

# Probabilities for machine-learning classifiers

## Classifiers as diagnostic tests

K. Dirland

&lt;\*\*\*@\*\*\*&gt;

A. S. Lundervold

&lt;\*\*\*@\*\*\*&gt;

P.G.L. Porta Mana 

&lt;pgl@portamana.org&gt;

(or any permutation thereof)


Draft. 14 April 2022; updated 19 April 2022



## 1 Sensible probabilities for classifiers


Some machine-learning algorithms for classification, such as support-vector machines, typically output a class label. Others, such as deep networks, output a set of real numbers. These real numbers can be positive, normalized to unity, and can bear some qualitative relation to the plausibilities of the classes. But they cannot be reliably interpreted as sensible probabilities, that is, as the degrees of belief assigned to each possible class by a rational agent<sup>1</sup>; or, in terms of ‘populations’<sup>2</sup>, as the expected frequencies of the classes in the hypothetical population of units (degrees of belief and frequencies being related by de Finetti’s theorem<sup>3</sup>).

Algorithms that internally do perform probabilistic calculations, such as naive-Bayes or logistic-regression classifiers<sup>4</sup>, unfortunately rest on probabilistic assumptions, such as independence and particular shapes of distributions, that are often unrealistic (and their consistency with the specific application is rarely checked). Only particular classifiers such as Bayesian neural networks<sup>5</sup> output sensible probabilities.

Why are probability values important? As we argue in a companion work , our ultimate purpose in classification is seldom only to guess a class; most often it is to choose a specific course of action, or to make a decision, among several available ones. A clinician, for example, does not

<sup>1</sup> MacKay 1992; Gal & Ghahramani 2016; Russell & Norvig 2022 chs 2, 12, 13. <sup>2</sup> Lindley & Novick 1981; Fisher 1967 § II.4. <sup>3</sup> Bernardo & Smith 2000 ch. 4; Dawid 2013. <sup>4</sup> Murphy 2012 § 3.5, ch. 8; Bishop 2006 §§ 8.2, 4.3; Barber 2020 ch. 10, § 17.4. <sup>5</sup> Neal & Zhang 2006; Bishop 2006 § 5.7.

simply tell a patient “you will probably not contract the disease”, but has to decide among dismissal or different kinds of preventive treatment<sup>6</sup>. Said otherwise, in classification we must choose the *optimal* class, not the probably true one. Making optimal choices in situations of uncertainty is the domain of Decision Theory<sup>7</sup>. In order to make an optimal choice, decision theory requires the use of probability values that properly reflect our state of uncertainty.

Determining class probabilities conditional on the input features is unfortunately computationally unfeasible at present for problems that involve very high-dimensional spaces, such as image classification; in fact if an exact probabilistic analysis were possible we would not be developing machine-learning classifiers in the first place<sup>8</sup>.  Maybe useful to add a reminder that probability theory is the *learning* theory par excellence (even if there's no ‘learning’ in its name)? Its rules are all about making logical updates given new data.

In the present work we propose an alternative solution that has a low computational cost and that can be applied to all commonly used classifiers, even those that only output class labels.

The essential idea comes from seeing an analogy between a classifier and a diagnostic test, such as any common diagnostic or prognostic test used in medicine for example. There are many parallels in the way machine-learning classifiers and diagnostic tests, a flu test for instance, are devised and work. Our basic motivation in using either is that we would like to assess some situational variable – class, pathological condition – by means of its correlation (in the general sense of the word, not the linear Pearson one; and including deterministic dependence as a particular case) with a set of ‘difficult’ variables that are either too complex or hidden – image pixels, presence of replicating viral agents –:

situational variable  $\longleftrightarrow$  difficult variables

We devise an auxiliary variable – algorithm output, test result – to be correlated with the difficult variables:

situational variable  $\longleftrightarrow$  difficult variables  $\longleftrightarrow$  aux variable

We can now assess the situational variable by observing the more easily accessible auxiliary variable instead of the difficult ones. In probability language we are *marginalizing* over the difficult variables. This is the

---

<sup>6</sup> Sox et al. 2013; Hunink et al. 2014. <sup>7</sup> Russell & Norvig 2022 ch. 15; Jeffrey 1965; North 1968; Raiffa 1970. <sup>8</sup> Russell & Norvig 2022 chs 2, 12; Pearl 1988.

procedure dictated by the probability calculus whenever we do not have informational access to a set of variables. The correlation of the auxiliary variable is achieved by the training process in the case of the machine-learning algorithm, and by the exploitation of biochemical processes or reactions in the case of the flu test.

