Approaching (Almost) Any Machine Learning Problem

An average data scientist deals with loads of data daily. Some say over 60-70% time is spent in data cleaning, munging and bringing data to a suitable format such that machine learning models can be applied on that data. This post focuses on the second part, i.e., applying machine learning models, including the preprocessing steps. The pipelines discussed in this post come as a result of over a hundred machine learning competitions that I’ve taken part in. It must be noted that the discussion here is very general but very useful and there can also be very complicated methods which exist and are practised by professionals.

We will be using python!

Data

Before applying the machine learning models, the data must be converted to a tabular form. This whole process is the most time consuming and difficult process and is depicted in the figure below.

![Data Conversion Diagram]

The machine learning models are then applied to the tabular data. Tabular
data is most common way of representing data in machine learning or data mining. We have a data table, rows with different samples of the data or X and labels, y. The labels can be single column or multi-column, depending on the type of problem. We will denote data by X and labels by y.

Types of labels

The labels define the problem and can be of different types, such as:

- Single column, binary values (classification problem, one sample belongs to one class only and there are only two classes)
- Single column, real values (regression problem, prediction of only one value)
- Multiple column, binary values (classification problem, one sample belongs to one class, but there are more than two classes)
- Multiple column, real values (regression problem, prediction of multiple values)
- And multilabel (classification problem, one sample can belong to several classes)

Evaluation Metrics

For any kind of machine learning problem, we must know how we are going to evaluate our results, or what the evaluation metric or objective is. For example in case of a skewed binary classification problem we generally choose area under the receiver operating characteristic curve (ROC AUC or simply AUC). In case of multi-label or multi-class classification problems, we generally
choose categorical cross-entropy or multiclass log loss and mean squared error in case of regression problems.

I won’t go into details of the different evaluation metrics as we can have many different types, depending on the problem.

**The Libraries**

To start with the machine learning libraries, install the basic and most important ones first, for example, numpy and scipy.

- To see and do operations on data: pandas (http://pandas.pydata.org/)
- For all kinds of machine learning models: scikit-learn (http://scikit-learn.org/stable/)
- The best gradient boosting library: xgboost (https://github.com/dmlc/xgboost)
- For neural networks: keras (http://keras.io/)
- For plotting data: matplotlib (http://matplotlib.org/)
- To monitor progress: tqdm (https://pypi.python.org/pypi/tqdm)

I don’t use Anaconda (https://www.continuum.io/downloads). It’s easy and does everything for you, but I want more freedom. The choice is yours. :)

**The Machine Learning Framework**
In 2015, I came up with a framework for automatic machine learning which is still under development and will be released soon. For this post, the same framework will be the basis. The framework is shown in the figure below:

![Framework Diagram](image)


In the framework shown above, the pink lines represent the most common paths followed. After we have extracted and reduced the data to a tabular format, we can go ahead with building machine learning models.

The very first step is identification of the problem. This can be done by looking at the labels. One must know if the problem is a binary classification, a multi-class or multi-label classification or a regression problem. After we have
identified the problem, we split the data into two different parts, a training set and a validation set as depicted in the figure below.

The splitting of data into training and validation sets “must” be done according to labels. In case of any kind of classification problem, use stratified splitting. In python, you can do this using scikit-learn very easily.

```python
from sklearn.cross_validation import StratifiedKFold
eval_size = 0.10
kf = StratifiedKFold(y, round(1. / eval_size))
train_indices, valid_indices = next(iter(kf))
X_train, y_train = X[train_indices], y[train_indices]
X_valid, y_valid = X[valid_indices], y[valid_indices]
```

In case of regression task, a simple K-Fold splitting should suffice. There are, however, some complex methods which tend to keep the distribution of labels same for both training and validation set and this is left as an exercise for the reader.

```python
from sklearn.cross_validation import KFold
eval_size = 0.10
kf = KFold(len(y), round(1. / eval_size))
train_indices, valid_indices = next(iter(kf))
X_train, y_train = X[train_indices], y[train_indices]
X_valid, y_valid = X[valid_indices], y[valid_indices]
```
I have chosen the eval_size or the size of the validation set as 10% of the full data in the examples above, but one can choose this value according to the size of the data they have.

