

How to avoid machine learning pitfalls: a guide for academic researchers

Michael A. Lones*

Abstract

This document gives a concise outline of some of the common mistakes that occur when using machine learning techniques, and what can be done to avoid them. It is intended primarily as a guide for research students, and focuses on issues that are of particular concern within academic research, such as the need to do rigorous comparisons and reach valid conclusions. It covers five stages of the machine learning process: what to do before model building, how to reliably build models, how to robustly evaluate models, how to compare models fairly, and how to report results.

1 Introduction

This guide aims to help newcomers avoid some of the mistakes that can occur when using machine learning (ML) within an academic research context. It's written by an academic, and focuses on lessons that were learnt whilst doing ML research in academia, and whilst supervising students doing ML research. It is primarily aimed at students and other researchers who are relatively new to the field of ML, and only assumes a basic knowledge of ML techniques. Unlike similar guides aimed at a more general ML audience, it reflects the scholarly concerns of academia: such as the need to rigorously evaluate and compare models in order to get work published. However, most of the lessons are applicable to the broader use of ML, and it could be used as an introductory guide to anyone getting started in this field. To make it more readable, the guidance is written informally, in a *Dos and Don'ts* style. It's not intended to be exhaustive, and references are provided for further reading. Since it doesn't cover issues specific to particular academic subjects, it's recommended that you also consult subject-specific guidance where available (e.g. for medicine [Luo et al., 2016, Stevens et al., 2020]). Feedback is welcome, and it is expected that this document will evolve over time. For this reason, if you cite it, please include the arXiv version number.

*School of Mathematical and Computer Sciences, Heriot-Watt University, Edinburgh, Scotland, UK,
Email: m.lones@hw.ac.uk, Web: <http://www.macs.hw.ac.uk/~ml355>.

Contents

1	Introduction	1
2	Before you start to build models	3
2.1	Do take the time to understand your data	3
2.2	Don't look at <i>all</i> your data	3
2.3	Do make sure you have enough data	3
2.4	Do talk to domain experts	4
2.5	Do survey the literature	4
2.6	Do think about how your model will be deployed	5
3	How to reliably build models	5
3.1	Don't allow test data to leak into the training process	5
3.2	Do try out a range of different models	6
3.3	Don't use inappropriate models	6
3.4	Do optimise your model's hyperparameters	6
3.5	Do be careful where you optimise hyperparameters and select features . .	7
4	How to robustly evaluate models	7
4.1	Do use an appropriate test set	7
4.2	Do use a validation set	8
4.3	Do evaluate a model multiple times	8
4.4	Do save some data to evaluate your final model instance	8
4.5	Don't use accuracy with imbalanced data sets	9
5	How to compare models fairly	9
5.1	Don't assume a bigger number means a better model	9
5.2	Do use statistical tests when comparing models	10
5.3	Do correct for multiple comparisons	10
5.4	Don't always believe results from community benchmarks	11
5.5	Do consider combinations of models	11
6	How to report your results	12
6.1	Do be transparent	12
6.2	Do report performance in multiple ways	12
6.3	Don't generalise beyond the data	13
6.4	Do be careful when reporting statistical significance	13
6.5	Do look at your models	13
7	Final thoughts	14
8	Acknowledgements	14

2 Before you start to build models

It's normal to want to rush into training and evaluating models, but it's important to take the time to think about the goals of a project, to fully understand the data that will be used to support these goals, to consider any limitations of the data that need to be addressed, and to understand what's already been done in your field. If you don't do these things, then you may end up with results that are hard to publish, or models that are not appropriate for their intended purpose.

2.1 Do take the time to understand your data

Eventually you will want to publish your work. This is a lot easier to do if your data is from a reliable source, has been collected using a reliable methodology, and is of good quality. For instance, if you are using data collected from an internet resource, make sure you know where it came from. Is it described in a paper? If so, take a look at the paper; make sure it was published somewhere reputable, and check whether the authors mention any limitations of the data. Do not assume that, because a data set has been used by a number of papers, it is of good quality — sometimes data is used just because it is easy to get hold of, and some widely used data sets are known to have significant limitations (see [Paullada et al., 2020] for a discussion of this). If you train your model using bad data, then you will most likely generate a bad model: a process known as **garbage in garbage out**. So, always begin by making sure your data makes sense. Do some **exploratory data analysis** (see Cox [2017] for suggestions). Look for missing or inconsistent records. It is much easier to do this now, before you train a model, rather than later, when you're trying to explain to reviewers why you used bad data.