The situational variable is *informationally screened* from the auxiliary variable by the difficult variables. That is, the auxiliary variable does not – in fact, cannot – contain any more information about the situational variable than that contained in the difficult variables. This means that the probability relationship between the three variables is as follows:

$$p\left(\begin{array}{c} \text{situational} \\ \text{variable} \end{array} \middle| \begin{array}{c} \text{aux} \\ \text{variable} \end{array}\right) = \sum_{\text{difficult variables}} p\left(\begin{array}{c} \text{situational} \\ \text{variable} \end{array} \middle| \begin{array}{c} \text{difficult} \\ \text{variables} \end{array}\right) \times p\left(\begin{array}{c} \text{difficult} \\ \text{variables} \end{array} \middle| \begin{array}{c} \text{aux} \\ \text{variable} \end{array}\right), \quad (1)$$

the sum running over all possible values of the difficult variables.

In the case of the diagnostic test we determine the probability  $p\left(\begin{array}{c} \text{situational} \\ \text{variable} \end{array} \middle| \begin{array}{c} \text{aux} \\ \text{variable} \end{array}\right)$  by carrying out the test on a representative sample of cases and collecting joint statistics between the test's output and the true situation, the presence of the flu in our example. These statistics are typically displayed in a so-called contingency table<sup>9</sup>, akin to a confusion matrix.

Unlike the case of a diagnostic test, the output of a machine-learning classifier is usually taken at face value: if the output is a class label, that label is regarded as the true class; if the output is a unity-normalized tuple of positive numbers, that tuple is regarded as the probability distribution for the classes.

We instead propose to *treat the classifier's output just like a diagnostic test's result*. This output, discrete or continuous, is regarded as a quantity that has some correlation with the true class. This correlation can be analysed in a set of representative samples and used to calculate a sensible probability for the class given the classifier's output. This analysis only needs to be made once and is computationally cheap, because the classifier output takes values in a discrete or low-dimensional space.

<sup>9</sup> Fienberg 2007; Mosteller et al. 2013.

This approach differs from the computationally infeasible one discussed above in that we are calculating the computationally easier probability

$$p(\text{class} \mid \text{output}) \quad (2)$$

rather than

$$p(\text{class} \mid \text{feature}) . \quad (3)$$

The former probability, as we saw in eq. (1), is the marginal

$$p(\text{class} \mid \text{output}) = \sum_{\text{feature}} p(\text{class} \mid \text{feature}) \times p(\text{feature} \mid \text{output}) . \quad (4)$$

We can thus think of this approach as a marginalization over the possible features, which is a necessary operation as have no effective access to them.


A hallmark of this approach is that we are calculating exact probabilities conditional on reduced information, rather than approximate probabilities conditional on full information. This protects us from biases that are typically present in the approximation method. The price of using reduced information is that the probabilities may be open to more variability as we collect more representative data. But as we shall see this variability is actually quite low, and moreover it can be exactly assessed.

This approach also offers the following advantages:


- It does not require any changes of the standard training procedures.
- It is easily implemented as an additional low-cost computation of a function at the end of the classifier's output, or as a replacement of a softmax-like computation.
- It does not make any assumptions such as linearity or gaussianity.
- It yields not only the probability distribution for the classes, but also a measure of how much this distribution could change if we collected more test data (the 'probability of the probability', so to speak).
- It allows us to use the classifier both in a discriminative and generative way. That is, we can use either  $p(\text{class} \mid \text{output})$ , or  $p(\text{output} \mid \text{class})$  in conjunction with Bayes's theorem. The latter approach enables us to avoid possible base-rate fallacies<sup>10</sup>.

---

<sup>10</sup> Russell & Norvig 2022 § 12.5; Axelsson 2000; Jenny et al. 2018.

- It can be seamlessly integrated with a utility matrix to compute the optimal class, as shown in the companion work .

In § 2 we present some notation and the general procedure for the calculation of the probabilities; more technical details are given in appendix 6. Section 3 explains how to augment a classifier's output with the probability calculation. Results of numerical experiments are presented in § 4.

 We could show that even if we used a biased test set, the method corrects the bias (provided we know what the bias is).

## 2 Calculation of the probabilities: general procedure

Let us denote the class variable by  $C$  and the classifier-output variable by  $X$ . We assume that  $C$  is discrete and finite, its values can be simply renamed  $1, 2, 3, \dots$ . We assume that  $X$  is either discrete and finite (it is isomorphic to  $C$  for many classifying algorithms) or a low-dimensional tuple of real variables; a combination of both cases can also be easily accommodated. We assume to have a sample of  $M$  such data pairs denoted collectively by  $D$ :

$$D := \{(c_1, x_1), (c_2, x_2), \dots, (c_M, x_M)\}. \quad (5)$$

We call them *calibration data*. Let us emphasize that these are not pairs of class & feature values, but pairs of class & classifier-output values, obtained as described in § 3.


Instead of the conditional probability  $p(\text{class} \mid \text{output})$ , that is,  $p(C \mid X)$ , we can actually calculate the joint probability

$$p(C, X) \quad (6)$$

given the sample data. The computational cost is the same, but from the joint probability we can easily derive both conditionals

$$p(C \mid X) = \frac{p(C, X)}{\sum_C p(C, X)}, \quad (7)$$

$$p(X \mid C) = \frac{p(C, X)}{\sum_X p(C, X)}. \quad (8)$$

It is advantageous to have both, as we shall see in § : if one of them is biased owing to the way the test samples were obtained, we can still use the other.