After the splitting of the data is done, leave this data out and don’t touch it. Any operations that are applied on training set must be saved and then applied to the validation set. Validation set, in any case, should not be joined with the training set. Doing so will result in very good evaluation scores and make the user happy but instead he/she will be building a useless model with very high overfitting.

Next step is identification of different variables in the data. There are usually three types of variables we deal with. Namely, numerical variables, categorical variables and variables with text inside them. Let’s take example of the popular Titanic dataset (https://www.kaggle.com/c/titanic/data).

<table>
<thead>
<tr>
<th>VARIABLE DESCRIPTIONS:</th>
</tr>
</thead>
<tbody>
<tr>
<td>survival</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>pclass</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>name</td>
</tr>
<tr>
<td>sex</td>
</tr>
<tr>
<td>age</td>
</tr>
<tr>
<td>sibsp</td>
</tr>
<tr>
<td>parch</td>
</tr>
<tr>
<td>ticket</td>
</tr>
<tr>
<td>fare</td>
</tr>
<tr>
<td>cabin</td>
</tr>
<tr>
<td>embarked</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Here, survival is the label. We have already separated labels from the training data in the previous step. Then, we have pclass, sex, embarked. These variables
have different levels and thus they are categorical variables. Variables like age, sibsp, parch, etc are numerical variables. Name is a variable with text data but I don’t think it’s a useful variable to predict survival.

Separate out the numerical variables first. These variables don’t need any kind of processing and thus we can start applying normalization and machine learning models to these variables.

There are two ways in which we can handle categorical data:

- Convert the categorical data to labels

```python
from sklearn.preprocessing import LabelEncoder

lbl_enc = LabelEncoder()
lbl_enc.fit(xtrain['categorical_features'])
xtrain_cat = lbl_enc.transform(xtrain['categorical_features'])
```

- Convert the labels to binary variables (one-hot encoding)

```python
from sklearn.preprocessing import OneHotEncoder

ohe = OneHotEncoder()
ohe.fit(xtrain['categorical_features'])
xtrain_cat = ohe.transform(xtrain['categorical_features'])
```

Please remember to convert categories to numbers first using LabelEncoder before applying OneHotEncoder on it.

Since, the Titanic data doesn’t have good example of text variables, let’s formulate a general rule on handling text variables. We can combine all the text variables into one and then use some algorithms which work on text data and convert it to numbers.
The text variables can be joined as follows:

```python
text_data = list(X_train.apply(lambda x: '%s %s' % (x['column_1'], x['column_2']), axis=1))
```

We can then use CountVectorizer or TfidfVectorizer on it:

```python
from sklearn.feature_extraction.text import CountVectorizer
cvv = CountVectorizer()
text_data_train = cvv.fit_transform(text_data_train)
text_data_valid = cvv.fit_transform(text_data_valid)
```

or,

```python
from sklearn.feature_extraction.text import TfidfVectorizer
tfv = TfidfVectorizer()
text_data_train = tfv.fit_transform(text_data_train)
text_data_valid = tfv.fit_transform(text_data_valid)
```

The TfidfVectorizer performs better than the counts most of the time and I have seen that the following parameters for TfidfVectorizer work almost all the time.

```python
from sklearn.feature_extraction.text import TfidfVectorizer
tfv = TfidfVectorizer(min_df=3, max_features=None,
                      strip_accents='unicode', analyzer='word',
                      token_pattern=r'\w{1,}', ngram_range=(1, 2),
                      use_idf=1, smooth_idf=1, sublinear_tf=1,
                      stop_words = 'english')
```

If you are applying these vectorizers only on the training set, make sure to dump it to hard drive so that you can use it later on the validation set.

```python
import cPickle
cPickle.dump(vectorizer, open('vectorizer.pkl', 'wb'), -1)
```

Next, we come to the stacker module. Stacker module is not a model stacker but a feature stacker. The different features after the processing steps
described above can be combined using the stacker module.