2.2 Don't look at all your data

As you look at data, it is quite likely that you will spot patterns and make insights that guide your modelling. This is another good reason to look at data. However, it is important that you do not make untestable assumptions that will later feed into your model. The “untestable” bit is important here; it's fine to make assumptions, but these should only feed into the training of the model, not the testing. So, to ensure this is the case, you should avoid looking closely at any test data in the initial exploratory analysis stage. Otherwise you might, consciously or unconsciously, make assumptions that limit the generality of your model in an untestable way. This is a theme I will return to several times, since the leakage of information from the test set into the training process is a common reason why ML models fail to generalise. See [Don't allow test data to leak into the training process](#) for more on this.

2.3 Do make sure you have enough data

If you don't have enough data, then it may not be possible to train a model that generalises. Working out whether this is the case can be challenging, and may not be evident until you start building models: it all depends on the signal to noise ratio in the data set.

If the signal is strong, then you can get away with less data; if it's weak, then you need more data. If you can't get more data — and this is a common issue in many research fields — then you can make better use of existing data by using cross-validation (see [Do evaluate a model multiple times](#)). You can also use **data augmentation** techniques (e.g. see [\[Wong et al., 2016, Shorten and Khoshgoftaar, 2019\]](#)), and these can be quite effective for boosting small data sets. Data augmentation is also useful in situations where you have limited data in certain parts of your data set, e.g. in classification problems where you have less samples in some classes than others — a situation known as **class imbalance** (see [Haixiang et al. \[2017\]](#) for a review of methods for dealing with this; also see [Don't use accuracy with imbalanced data sets](#)). However, if you have limited data, then it's likely that you will also have to limit the complexity of the ML models you use, since models with many parameters, like deep neural networks, can easily overfit small data sets. Either way, it's important to identify this issue early on, and come up with a suitable (and defensible) strategy to mitigate it.

2.4 Do talk to domain experts

Domain experts can be very valuable. They can help you to understand which problems are useful to solve, they can help you choose the most appropriate feature set and ML model to use, and they can help you publish to the most appropriate audience. Failing to consider the opinion of domain experts can lead to projects which don't solve useful problems, or which solve useful problems in inappropriate ways. An example of the latter is using an opaque ML model to solve a problem where there is a strong need to understand how the model reaches an outcome, e.g. in making medical or financial decisions (see [\[Rudin, 2019\]](#)). At the beginning of a project, domain experts can help you to understand the data, and point you towards features that are likely to be predictive. At the end of a project, they can help you to publish in domain-specific journals, and hence reach an audience that is most likely to benefit from your research.

2.5 Do survey the literature

You're probably not the first person to throw ML at a particular problem domain, so it's important to understand what has and hasn't been done previously. Other people having worked on the same problem isn't a bad thing; academic progress is typically an iterative process, with each study providing information that can guide the next. It may be discouraging to find that someone has already explored your great idea, but they most likely left plenty of avenues of investigation still open, and their previous work can be used as justification for your work. To ignore previous studies is to potentially miss out on valuable information. For example, someone may have tried your proposed approach before and found fundamental reasons why it won't work (and therefore saved you a few years of frustration), or they may have partially solved the problem in a way that you can build on. So, it's important to do a literature review before you start work; leaving it too late may mean that you are left scrambling to explain why you are covering the same ground or not building on existing knowledge when you come to write a paper.

2.6 Do think about how your model will be deployed

Why do you want to build an ML model? This is an important question, and the answer should influence the process you use to develop your model. Many academic studies are just that — studies — and not really intended to produce models that will be used in the real world. This is fair enough, since the process of building and analysing models can itself give very useful insights into a problem. However, for many academic studies, the eventual goal is to produce an ML model that can be deployed in a real world situation. If this is the case, then it's worth thinking early on about how it is going to be deployed. For instance, if it's going to be deployed in a resource-limited environment, such as a sensor or a robot, this may place limitations on the complexity of the model. If there are time constraints, e.g. a classification of a signal is required within milliseconds, then this also needs to be taken into account when selecting a model. Another consideration is how the model is going to be tied into the broader software system within which it is deployed. This procedure is often far from simple (see [Sculley et al., 2015]). However, emerging approaches such as **ML Ops** aim to address some of the difficulties; see [Tamburri, 2020].

3 How to reliably build models

Building models is one of the more enjoyable parts of ML. With modern ML frameworks, it's easy to throw all manner of approaches at your data and see what sticks. However, this can lead to a disorganised mess of experiments that's hard to justify and hard to write up. So, it's important to approach model building in an organised manner, making sure you use data correctly, and putting adequate consideration into the choice of models.