In our specific inference problem, where no time trends are assumed to exist in future data (the probability distribution for future data is exchangeable), probability theory dictates that the joint probability (6) for a new datapoint  $(c_0, x_0)$  is equal to the *expected* frequency of that datapoint in a hypothetically infinite run of observations, that is, the average

$$p(c_0, x_0) = \int F(c_0, x_0) w(F) dF . \quad (9)$$


This formula is de Finetti's theorem<sup>11</sup>. It is derived from first principles but can be intuitively interpreted: We are considering every possible long-run frequency distribution  $F(\cdot, \cdot)$ , giving it a weight  $w(F)$ , and then taking the weighted sum of all such distributions. The result is still a distribution, and its value at  $(c_0, x_0)$  is the probability of this datapoint.

The weight  $w(F)$  – a probability density – given to a frequency distribution  $F$  is proportional to two factors:

$$w(F) \propto F(D) w_g(F) . \quad (10)$$

- The first factor ('likelihood')  $F(D)$  quantifies how well  $F$  fits known data of the same kind, the sample data  $D$  in our case. It is simply proportional to how frequent the known data would be, according to  $F$ :

$$F(D) = F(c_1, x_1) F(c_2, x_2) \cdots F(c_M, x_M) . \quad (11)$$

- The second factor ('prior')  $w_g(F)$  quantifies how well  $F$  generalizes beyond the data we have seen, owing to reasons such as physical or biological constraints for example. In our case we expect  $F$  to be somewhat smooth in  $X$  when this variable is continuous<sup>12</sup>  **add a picture – a sample from the prior over  $F$  – to illustrate the expected range of smoothness.** No assumptions are made about  $F$  when  $X$  is discrete.

The proportionality constant in eq. (10) is simply the integral  $\int F(D) w_g(F) dF$  ensuring that  $w(F)$  is normalized.

The first factor becomes larger as the number of known data increases. Thus a large amount of data indicating a non-smooth distribution  $F$  will override any smoothness preferences embodied in the second factor.

<sup>11</sup> Bernardo & Smith 2000 ch. 4; Dawid 2013; de Finetti 1929; 1937. <sup>12</sup> Cf. Good & Gaskins 1971.

Note that no assumptions about the shape of  $F$  – no gaussians, logistic curves, sigmoids, and so on – are made in this approach.

The integral in (9) is calculated in either of two ways, depending on whether  $X$  is discrete or continuous. For  $X$  discrete and taking on the same values as the class variable  $C$ , the integral is over  $\mathbf{R}^{n_c}$  where  $n_c$  is the number of possible classes, and can be done analytically. For  $X$  continuous, the integral is numerically approximated by a sum over a representative sample, obtained by Markov-chain Monte Carlo, of distributions  $F$  according to the weights (10). The error of this approximation can be calculated and made as small as required by increasing the number of Monte Carlo samples.

The expected value (9) is calculated for all possible values of  $(c_0, x_0)$ , obtaining the full joint probability distribution  $p(C, X)$ . From this joint distribution we calculate the direct and inverse conditional distributions

$$p(C | X) = \frac{p(C, X)}{\sum_C p(C, X)} , \quad (12)$$

$$p(X | C) = \frac{p(C, X)}{\sum_X p(C, X)} . \quad (13)$$

It is very convenient to have both, as discussed in § 5.

The conditional distributions above are just matrices when  $X$  is discrete. For continuous  $X$  they can be regarded as  $n_c$  tuples of functions in  $X$ . We can find convenient approximate expressions, such as polynomial interpolants, for faster numerical implementations of these functions.

The integration procedure for (9) also tells us how much the probability distribution  $p(C, X)$  would change if we acquired new data (a sort of ‘probability of the probability’).

For further mathematical details see appendix 6.

### 3 Implementation in the classifier output

The implementation of our approach takes place after the training of the classifier has been carried out in the usual way. We assume that a collection of  $M$  test data were set aside as usual:

$$T := \{(c_1, z_1), (c_2, z_2), \dots, (c_M, z_M)\} , \quad (14)$$

where the  $c_i$  are the true classes and  $z_i$  the corresponding feature values.

The  $M$  feature values  $z_i$  are given as inputs to the classifier, which produces  $M$  corresponding outputs  $x_i$ . We now consider data pairs consisting in the true classes  $c_i$  and the outputs  $x_i$ : these are the *calibration data* discussed in § 2:

$$D := \{(c_1, x_1), (c_2, x_2), \dots, (c_M, x_M)\}.$$


They are used to find the direct and inverse conditional probability distributions  $p(C | X)$  and  $p(X | C)$  as described in § 2.

