of exposition, our focus will be on explanations...
obtained via a deterministic map
\[ e(\cdot) : \mathbb{R}^n \to \mathbb{R} : x \mapsto e := e(x), \] (4)
from the features \( x \) of a data point. However, our approach
can be generalized without difficulty to handle explanations
obtained by a (stochastic) map. In the end, we only require the
specification of the conditional probability distribution \( p(e|x) \).

Explanations can be constructed in quite different ways. An
explanation could be a subset of features of a data point (see
[23] and Section III). More generally, explanations could be
obtained from simple local statistics (averages) of features that
are considered related, such as near-by pixels in an image or
consecutive samples of an audio signal. Instead of individual
features, carefully chosen data points can also serve as an
explanation ([18], [24]).

To obtain comprehensible explanations that can be computed
efficiently, we must typically restrict the space of possible
explanations to a small subset \( \mathcal{F} \) of maps ([10]). This is
conceptually similar to the restriction of the space of possible
deterministic maps in a ML method to a small subset of maps
which is known as the hypothesis space.

We consider data points as independent and identically
distributed (i.i.d.) realizations of a random variable with fixed
underlying probability distribution \( p(x,y) \). Modelling the data
point as random implies that the user summary \( u \), prediction
\( \hat{y} \) and explanation \( e \) are also random variables.
The joint distribution \( p(u,\hat{y},e,x,y) \) conforms with the Bayesian network
([22]) (depicted in Figure 2) since
\[ p(u,\hat{y},e,x,y) = p(u|x) \cdot p(e|x) \cdot p(\hat{y}|x) \cdot p(x,y). \] (5)

We measure the amount of additional information provided
by an explanation \( e \) for a prediction \( \hat{y} \) to some user \( u \) via the
conditional MI [4, Ch. 2 and 8]
\[ I(e;\hat{y}|u) := \mathbb{E} \left\{ \log \frac{p(\hat{y},e|u)}{p(\hat{y}|u)p(e|u)} \right\}. \] (6)
The conditional MI \( I(e;\hat{y}|u) \) can also be interpreted as a
measure for the amount by which the explanation \( e \) reduces the
uncertainty about the prediction \( \hat{y} \) which is delivered to
some user \( u \). Thus, constructing explanations via solving ([6]
conforms with the apparent human need to understand observed
phenomena, such as the predictions from a ML method ([15]).

III. OPTIMAL EXPLANATIONS
Capturing the effect of an explanation using the probabilistic
model ([6] offers a principled approach to computing an
optimal explanation \( e \). We require the optimal explanation
\( e^* \) to maximize the conditional MI ([6] between the explanation
\( e \) and the prediction \( \hat{y} \) conditioned on the user summary \( u \) of
the data point.

Formally, an optimal explanation \( e^* \) solves
\[ I(e^*;\hat{y}|u) = \sup_{e \in \mathcal{F}} I(e;\hat{y}|u). \] (7)
The choice for the subset \( \mathcal{F} \) of valid explanations offers a
trade-off between comprehensibility, informativeness and
computational cost incurred by an explanation \( e^* \) (solving ([7]).

The maximization problem ([7] for obtaining optimal
explanations is similar to the approach in ([3]). However,
while ([3] uses the unconditional MI between explanation and
prediction, ([7] involves the conditional MI given the user
summary \( u \).

Let us illustrate the concept of optimal explanations ([7] using a linear regression method. We model the features \( x \) as
a realization of a multivariate normal random vector with zero
mean and covariance matrix \( C_x \).
\[ x \sim \mathcal{N}(0,C_x). \] (8)
The predictor and the user summary are linear functions of
the features,
\[ \hat{y} := w^T x, \quad u := v^T x. \] (9)
We construct explanations via subsets of individual features
\( x_i \) that are considered most relevant for a user to understand
the prediction \( \hat{y} \) (see ([21], Definition 2) and ([20])). Thus, we
consider explanations of the form
\[ e := \{x_i\}_{i \in E} \text{ with some subset } E \subseteq \{1, \ldots, n\}. \] (10)
The complexity of an explanation \( e \) is measured by the
number \( |E| \) of features that contribute to it. We limit the number
of features contributing to an explanation by a fixed (small)
sparsity level,
\[ |E| \leq s(\ll n). \] (11)

Modelling the feature vector \( x \) as Gaussian ([8] implies that
the prediction \( \hat{y} \) and user summary \( u \) obtained from ([9] is jointly
Gaussian for a given \( E \) ([10]). Basic properties of multivariate
normal distributions ([4], Ch. 8), allow to develop ([7] as
\[ \max_{E \subseteq \{1, \ldots, n\}} \max_{|E| \leq s} I(e;\hat{y}|u) = h(\hat{y}|u) - h(\hat{y}|u,E) \]
\[ = (1/2) \log C_{\hat{y}|u} - (1/2) \log \det C_{\hat{y}|u,E} \]
\[ = (1/2) \log \sigma_{\hat{y}|u}^2 - (1/2) \log \sigma_{\hat{y}|u,E}^2. \] (12)
Here, \( \sigma_{\hat{y}|u}^2 \) denotes the conditional variance of the prediction \( \hat{y} \),
conditioned on the user summary \( u \). Similarly, \( \sigma_{\hat{y}|u,E}^2 \) denotes
the conditional variance of \( \hat{y} \), conditioned on the user summary
\( u \) and the subset \( \{x_r\}_{r \in E} \) of features. The last step in ([12]
follows from the fact that \( \hat{y} \) is a scalar random variable.