3.1 Don't allow test data to leak into the training process

It's essential to have data that you can use to measure how well your model generalises. A common problem is allowing information about this data to leak into the configuration, training or selection of models. When this happens, the data no longer provides a reliable measure of generality, and this is a common reason why published ML models often fail to generalise to real world data. There are a number of ways that information can leak from a test set. Some of these seem quite innocuous. For instance, during data preparation, using information about the means and ranges of variables within the whole data set to carry out variable scaling — in order to prevent information leakage, this kind of thing should only be done with the training data. Other common examples of information leakage are carrying out feature selection before partitioning the data (see [Do be careful where you optimise hyperparameters and select features](#)), and using the same test data to evaluate the generality of multiple models (see [Do use a validation set](#) and [Don't always believe results from community benchmarks](#)). The best thing you can do to prevent these issues is to partition off a subset of your data right at the start of your project, and only use this independent test set once to measure the generality of a single model at the end of the project (see [Do save some data to evaluate your final](#)

model instance). See [Cawley and Talbot, 2010] and [Kaufman et al., 2012] for a broader discussion of this.

3.2 Do try out a range of different models

Generally speaking, there’s no such thing as a single best ML model. In fact, there’s a proof of this, in the form of the No Free Lunch theorem, which shows that no ML approach is any better than any other when considered over every possible problem [Wolpert, 2002]. So, your job is to find the ML model that works well for your particular problem. There may be some *a priori* knowledge of this, in the form of good quality research on closely related problems, but most of the time you’re operating in the dark. Fortunately, modern ML libraries in Python (e.g. scikit-learn [Varoquaux et al., 2015]), R (e.g. caret [Kuhn, 2015]), Julia (e.g. MLJ [Blaom et al., 2020]) etc. allow you to try out multiple models with only small changes to your code, so there’s no reason not to try out multiple models and find out for yourself which one works best. In the light of No Free Lunch, it’s important to avoid “not invented here syndrome”, i.e. only using models that have been invented at your own institution, since this may cause you to omit the best model for a particular problem.

3.3 Don’t use inappropriate models

By lowering the barrier to implementation, modern ML libraries also make it easy to apply inappropriate models to your data. Examples of this include applying models that expect categorical features to a data set comprised of numeric features, or attempting to apply a model that assumes no dependencies between variables to time series data. This is particularly something to consider in the light of publication, since reporting results from inappropriate models will give reviewers a bad impression of your work. Another example is using a model that is unnecessarily complex. For instance, a deep neural network is not a good choice if you have limited data, if domain knowledge suggests the underlying pattern is quite simple, or if the model needs to be interpretable. Finally, don’t use recency as a justification for choosing a model: old, established, models often work better than new ones.

3.4 Do optimise your model’s hyperparameters

Many models have **hyperparameters** — that is, numbers or settings that affect the configuration of the model. Examples include the kernel function used in an SVM, the number of trees in a random forest, and the architecture of a neural network. Many of these hyperparameters significantly effect the performance of the model, and there is generally no one-size-fits-all. That is, they need to be fitted to your particular data set in order to get the most out of the model. Whilst it may be tempting to fiddle around with hyperparameters until you find something that works, this is not likely to be an optimal approach. It’s much better to use some kind of **hyperparameter optimisation** strategy, and this is much easier to justify when you write it up. Basic strategies include random search and grid search, but these don’t scale well to large

numbers of hyperparameters or to models that are expensive to train, so it's worth using tools that search for optimal configurations in a more intelligent manner (surveyed in [Yang and Shami, 2020]). It is also possible to use **AutoML** techniques to optimise both the choice of model and its hyperparameters, in addition to other parts of the data mining pipeline — see He et al. [2021] for a review.

3.5 Do be careful where you optimise hyperparameters and select features

Another common stage of training a model is to carry out **feature selection** (surveyed by Cai et al. [2018]). However, when carrying out both hyperparameter optimisation and feature selection, it is important to treat them as part of model training, and not something more general that you do before model training. A particularly common error is to do feature selection on the whole data set before model training begins, but this will result in information leaking from the test set into the training process. So, if you optimise the hyperparameters or features used by a model, you should ideally use exactly the same data that you use to train the model. A common technique for doing this is **nested cross-validation** (also known as double cross-validation), which involves doing hyperparameter optimisation and feature selection as an extra loop inside the main cross-validation loop. See Cawley and Talbot [2010] for a broader discussion, and [Do evaluate a model multiple times](#) for more information about cross-validation.

4 How to robustly evaluate models

In order to contribute to progress in your field, you need to have valid results that you can draw reliable conclusions from. Unfortunately it's really easy to evaluate ML models unfairly, and, by doing so, muddy the waters of academic progress. So, think carefully about how you are going to use data in your experiments, how you are going to measure the true performance of your models, and how you are going to report this performance in a meaningful and informative way.