We can finally augment our classifier either in a ‘direct’ or ‘discriminative’ way, or an ‘inverse’ or ‘generative’ way, by adding one computation step at the end of the classifier’s operation:

**Direct:** from its output  $x_0$  we obtain the probability for each class,  $p(c | x_0)$ .

**Inverse:** from its output  $x_0$  we obtain the probability of the output itself, conditional on each class,  $p(x_0 | c)$ .

These  $n_c$  probabilities are the final output of the augmented classifier.

In the direct or discriminative case, at each new use of the classifier the output probabilities can be used together with a utility matrix to choose the *optimal* class for that case, as discussed in the companion paper .

In the inverse or generative case, at each new use of the classifier the probabilities for the classes are obtained via Bayes’s theorem:

$$p(c) = \frac{p(x_0 | c) B(c)}{\sum_c p(x_0 | c) B(c)}, \quad (15)$$

where  $B(c)$  is the base rate of class  $c$ . The probabilities  $p(c)$  can finally be used together with a utility matrix to choose the *optimal* class.


## 4 Numerical experiments and results

### 5 Circumventing biases

### 6 Mathematical details of the nonparametric density regression

The joint probability (6) is calculated nonparametrically, that is, without making any assumptions such as linearity or gaussianity, besides very mild and reasonable assumptions of continuity.



using the versatile computational approach by Dunson & Bhattacharya (2011), and obtain the probability (2) by conditionalization. The calculation requires Monte Carlo sampling  [refs here](#) but needs to be made only once.

## 7 Summary and discussion

## Appendix: broader overview of binary classification

Let us consider our binary-classification problem from a general perspective and summarize how it would be approached and solved from first principles<sup>13</sup> if our computational resources had no constraints.

In our long-term task we will receive ‘units’ of a specific kind; the units for example could be gadgets, individuals, or investment portfolios. Each new unit will belong to one of two classes, which we can denote  $X=0$  and  $X=1$ ; for example they could be ‘defective’ vs ‘non-defective’, ‘ill’ vs ‘healthy’. The class will be unknown to us. For each new unit we shall need to decide among two possible actions, which we can denote  $A=\hat{0}$  and  $A=\hat{1}$ ; for example ‘discard’ vs ‘keep’, or ‘treat’ vs ‘dismiss’. The utility of each action depends on the unknown class of the unit; we denote these utilities by  $U(A | X)$ . For each new unit we will be able to measure a ‘feature’  $Z$  of a specific kind common to all units; for example  $Z$  could be a set of categorical and real quantities, or an image such as a brain scan. We have a set of units – our ‘sample units’ or ‘sample data’ – that are somehow “representative” of the units we will receive in our long-term task<sup>14</sup>. we know both the class and the feature of each of these sample units. Let us denote this sample information by  $D$ .

According to the principles of decision theory and probability theory, for each new unit we would proceed as follows:

1. Assign probabilities to the two possible values of the unit’s class, given the value of the unit’s feature  $Z=z$ , our sample data  $D$ , and any other available information:

$$p(X=0 | Z=z, D), \quad p(X=1 | Z=z, D) \equiv 1 - p(X=0 | Z=z, D), \quad (16)$$

according to the rules of the probability calculus.

2. Calculate the expected utilities  $\bar{u}$  of the two possible actions:

$$\begin{aligned} \bar{u}(\hat{0}) &:= U(\hat{0} | X=0) p(X=0 | Z=z, D) + U(\hat{0} | X=1) p(X=1 | Z=z, D) \\ \bar{u}(\hat{1}) &:= U(\hat{1} | X=0) p(X=0 | Z=z, D) + U(\hat{1} | X=1) p(X=1 | Z=z, D) \end{aligned} \quad (17)$$

and choose the action having maximal expected utility.

<sup>13</sup> Russell & Norvig 2022 part IV. <sup>14</sup> for a critical analysis of the sometimes hollow term ‘representative sample’ see Kruskal & Mosteller 1979a,b,c; 1980.

How is the probability  $p(X | Z=z, D)$  determined by the probability calculus? Here is a simplified, intuitive picture. First consider the case where the feature  $Z$  can only assume a small number of possible values, so that many units can in principle have the same value of  $Z$ .

Consider the collection of all units having  $Z = z$  that we received in the past and will receive in the future. Among them, a proportion  $F(X=0 | Z=z)$  belong to class 0, and a proportion  $1 - F(X=0 | Z=z) \equiv F(X=1 | Z=z)$  to class 1. For example these two proportions could be 74% and 26%. Our present unit with  $Z=z$  is a member of this collection. The probability  $p(X=0 | Z=z)$  that our unit belongs to class 0, given that its feature has value  $z$ , is then intuitively equal to the proportion  $F(X=0 | Z=z)$ . Analogously for  $X=1$ .