Fig. 2. A simple probabilistic model for explainable ML.
The first component of the last expression in (12) does not depend on the choice \( E \) for the explanation \( e \) (see (10)). Therefore, the optimal choice \( E \) solves
\[
\sup_{|E| \leq s} -(1/2) \log \sigma^2_{\|u,E\|}. \tag{13}
\]
The maximization (13) is equivalent to
\[
\inf_{|E| \leq s} \sigma^2_{\|u,E\|}. \tag{14}
\]

In order to solve (14), we relate the conditional variance \( \sigma^2_{\|u,E\|} \) to a particular decomposition
\[
\hat{y} = \alpha u + \sum_{i \in E} \beta_i x_i + \epsilon. \tag{15}
\]

For an optimal choice of the coefficients \( \alpha \) and \( \beta_i \), the variance of the error term in (15) is given by \( \sigma^2_{\|u,E\|,c} \). Indeed,
\[
\min_{\alpha,\beta_i \in R} E\left\{ \left( \hat{y} - \alpha u - \sum_{i \in E} \beta_i x_i \right)^2 \right\} = \sigma^2_{\|u,E\|,c}. \tag{16}
\]

Inserting (16) into (14), an optimal choice \( E \) (of feature) for the explanation of prediction \( \hat{y} \) to user \( u \) is obtained from
\[
\inf_{|E| \leq s} \min_{\alpha,\beta_i \in R} E\left\{ \left( \hat{y} - \alpha u - \sum_{i \in E} \beta_i x_i \right)^2 \right\} = \min_{\|\beta\|_0 \leq s} E\left\{ \left( \hat{y} - \alpha u - \beta^T x \right)^2 \right\}. \tag{17}
\]

An optimal subset \( E_{\text{opt}} \) of features defining the explanation \( E \) (10) is obtained from any solution \( \beta_{\text{opt}} \) of (18) via
\[
E_{\text{opt}} = \text{supp} \beta_{\text{opt}}. \tag{19}
\]

### IV. A SIMPLE XML ALGORITHM

Under a Gaussian model (8) for the features of data points, Section III shows how to construct optimal explanations via the (support of the) solutions \( \beta_{\text{opt}} \) of the sparse linear regression problem (18).

In order to obtain a practical algorithm for computing (approximately) optimal explanations (19), we need to approximate the expectation in (18) with an empirical average over i.i.d. samples \((x^{(i)}, \hat{y}^{(i)}, u^{(i)})\) of features, predictions and user summaries. This results in Algorithm 1.

**Algorithm 1:** XML Algorithm

**Input:** explanation sparsity \( s \), training samples \((x^{(i)}, \hat{y}^{(i)}, u^{(i)})\) for \( i = 1, \ldots, m \)

1. compute \( \hat{\beta} \) by solving
\[
\hat{\beta} \in \arg\min_{\|\beta\|_0 \leq s} \sum_{i=1}^m \left( \hat{y}^{(i)} - \alpha u^{(i)} - \beta^T x^{(i)} \right)^2.
\]

**Output:** feature set \( \hat{E} := \text{supp} \hat{\beta} \)

Note that Algorithm 1 is interactive since the user has to provide samples \( u^{(i)} \) of its summary for the data points with features \( x^{(i)} \). Based on the user input \( u^{(i)} \), for \( i = 1, \ldots, m \), Algorithm 1 learns an optimal subset \( \hat{E} \) of features (10) that are used for the explanation of predictions.

The sparse regression problem (20) becomes intractable for large feature length \( n \). However, if the features are weakly correlated with each other and the user summary \( u \), the solutions of (20) can be found by convex optimization. Indeed, for a wide range of settings, sparse regression (20) can be solved via a convex relaxation, known as the least absolute shrinkage and selection operator (Lasso) [11].

\[
\hat{\beta} \in \arg\min_{\beta \in R^n} \sum_{i=1}^m \left( \hat{y}^{(i)} - \alpha u^{(i)} - \beta^T x^{(i)} \right)^2 + \lambda \|\beta\|_1. \tag{21}
\]

We have already a good understanding of choosing the Lasso parameter \( \lambda \) in (21) such that its solutions coincide with the solutions of (20) (see, e.g., [11]).

### V. NUMERICAL EXPERIMENTS

We verify the ability of Algorithm 1 to provide explainable ML using a computer vision application. In particular, we consider data points representing square patches of a greyscale aerial photograph of Helsinki city area\(^1\). The goal is to predict the greyscale value \( y \) of the center (“target”) pixel. In order to predict the greyscale value of the \( i \)th pixel \( y^{(i)} \) we use the greyscale values \( x_j^{(i)} \) of close-by pixels \( j \in P^{(i)} \). As depicted in Figure 3 the neighbourhood \( j \in P^{(i)} \) is constituted by two rectangular areas that are adjacent to pixel \( i \). A user having

![Fig. 3. The greyscale level of a particular target pixel within an aerial photograph can be predicted based on the greyscale values of nearby pixels within adjacent rectangles (indicated).](https://kar.helm/)

some prior experience in processing natural images might consider the average greyscale value
\[
u^{(i)} = (1/|P^{(i)}|) \sum_{j \in P^{(i)}} x_j^{(i)} \tag{22}
\]
as a reasonable value of the features \( x^{(i)} := \{x_j^{(i)}\}_{j \in P^{(i)}} \). We refer to the Python notebook [https://github.com/alexjungaalto/ResearchPublic/blob/master/lxml.ipynb] for the results of the experiments.

### VI. CONCLUSION

We have introduced a simple probabilistic model for the predictions of a ML method and the user background. The user background is represented by a summary of the features of a data point. The effect of an explanation is measured by the conditional MI between prediction and explanation, given the user summary of a data point.

\(^1\)The data is freely available via the online map service [https://kar.helm/](https://kar.helm/)
REFERENCES