4.1 Do use an appropriate test set

First of all, always use a test set to measure the generality of an ML model. How well a model performs on the training set is almost meaningless, and a sufficiently complex model can entirely learn a training set yet capture no generalisable knowledge. It's also important to make sure the data in the test set is appropriate. That is, it should not overlap with the training set and it should be representative of the wider population. For example, consider a photographic data set of objects where the images in the training and test set were collected outdoors on a sunny day. The presence of the same weather conditions mean that the test set will not be independent, and by not capturing a broader variety of weather conditions, it will also not be representative. Similar situations can occur when a single piece of equipment is used to collect both the training and test data. If the model overlearns characteristics of the equipment, it will likely not generalise to

other pieces of equipment, and this will not be detectable by evaluating it on the test set.

4.2 Do use a validation set

It's not unusual to train multiple models in succession, using knowledge gained about each model's performance to guide the configuration of the next. When doing this, it's important not to use the test set within this process. Rather, a separate validation set should be used to measure performance. This contains a set of samples that are not directly used in training, but which are used to guide training. If you use the test set for this purpose, then the test set will become an implicit part of the training process, and will no longer be able to serve as an independent measure of generality, i.e. your models will progressively overfit the test set [Cawley and Talbot, 2010]. Another benefit of having a validation set is that you can do **early stopping**, where, during the training of a single model, the model is measured against the validation set at each iteration of the training process. Training is then stopped when the validation score starts to fall, since this indicates that the model is starting to overfit the training data.

4.3 Do evaluate a model multiple times

Many ML models are unstable. That is, if you train them multiple times, or if you make small changes to the training data, then their performance varies significantly. This means that a single evaluation of a model can be unreliable, and may either underestimate or overestimate the model's true potential. For this reason, it is common to carry out multiple evaluations. There are numerous ways of doing this, and most involve training the model multiple times using different subsets of the training data. **Cross-validation** (CV) is particularly popular, and comes in numerous varieties [Arlot et al., 2010]. Ten-fold CV, where training is repeated ten times, is arguably the standard, but you can add more rigour by using repeated CV, where the whole CV process is repeated multiple times with different partitionings of the data. If some of your data classes are small, it's important to do **stratification**, which ensures each class is adequately represented in each fold. It is common to report the mean and standard deviation of the multiple evaluations, but it is also advisable to keep a record of the individual scores in case you later use a statistical test to compare models (see [Do use statistical tests when comparing models](#)).

4.4 Do save some data to evaluate your final model instance

I've used the term *model* quite loosely, but there is an important distinction between evaluating the potential of a general model (e.g. how well a neural network can solve your problem), and the performance of a particular model instance (e.g. a specific neural network produced by one run of back-propagation). Cross-validation is good at the former, but it's less useful for the latter. Say, for instance, that you carried out ten-fold cross-validation. This would result in ten model instances. Say you then select the instance with the highest test fold score as the model which you will use in practice.

How do you report its performance? Well, you might think that its test fold score is a reliable measure of its performance, but it probably isn't. First, the amount of data in a single fold is relatively small. Second, the instance with the highest score could well be the one with the easiest test fold, so the evaluation data it contains may not be representative. Consequently, the only way of getting a reliable estimate of a model instance's generality may be to use another test set. So, if you have enough data, it's better to keep some aside and only use it once to provide an unbiased estimate of the final selected model instance.

4.5 Don't use accuracy with imbalanced data sets

Finally, be careful which metrics you use to evaluate your ML models. For instance, in the case of classification models, the most commonly used metric is accuracy, which is the proportion of samples in the data set that were correctly classified by the model. This works fine if your classes are balanced, i.e. if each class is represented by a similar number of samples within the data set. But many data sets are not balanced, and in this case accuracy can be a very misleading metric. Consider, for example, a data set in which 90% of the samples represent one class, and 10% of the samples represent another class. A binary classifier which always outputs the first class, regardless of its input, would have an accuracy of 90%, despite being completely useless. In this kind of situation, it would be preferable to use a metric such as Cohen's kappa coefficient (κ) or Matthews Correlation Coefficient (MCC), both of which are relatively insensitive to class size imbalance (also see [Do report performance in multiple ways](#)). For a broader review of methods for dealing with imbalanced data, see [Haixiang et al. \[2017\]](#).

5 How to compare models fairly

Comparing models is the basis of academic research, but it's surprisingly difficult to get it right. If you carry out a comparison unfairly, and publish it, then other researchers may subsequently be led astray. So, do make sure that you evaluate different models within the same context, do explore multiple perspectives, and do use make correct use of statistical tests.