The problem is that we do not know the proportion  $F(X=0 | Z=z)$ . However, we expect it to be roughly equal to the analogous proportion seen in our sample data; let us denote the latter by  $F_s(X=0 | Z=z)$ :

$$F(X=0 | Z=z) \sim F_s(X=0 | Z=z) . \quad (18)$$

this is indeed what we mean by saying that our sample data are ‘representative’ of the future units. Later we shall discuss the case in which such representativeness is of different kinds. We expect the discrepancy between  $F(X=0 | Z=z)$  and  $F_s(X=0 | Z=z)$  to be smaller, the larger the number of sample data. Vice versa we expect it to be larger, the smaller the number of sample data.

If  $Z$  can assume a continuum of values, as is the case for a brain scan for example, then the collection of units having  $Z=z$  is more difficult to imagine. In this case each unit will be unique in its feature value – no two brains are exactly alike.

---

old text below

Given the unit’s feature  $Z$  we will assign probabilities to the possible values of the unit’s class: according to the rules of the probability calculus.

Suppose we have a population of units or individuals characterized by a possibly multidimensional variable  $Z$  and a binary variable  $X \in \{0, 1\}$ . Different joint combinations of  $(X, Z)$  values can appear in this population. Denote by  $F(X=x, Z=z)$ , or more simply  $F(x, z)$  when there is no confusion, the number of individuals having specific joint values  $(X=x, Z=z)$ . This is the absolute frequency of the values  $(x, z)$ . We can also count the number of individuals having a specific value of  $Z=z$ ,

regardless of  $X$ ; this is the marginal absolute frequency  $F(z)$ . It is easy to see that

$$F(z) = F(X=0, z) + F(X=1, z) \equiv \sum_x F(x, z). \quad (19)$$

Analogously for  $F(x)$ .

Select only the subpopulation of individuals that have a specific value  $Z=z$ . In this subpopulation, the *proportion* of individuals having a specific value  $X=x$  is  $f(x | Z=z)$ . This is the conditional relative frequency of  $x$  given that  $z$ . It is easy to see that

$$f(x | z) = \frac{F(x, z)}{F(z)}. \quad (20)$$

Now suppose that we know all these statistics about this population. An individual coming from this population is presented to us. We measure its  $Z$  and obtain the value  $z$ . What could be the value of  $X$  for this individual? We know that among all individuals having  $Z=z$  (and the individual before us is one of them) a proportion  $f(x | z)$  has  $X=x$ . Thus we can say that there is a probability  $f(x | z)$  that our individual has  $X=x$ . And this is all we can say if we only know  $Z$ .

For this individual we must choose among two actions  $\{a, b\}$ . The utility of performing action  $a$  if the individual has  $X=x$ , and given any other known circumstances, is  $U(a | x)$ ; similarly for  $b$ . If we knew the value of  $X$ , say  $X=0$ , we would simply choose the action leading to maximal utility:

$$\begin{aligned} &\text{if } U(a | X=0) > U(b | X=0) \quad \text{then choose action } a, \\ &\text{if } U(a | X=0) < U(b | X=0) \quad \text{then choose action } b, \\ &\text{else} \quad \text{it does not matter which action is chosen.} \end{aligned} \quad (21)$$

But we do not know the actual value of  $X$ . We have probabilities for the possible values of  $X$  given that  $Z=z$  for our individual. Since  $X$  is uncertain, the final utilities of the two actions are also uncertain; but we can calculate their *expected* values  $\bar{U}(a | Z=z)$  and  $\bar{U}(b | Z=z)$ :

$$\begin{aligned} \bar{U}(a | z) &:= U(a | X=0) f(X=0 | z) + U(a | X=1) f(X=1 | z), \\ \bar{U}(b | z) &:= U(b | X=0) f(X=0 | z) + U(b | X=1) f(X=1 | z). \end{aligned} \quad (22)$$

Decision theory shows that the optimal action is the one having the maximal expected utility. Our choice therefore proceeds as follows:

$$\begin{aligned} &\text{if } \bar{U}(a | z) > \bar{U}(b | z) \quad \text{then choose action } a, \\ &\text{if } \bar{U}(a | z) < \bar{U}(b | z) \quad \text{then choose action } b, \\ &\text{else} \quad \text{it does not matter which action is chosen.} \end{aligned} \quad (23)$$

The decision procedure just discussed is very simple and does not need any machine-learning algorithms. It could be implemented in a simple algorithm that takes as input the full statistics  $F(X, Z)$  of the population, the utilities, and yields an output according to (23).

Our main problem is that the full statistics  $F(X, Z)$  is almost universally not known. Typically we only have the statistics  $F_s(X, Z)$  of a sample of individuals that come from the population of interest or from populations that are somewhat related to the one of interest. This is where probability theory steps in. It allows us to assign probabilities to all the possible statistics  $F(X, Z)$ . From these probabilities we can calculate the *expected* value  $\bar{f}(x | z)$  of the conditional frequencies  $f(x | z)$ . Decision theory says that the expected value  $\bar{f}(x | z)$  should then be used, in this uncertain case, in eq. (22) in place of the unknown  $f(x | z)$ . The decision procedure (23) can then be used again.