5.1 Don't assume a bigger number means a better model

It's not uncommon for a paper to state something like "In previous research, accuracies of up to 94% were reported. Our model achieved 95%, and is therefore better." There are various reasons why a higher figure does not imply a better model. For instance, if the models were trained or evaluated on different partitions of the same data set, then small differences in performance may be due to this. If they used different data sets entirely, then this may account for even large differences in performance. Another reason for unfair comparisons is the failure to carry out the same amount of hyperparameter optimisation (see [Do optimise your model's hyperparameters](#)) when comparing models; for instance, if one model has default settings and the other has been optimised, then the

comparison won't be fair. For these reasons, and others, comparisons based on published figures should always be treated with caution. To really be sure of a fair comparison between two approaches, you should freshly implement all the models you're comparing, optimise each one to the same degree, carry out multiple evaluations (see [Do evaluate a model multiple times](#)), and then use statistical tests (see [Do use statistical tests when comparing models](#)) to determine whether the differences in performance are significant.

5.2 Do use statistical tests when comparing models

If you want to convince people that your model is better than someone else's, then a statistical test is a very useful tool. Broadly speaking, there are two categories of tests for comparing individual ML models. The first is used to compare individual model instances, e.g. two trained decision trees. For example, McNemar's test is a fairly common choice for comparing two classifiers, and works by comparing the classifiers' output labels for each sample in the test set (so do remember to record these). The second category of tests are used to compare two models more generally, e.g. whether a decision tree or a neural network is a better fit for the data. These require multiple evaluations of each model, which you can get by using cross-validation or repeated resampling (or, if your training algorithm is stochastic, multiple repeats using the same data). The test then compares the two resulting distributions. Student's T test is a common choice for this kind of comparison, but it's only reliable when the distributions are normally distributed, which is often not the case. A safer bet is Mann-Whitney's U test, since this does not assume that the distributions are normal. For more information, see [[Raschka, 2020](#)] and [[Carrasco et al., 2020](#)]. Also see [Do correct for multiple comparisons](#) and [Do be careful when reporting statistical significance](#).

5.3 Do correct for multiple comparisons

Things get a bit more complicated when you want to use statistical tests to compare more than two models, since doing multiple pairwise tests is a bit like using the test set multiple times — it can lead to overly-optimistic interpretations of significance. Basically, each time you carry out a comparison between two models using a statistical test, there's a probability that it will discover significant differences where there aren't any. This is represented by the confidence level of the test, usually set at 95%: meaning that 1 in 20 times it will give you a false positive. For a single comparison, this may be a level of uncertainty you can live with. However, it accumulates. That is, if you do 20 pairwise tests with a confidence level of 95%, one of them is likely to give you the wrong answer. This is known as the **multiplicity effect**, and is an example of a broader issue in data science known as **data dredging** or **p-hacking** — see [[Head et al., 2015](#)]. To address this problem, you can apply a correction for multiple tests. The most common approach is the Bonferroni correction, a very simple method that lowers the significance threshold based on the number of tests that are being carried out — see [[Salzberg, 1997](#)] for a gentle introduction. However, there are numerous other approaches, and there is also some debate about when and where these corrections should be applied; for an

accessible overview, see [\[Streiner, 2015\]](#).

5.4 Don't always believe results from community benchmarks

In certain problem domains, it has become commonplace to use benchmark data sets to evaluate new ML models. The idea is that, because everyone is using the same data to train and test their models, then comparisons will be more transparent. Unfortunately this approach has some major drawbacks. First, if access to the test set is unrestricted, then you can't assume that people haven't used it as part of the training process. This is known as "developing to the test set", and leads to results that are heavily over-optimistic. A more subtle problem is that, even if everyone who uses the data only uses the test set once, collectively the test set is being used many times by the community. In effect, by comparing lots of models on the same test set, it becomes increasingly likely that the best model just happens to over-fit the test set, and doesn't necessarily generalise any better than the other models (see [Do correct for multiple comparisons](#)). For these, and other reasons, you should be careful how much you read into results from a benchmark data set, and don't assume that a small increase in performance is significant. See [\[Paullada et al., 2020\]](#) for a wider discussion of issues surrounding the use of shared datasets. Also see [Do report performance in multiple ways](#).

5.5 Do consider combinations of models

Whilst this section focuses on comparing models, it's good to be aware that ML is not always about choosing between different models. Often it makes sense to use combinations of models. Different ML models explore different trade-offs; by combining them, you can sometimes compensate for the weaknesses of one model by using the strengths of another model, and vice versa. Such composite models are known as **ensembles**, and the process of generating them is known as **ensemble learning**. There are lots of ensemble learning approaches — see [\[Dong et al., 2020\]](#) for a review. However, they can be roughly divided into those that form ensembles out of the same base model type, e.g. an ensemble of decision trees, and those that combine different kinds of ML models, e.g. a combination of a decision tree, an SVM, and a deep neural network. The first category includes many classic approaches, such as bagging and boosting. Ensembles can either be formed from existing trained models, or the base models can be trained as part of the process, typically with the aim of creating a diverse selection of models that make mistakes on different parts of the data space. A general consideration in ensemble learning is how to combine the different base models; approaches to this vary from very simple methods such as voting, to more complex approaches that use another ML model to aggregate the outputs of the base models. This latter approach is often referred to as **stacking** or **stacked generalisation**.

6 How to report your results

The aim of academic research is not self-aggrandisement, but rather an opportunity to contribute to knowledge. In order to effectively contribute to knowledge, you need to provide a complete picture of your work, covering both what worked and what didn't. ML is often about trade-offs — it's very rare that one model is better than another in every way that matters — and you should try to reflect this with a nuanced and considered approach to reporting results and conclusions.

6.1 Do be transparent

First of all, always try to be transparent about what you've done, and what you've discovered, since this will make it easier for other people to build upon your work. In particular, it's good practice to share your models in an accessible way. For instance, if you used a script to implement all your experiments, then share the script when you publish the results. This means that other people can easily repeat your experiments, which adds confidence to your work. It also makes it a lot easier for people to compare models, since they no longer have to reimplement everything from scratch in order to ensure a fair comparison. Knowing that you will be sharing your work also encourages you to be more careful, document your experiments well, and write clean code, which benefits you as much as anyone else. It's also worth noting that issues surrounding reproducibility are gaining prominence in the ML community, so in the future you may not be able to publish work unless your workflow is adequately documented and shared — for example, see [Pineau et al., 2020].

6.2 Do report performance in multiple ways

One way to achieve better rigour when evaluating and comparing models is to use multiple data sets. This helps to overcome any deficiencies associated with individual data sets (see [Don't always believe results from community benchmarks](#)) and allows you to present a more complete picture of your model's performance. It's also good practice to report multiple metrics for each data set, since different metrics can present different perspectives on the results, and increase the transparency of your work. For example, if you use accuracy, it's also a good idea to include metrics that are less sensitive to class imbalances (see [Don't use accuracy with imbalanced data sets](#)). If you use a partial metric like precision, recall, sensitivity or specificity, also include a metric that gives a more complete picture of your model's error rates. And make sure it's clear which metrics you are using. For instance, if you report F-scores, be clear whether this is F1, or some other balance between precision and recall. If you report AUC, indicate whether this is the area under the ROC curve or the PR curve. For a broader discussion, see [Blagec et al., 2020].

6.3 Don't generalise beyond the data

It's important not to present invalid conclusions, since this can lead other researchers astray. A common mistake is to make general statements that are not supported by the data used to train and evaluate models. For instance, if your model does really well on one data set, this does not mean that it will do well on other data sets. Whilst you can get more robust insights by using multiple data sets (see [Do report performance in multiple ways](#)), there will always be a limit to what you can infer from any experimental study. There are numerous reasons for this (see [\[Paullada et al., 2020\]](#)), many of which are to do with how datasets are curated. One common issue is bias, or **sampling error**: that the data is not sufficiently representative of the real world. Another is overlap: multiple data sets may not be independent, and may have similar biases. There's also the issue of quality: and this is a particular issue in deep learning datasets, where the need for quantity of data limits the amount of quality checking that can be done. So, in short, don't overplay your findings, and be aware of their limitations.

6.4 Do be careful when reporting statistical significance

I've already discussed statistical tests (see [Do use statistical tests when comparing models](#)), and how they can be used to determine differences between ML models. However, statistical tests are not perfect. Some are conservative, and tend to under-estimate significance; others are liberal, and tend to over-estimate significance. This means that a positive test doesn't always indicate that something is significant, and a negative test doesn't necessarily mean that something isn't significant. Then there's the issue of using a threshold to determine significance; for instance, a 95% confidence threshold (i.e. when the $p\text{-value} < 0.05$) means that 1 in 20 times a difference flagged as significant won't be significant. In fact, statisticians are increasingly arguing that it is better not to use thresholds, and instead just report p -values and leave it to the reader to interpret these. Beyond statistical significance, another thing to consider is whether the difference between two models is actually important. If you have enough samples, you can always find significant differences, even when the actual difference in performance is miniscule. To give a better indication of whether something is important, you can measure **effect size**. There are a range of approaches used for this: Cohen's d statistic is probably the most common, but more robust approaches, such as Kolmogorov-Smirnov, are preferable. For more on this, see [\[Betensky, 2019\]](#).