Probability theory says that in this particular situation the probability of a particular possible statistics  $F(X, Z)$  is the product of two factors having intuitive interpretations:

- the probability of observing the statistics  $F_s(X, Z)$  of our data sample, assuming the full statistics to be  $F(X, Z)$ . With some combinatorics it can be shown that this probability is proportional to

$$\exp \left[ \sum_{X, Z} F_s(X, Z) \ln F(X, Z) \right] \quad (24)$$

The argument of the exponential is the cross-entropy between  $F_s(X, Z)$  and  $F(X, Z)$ ; this is the reason of its appearance in the loss function used for classifiers<sup>15</sup>.

This factor tells us how much the possible statistics *fit* the sample data; it gives more weight to statistics with a better fit.

---

<sup>15</sup> Bridle 1990; MacKay 1992.

- the probability of the full statistics  $F(X, Z)$  for reasons not present in the data, for example because of physical laws, biological plausibility, or similar.

This factor tells us whether the possible statistics should be favourably considered, or maybe even discarded instead, for reasons that go beyond the data we have seen; in other words, whether the hypothetical statistics would *generalize* well beyond the sample data.

The final probability comes from the balance between these ‘fit’ and ‘generalization’ factors. Note that the first factor becomes more important as the sample size and therefore  $F_s(X, Z)$  increases; the sample data eventually determine what the most probable statistics is, if the sample is large enough.

A similar probabilistic reasoning applies if our sample data come not from the population of interest but from a population having at least the same *conditional* frequencies of as the one of interest, either  $f(X | Z)$  or  $f(Z | X)$ . The latter case must be examined with care when our purpose is to guess  $X$  from  $Z$ . In this case we cannot use the conditional frequencies  $f_s(X | Z)$  that appear in the data to obtain the expected value  $\bar{f}(X | Z)$ : they could be completely different from the ones of the population of interest. We must instead use the sample conditional frequencies  $f_s(Z | X)$  to obtain the expected value  $\bar{f}(Z | X)$ , and then combine the latter with an appropriate probability  $P(X)$  through Bayes’s theorem:

$$\frac{\bar{f}(Z | X) P(X)}{\sum_X \bar{f}(Z | X) P(X)} . \quad (25)$$

The probability  $P(X)$  cannot be obtained from the data, but requires a separate study or survey. In medical applications, where  $X$  represents for example the presence or absence of a disease, the probability  $P(X)$  is the base rate of the disease. Direct use of  $f_s(X | Z)$  from the data instead of (25) is the ‘base-rate fallacy’<sup>16</sup>.

In supervised learning the classifier is trained to learn the most probable  $f(X | Z)$  from the data. The training finds the  $f(X | Z)$  that most closely fits the conditional frequency  $f_s(X | Z)$  of the sampled data; this roughly corresponds to maximizing the first factor (24) described above.

<sup>16</sup> Russell & Norvig 2022 § 12.5; Axelsson 2000; Jenny et al. 2018.

The architecture and the parameter regularizer of the classifier play the role of the second factor.