6.5 Do look at your models

Trained models contain a lot of useful information. Unfortunately many authors just report the performance metrics of a trained model, without giving any insight into what it actually learnt. Remember that the aim of research is not to get a slightly higher accuracy than everyone else. Rather, it's to generate knowledge and understanding and share this with the research community. If you can do this, then you're much more likely to get a decent publication out of your work. So, do look inside your models and do try to understand how they reach a decision. For relatively simple models like decision

trees, it can also be beneficial to provide visualisations of your models, and most libraries have functions that will do this for you. For complex models, like deep neural networks, consider using **explainable AI** (XAI) techniques to extract knowledge (surveyed in [Li et al. \[2020\]](#)); they're unlikely to tell you exactly what the model is doing, but they may give you some useful insights.

7 Final thoughts

This document doesn't tell you everything you need to know, the lessons sometimes have no firm conclusions, and some of the things I've told you might be wrong, or at least debateable. This, I'm afraid, is the nature of research. The theory of how to do ML almost always lags behind the practice, academics will always disagree about the best ways of doing things, and what we think is correct today may not be correct tomorrow. Therefore, you have to approach ML in much the same way you would any other aspect of research: with an open mind, a willingness to keep up with recent developments, and the humility to accept you don't know everything.

8 Acknowledgements

Thanks to everyone who gave me feedback on the draft manuscript.

References

- S. Arlot, A. Celisse, et al. A survey of cross-validation procedures for model selection. *Statistics surveys*, 4:40–79, 2010. URL <https://doi.org/10.1214/09-SS054>.
- R. A. Betensky. The p-value requires context, not a threshold. *The American Statistician*, 73(sup1):115–117, 2019. URL <https://www.tandfonline.com/doi/full/10.1080/00031305.2018.1529624>.
- K. Blagec, G. Dorffner, M. Moradi, and M. Samwald. A critical analysis of metrics used for measuring progress in artificial intelligence, 2020. URL <https://arxiv.org/abs/2008.02577>.
- A. D. Blaom, F. Kiraly, T. Lienart, Y. Simillides, D. Arenas, and S. J. Vollmer. Mlj: A julia package for composable machine learning. *Journal of Open Source Software*, 5(55):2704, 2020. URL <https://doi.org/10.21105/joss.02704>.
- J. Cai, J. Luo, S. Wang, and S. Yang. Feature selection in machine learning: A new perspective. *Neurocomputing*, 300:70–79, 2018. URL <https://doi.org/10.1016/j.neucom.2017.11.077>.
- J. Carrasco, S. García, M. Rueda, S. Das, and F. Herrera. Recent trends in the use of statistical tests for comparing swarm and evolutionary computing algorithms: Practi-

- cal guidelines and a critical review. *Swarm and Evolutionary Computation*, 54:100665, 2020. URL <https://doi.org/10.1016/j.swevo.2020.100665>.
- G. C. Cawley and N. L. Talbot. On over-fitting in model selection and subsequent selection bias in performance evaluation. *The Journal of Machine Learning Research*, 11:2079–2107, 2010. URL <https://www.jmlr.org/papers/volume11/cawley10a/cawley10a.pdf>.
- V. Cox. Exploratory data analysis. In *Translating Statistics to Make Decisions*, pages 47–74. Springer, 2017.
- X. Dong, Z. Yu, W. Cao, Y. Shi, and Q. Ma. A survey on ensemble learning. *Frontiers of Computer Science*, 14(2):241–258, 2020. URL <https://doi.org/10.1007/s11704-019-8208-z>.
- G. Haixiang, L. Yijing, J. Shang, G. Mingyun, H. Yuanyue, and G. Bing. Learning from class-imbalanced data: Review of methods and applications. *Expert Systems with Applications*, 73:220–239, 2017. URL <https://doi.org/10.1016/j.eswa.2016.12.035>.
- X. He, K. Zhao, and X. Chu. Automl: A survey of the state-of-the-art. *Knowledge-Based Systems*, 212:106622, 2021. URL <https://arxiv.org/abs/1908.00709>.
- M. L. Head, L. Holman, R. Lanfear, A. T. Kahn, and M. D. Jennions. The extent and consequences of p-hacking in science. *PLoS Biol*, 13(3):e1002106, 2015. URL <https://doi.org/10.1371/journal.pbio.1002106>.
- S. Kaufman, S. Rosset, C. Perlich, and O. Stitelman. Leakage in data mining: Formulation, detection, and avoidance. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 6(4):1–21, 2012. URL <https://doi.org/10.1145/2382577.2382579>.
- M. Kuhn. A short introduction to the caret package. *R Found Stat Comput*, 1, 2015. URL <https://cran.r-project.org/web/packages/caret/vignettes/caret.html>.
- X.-H. Li, C. C. Cao, Y. Shi, W. Bai, H. Gao, L. Qiu, C. Wang, Y. Gao, S. Zhang, X. Xue, et al. A survey of data-driven and knowledge-aware explainable ai. *IEEE Transactions on Knowledge and Data Engineering*, 2020. URL <https://doi.org/10.1109/TKDE.2020.2983930>.
- W. Luo, D. Phung, T. Tran, S. Gupta, S. Rana, C. Karmakar, A. Shilton, J. Yearwood, N. Dimitrova, T. B. Ho, et al. Guidelines for developing and reporting machine learning predictive models in biomedical research: a multidisciplinary view. *Journal of medical Internet research*, 18(12):e323, 2016. URL <https://doi.org/10.2196/jmir.5870>.
- A. Paullada, I. D. Raji, E. M. Bender, E. Denton, and A. Hanna. Data and its (dis)contents: A survey of dataset development and use in machine learning research, 2020. URL <https://arxiv.org/abs/2012.05345>.