## Bibliography

- (‘de  $X$ ’ is listed under D, ‘van  $X$ ’ under V, and so on, regardless of national conventions.)
- Axelsson, S. (2000): *The base-rate fallacy and the difficulty of intrusion detection*. ACM Trans. Inf. Syst. Secur. **3**<sup>3</sup>, 186–205. DOI:10.1145/357830.357849, <http://www.scs.carleton.ca/~soma/id-2007w/readings/axelsson-base-rate.pdf>.
- Barber, D. (2020): *Bayesian Reasoning and Machine Learning*, online update. (Cambridge University Press, Cambridge). <http://www.cs.ucl.ac.uk/staff/d.barber/brml>. First publ. 2007.
- Bernardo, J. M., Bayarri, M. J., Berger, J. O., Dawid, A. P., Heckerman, D., Smith, A. F. M., West, M., eds. (2011): *Bayesian Statistics 9*. (Oxford University Press, Oxford). DOI: 10.1093/acprof:oso/9780199694587.001.0001.
- Bernardo, J.-M., Smith, A. F. (2000): *Bayesian Theory*, repr. (Wiley, New York). DOI: 10.1002/9780470316870. First publ. 1994.
- Bishop, C. M. (2006): *Pattern Recognition and Machine Learning*. (Springer, New York). <https://www.microsoft.com/en-us/research/people/cmbishop/prml-book>.
- Bridle, J. S. (1990): *Probabilistic interpretation of feedforward classification network outputs, with relationships to statistical pattern recognition*. Neurocomputing **68**, 227–236. DOI: 10.1007/978-3-642-76153-9\_28.
- Cifarelli, D. M., Regazzini, E. (1979): *Considerazioni generali sull’impostazione bayesiana di problemi non parametrici. Le medie associative nel contesto del processo aleatorio di Dirichlet*. Riv. mat. sci. econ. soc. **2**<sup>1,2</sup>, 39–52, 95–111.
- Damien, P., Dellaportas, P., Polson, N. G., Stephens, D. A., eds. (2013): *Bayesian Theory and Applications*. (Oxford University Press, Oxford). DOI:10.1093/acprof:oso/9780199695607.001.0001.
- Dawid, A. P. (2013): *Exchangeability and its ramifications*. In: Damien, Dellaportas, Polson, Stephens (2013): ch. 2:19–29. DOI:10.1093/acprof:oso/9780199695607.003.0002.
- de Finetti, B. (1929): *Funzione caratteristica di un fenomeno aleatorio*. In: *Atti del Congresso Internazionale dei Matematici*: ed. by S. Pincherle (Zanichelli, Bologna): 179–190. <https://www.mathunion.org/icm/proceedings>, <http://www.brunodefinetti.it/Opere.htm>. Transl. in Cifarelli, Regazzini (1979). See also de Finetti (1930).
- (1930): *Funzione caratteristica di un fenomeno aleatorio*. Atti Accad. Lincei: Sc. Fis. Mat. Nat. **IV**<sup>5</sup>, 86–133. <http://www.brunodefinetti.it/Opere.htm>. Summary in de Finetti (1929).
- (1937): *La prévision: ses lois logiques, ses sources subjectives*. Ann. Inst. Henri Poincaré **7**<sup>1</sup>, 1–68. [http://www.numdam.org/item/AIHP\\_1937\\_\\_7\\_1\\_1\\_0](http://www.numdam.org/item/AIHP_1937__7_1_1_0). Transl. in Kyburg, Smokler (1980), pp. 53–118, by Henry E. Kyburg, Jr.
- Dunson, D. B., Bhattacharya, A. (2011): *Nonparametric Bayes regression and classification through mixtures of product kernels*. In: Bernardo, Bayarri, Berger, Dawid, Heckerman, Smith, West (2011): 145–158. <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.178.1521>, DOI:10.1093/acprof:oso/9780199694587.003.0005, older version at [https://www.researchgate.net/publication/228447342\\_Nonparametric\\_Bayes\\_Regression\\_and\\_Classification\\_Through\\_Mixtures\\_of\\_Product\\_Kernels](https://www.researchgate.net/publication/228447342_Nonparametric_Bayes_Regression_and_Classification_Through_Mixtures_of_Product_Kernels).

- Fienberg, S. E. (2007): *The Analysis of Cross-Classified Categorical Data*, 2nd ed. (Springer, New York). DOI:10.1007/978-0-387-72825-4. First publ. 1980.
- Fisher, R. A. (1967): *Statistical Methods and Scientific Inference*, repr. of 2nd rev. ed. (Oliver and Boyd, Edinburgh). First publ. 1956.
- Gal, Y., Ghahramani, Z. (2016): Dropout as a Bayesian approximation: representing model uncertainty in deep learning. Proc. Mach. Learn. Res. **48**, 1050–1059. See also Appendix at arXiv DOI:10.48550/arXiv.1506.02157.
- Good, I. J., Gaskins, R. A. (1971): Nonparametric roughness penalties for probability densities. *Biometrika* **58**<sup>2</sup>, 255–277. DOI:10.1093/biomet/58.2.255.
- Goodman, L. A., Kruskal, W. H. (1954): Measures of association for cross classifications. *J. Am. Stat. Assoc.* **49**<sup>268</sup>, 732–764. DOI:10.1080/01621459.1954.10501231. See corrections Goodman, Kruskal (1957; 1958) and also Goodman, Kruskal (1959; 1963; 1972).
- (1957): Corrigenda: Measures of association for cross classifications. *J. Am. Stat. Assoc.* **52**<sup>280</sup>, 578. DOI:10.1080/01621459.1957.10501415. See Goodman, Kruskal (1954).
- (1958): Corrigenda: Measures of association for cross classifications. *J. Am. Stat. Assoc.* **53**<sup>284</sup>, 1031. DOI:10.1080/01621459.1958.10501492. See Goodman, Kruskal (1954).
- (1959): Measures of association for cross classifications. II: Further discussion and references. *J. Am. Stat. Assoc.* **54**<sup>285</sup>, 123–163. DOI:10.1080/01621459.1959.10501503. See also Goodman, Kruskal (1954; 1963; 1972).
- (1963): Measures of association for cross classifications. III: Approximate sampling theory. *J. Am. Stat. Assoc.* **58**<sup>302</sup>, 310–364. DOI:10.1080/01621459.1963.10500850. See correction Goodman, Kruskal (1970) and also Goodman, Kruskal (1954; 1959; 1972).
- (1970): Corrigenda: Measures of association for cross classifications. III: Approximate sampling theory. *J. Am. Stat. Assoc.* **65**<sup>330</sup>, 1011. DOI:10.1080/01621459.1970.10481142. See Goodman, Kruskal (1963).
- (1972): Measures of association for cross classifications, IV: Simplification of asymptotic variances. *J. Am. Stat. Assoc.* **67**<sup>338</sup>, 415–421. DOI:10.1080/01621459.1972.10482401. See also Goodman, Kruskal (1954; 1959; 1963).
- Guyon, I., Gunn, S., Nikravesh, M., Zadeh, L. A., eds. (2006): *Feature Extraction: Foundations and Applications*. (Springer, Berlin). DOI:10.1007/978-3-540-35488-8.
- Hunink, M. G. M., Weinstein, M. C., Wittenberg, E., Drummond, M. F., Pliskin, J. S., Wong, J. B., Glasziou, P. P. (2014): *Decision Making in Health and Medicine: Integrating Evidence and Values*, 2nd ed. (Cambridge University Press, Cambridge). DOI:10.1017/CB09781139506779. First publ. 2001.
- Jeffrey, R. C. (1965): *The Logic of Decision*. (McGraw-Hill, New York).
- Jenny, M. A., Keller, N., Gigerenzer, G. (2018): Assessing minimal medical statistical literacy using the Quick Risk Test: a prospective observational study in Germany. *BMJ Open* **8**, e020847, e020847/corr2. DOI:10.1136/bmjopen-2017-020847, DOI:10.1136/bmjopen-2017-020847/corr2.
- Kruskal, W., Mosteller, F. (1979a): Representative sampling, I: Non-scientific literature. *Int. Stat. Rev.* **47**<sup>1</sup>, 13–24. See also Kruskal, Mosteller (1979b,c; 1980).
- (1979b): Representative sampling, II: Scientific literature, excluding statistics. *Int. Stat. Rev.* **47**<sup>2</sup>, 111–127. See also Kruskal, Mosteller (1979a,c; 1980).
- (1979c): Representative sampling, III: The current statistical literature. *Int. Stat. Rev.* **47**<sup>3</sup>, 245–265. See also Kruskal, Mosteller (1979a,b; 1980).
- (1980): Representative sampling, IV: The history of the concept in statistics, 1895–1939. *Int. Stat. Rev.* **48**<sup>2</sup>, 169–195. See also Kruskal, Mosteller (1979a,b,c).



- Kyburg Jr., H. E., Smokler, H. E., eds. (1980): *Studies in Subjective Probability*, 2nd ed. (Robert E. Krieger, Huntington, USA). First publ. 1964.
- Lindley, D. V., Novick, M. R. (1981): *The role of exchangeability in inference*. *Ann. Stat.* **9**<sup>1</sup>, 45–58. [DOI:10.1214/aos/1176345331](#).
- MacKay, D. J. C. (1992): *The evidence framework applied to classification networks*. *Neural Comput.* **4**<sup>5</sup>, 720–736. <http://www.inference.phy.cam.ac.uk/mackay/PhD.html>, [DOI:10.1162/neco.1992.4.5.720](#).
- Mosteller, F., Fienberg, S. E., Rourke, R. E. K. (2013): *Beginning statistics with data analysis*, repr. (Dover, Mineola, USA). First publ. 1983.
- Murphy, K. P. (2012): *Machine Learning: A Probabilistic Perspective*. (MIT Press, Cambridge, USA). <https://problml.github.io/pml-book/book0.html>.
- Neal, R. M., Zhang, J. (2006): *High dimensional classification with Bayesian neural networks and Dirichlet diffusion trees*. In: Guyon, Gunn, Nikravesh, Zadeh (2006): ch. 10:265–296. [DOI:10.1007/978-3-540-35488-8\\_11](#).
- North, D. W. (1968): *A tutorial introduction to decision theory*. *IEEE Trans. Syst. Sci. Cybern.* **4**<sup>3</sup>, 200–210. [DOI:10.1109/TSSC.1968.300114](#), <https://stat.duke.edu/~scs/Courses/STAT102/DecisionTheoryTutorial.pdf>.
- Pearl, J. (1988): *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, rev. 2nd pr. (Kaufmann, San Francisco). [DOI:10.1016/C2009-0-27609-4](#).
- Raiffa, H. (1970): *Decision Analysis: Introductory Lectures on Choices under Uncertainty*, 2nd pr. (Addison-Wesley, Reading, USA). First publ. 1968.
- Russell, S. J., Norvig, P. (2022): *Artificial Intelligence: A Modern Approach*, Fourth Global ed. (Pearson, Harlow, UK). First publ. 1995.
- Sox, H. C., Higgins, M. C., Owens, D. K. (2013): *Medical Decision Making*, 2nd ed. (Wiley, New York). [DOI:10.1002/9781118341544](#). First publ. 1988.