- J. Pineau, P. Vincent-Lamarre, K. Sinha, V. Larivière, A. Beygelzimer, F. d’Alché Buc, E. Fox, and H. Larochelle. Improving reproducibility in machine learning research (a report from the neurips 2019 reproducibility program), 2020. URL <https://arxiv.org/abs/2003.12206>.
- S. Raschka. Model evaluation, model selection, and algorithm selection in machine learning, 2020. URL <https://arxiv.org/abs/1811.12808>.
- C. Rudin. Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, 1(5):206–215, 2019. URL <https://arxiv.org/abs/1811.10154>.
- S. L. Salzberg. On comparing classifiers: Pitfalls to avoid and a recommended approach. *Data mining and knowledge discovery*, 1(3):317–328, 1997. URL <https://doi.org/10.1023/A:1009752403260>.
- D. Sculley, G. Holt, D. Golovin, E. Davydov, T. Phillips, D. Ebner, V. Chaudhary, M. Young, J.-F. Crespo, and D. Dennison. Hidden technical debt in machine learning systems. *Advances in neural information processing systems*, 28:2503–2511, 2015. URL <https://papers.nips.cc/paper/2015/file/86df7dcfd896fcdf2674f757a2463eba-Paper.pdf>.
- C. Shorten and T. M. Khoshgoftaar. A survey on image data augmentation for deep learning. *Journal of Big Data*, 6(1):1–48, 2019. URL <https://doi.org/10.1186/s40537-019-0197-0>.
- L. M. Stevens, B. J. Mortazavi, R. C. Deo, L. Curtis, and D. P. Kao. Recommendations for reporting machine learning analyses in clinical research. *Circulation: Cardiovascular Quality and Outcomes*, 13(10):e006556, 2020. URL <https://doi.org/10.1161/CIRCOUTCOMES.120.006556>.
- D. L. Streiner. Best (but oft-forgotten) practices: the multiple problems of multiplicity—whether and how to correct for many statistical tests. *The American journal of clinical nutrition*, 102(4):721–728, 2015. URL <https://doi.org/10.3945/ajcn.115.113548>.
- D. A. Tamburri. Sustainable MLOps: Trends and challenges. In *2020 22nd International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*, pages 17–23. IEEE, 2020. URL <https://doi.org/10.1109/SYNASC51798.2020.00015>.
- G. Varoquaux, L. Buitinck, G. Louppe, O. Grisel, F. Pedregosa, and A. Mueller. Scikit-learn: Machine learning without learning the machinery. *GetMobile: Mobile Computing and Communications*, 19(1):29–33, 2015. URL <https://doi.org/10.1145/2786984.2786995>.

- D. H. Wolpert. The supervised learning no-free-lunch theorems. *Soft computing and industry*, pages 25–42, 2002. URL https://doi.org/10.1007/978-1-4471-0123-9_3.
- S. C. Wong, A. Gatt, V. Stamatescu, and M. D. McDonnell. Understanding data augmentation for classification: when to warp? In *2016 international conference on digital image computing: techniques and applications (DICTA)*, pages 1–6. IEEE, 2016. URL <https://arxiv.org/abs/1609.08764>.
- L. Yang and A. Shami. On hyperparameter optimization of machine learning algorithms: Theory and practice. *Neurocomputing*, 415:295–316, 2020. URL <https://doi.org/10.1016/j.neucom.2020.07.061>.