![Stacker Diagram](image)

You can horizontally stack all the features before putting them through further processing by using numpy hstack or sparse hstack depending on whether you have dense or sparse features.

```python
import numpy as np
from scipy import sparse

# in case of dense data
X = np.hstack((x1, x2, ...))

# in case data is sparse
X = sparse.hstack((x1, x2, ...))
```

And can also be achieved by FeatureUnion module in case there are other processing steps such as pca or feature selection (we will visit decomposition and feature selection later in this post).

```python
from sklearn.pipeline import FeatureUnion
from sklearn.decomposition import PCA
from sklearn.feature_selection import SelectKBest

pca = PCA(n_components=10)
skb = SelectKBest(k=1)
combined_features = FeatureUnion(["pca", pca], ["skb", skb])
```

Once, we have stacked the features together, we can start applying machine learning models. At this stage only models you should go for should be ensemble tree based models. These models include:

- RandomForestClassifier
• RandomForestRegressor
• ExtraTreesClassifier
• ExtraTreesRegressor
• XGBClassifier
• XGBRegressor

We cannot apply linear models to the above features since they are not normalized. To use linear models, one can use Normalizer or StandardScaler from scikit-learn.

These normalization methods work only on dense features and don’t give very good results if applied on sparse features. Yes, one can apply StandardScaler on sparse matrices without using the mean (parameter: with_mean=False).

If the above steps give a “good” model, we can go for optimization of hyperparameters and in case it doesn’t we can go for the following steps and improve our model.

The next steps include decomposition methods:

For the sake of simplicity, we will leave out LDA and QDA transformations. For high dimensional data, generally PCA is used decompose the data. For images start with 10-15 components and increase this number as long as the quality of result improves substantially. For other type of data, we select 50-60
components initially (we tend to avoid PCA as long as we can deal with the numerical data as it is).

```
from sklearn.decomposition import PCA
pca = PCA(n_components=12)
pca.fit(xtrain)
xtrain = pca.transform(xtrain)
```

For text data, after conversion of text to sparse matrix, go for Singular Value Decomposition (SVD). A variation of SVD called TruncatedSVD can be found in scikit-learn.

```
from sklearn.decomposition import TruncatedSVD
svd = TruncatedSVD(n_components=120)
svd.fit(xtrain)
xtrain = svd.transform(xtrain)
```

The number of SVD components that generally work for TF-IDF or counts are between 120-200. Any number above this might improve the performance but not substantially and comes at the cost of computing power.

After evaluating further performance of the models, we move to scaling of the datasets, so that we can evaluate linear models too. The normalized or scaled features can then be sent to the machine learning models or feature selection modules.
There are multiple ways in which feature selection can be achieved. One of the most common way is greedy feature selection (forward or backward). In greedy feature selection we choose one feature, train a model and evaluate the performance of the model on a fixed evaluation metric. We keep adding and removing features one-by-one and record performance of the model at every step. We then select the features which have the best evaluation score. One implementation of greedy feature selection with AUC as evaluation metric can be found here: [https://github.com/abhishekkrrthakur/greedyFeatureSelection](https://github.com/abhishekkrrthakur/greedyFeatureSelection). It must be noted that this implementation is not perfect and must be changed/modified according to the requirements.

Other faster methods of feature selection include selecting best features from a model. We can either look at coefficients of a logit model or we can train a random forest to select best features and then use them later with other machine learning models.

```python
from sklearn.ensemble import RandomForestClassifier
clf = RandomForestClassifier(n_estimators=100, n_jobs=-1)
clf.fit(X, y)
X_selected = clf.transform(X)
```

Remember to keep low number of estimators and minimal optimization of hyper parameters so that you don’t overfit.

The feature selection can also be achieved using Gradient Boosting Machines. It is good if we use xgboost instead of the implementation of GBM in scikit-learn since xgboost is much faster and more scalable.

```python
import xgboost as xgb
params = {}
model = xgb.train(params, dtrain, num_boost_round=100)
sorted(model.get_fscore().items(), key=lambda t: -t[1])
```
We can also do feature selection of sparse datasets using RandomForestClassifier / RandomForestRegressor and xgboost.

Another popular method for feature selection from positive sparse datasets is chi-2 based feature selection and we also have that implemented in scikit-learn.

```python
from sklearn.feature_selection import SelectKBest
from sklearn.feature_selection import chi2

skb = SelectKBest(chi2, k=20)
skb.fit_transform(X, y)
```

Here, we use chi2 in conjunction with SelectKBest to select 20 features from the data. This also becomes a hyperparameter we want to optimize to improve the result of our machine learning models.

Don’t forget to dump any kinds of transformers you use at all the steps. You will need them to evaluate performance on the validation set.

Next (or intermediate) major step is model selection + hyperparameter optimization.
We generally use the following algorithms in the process of selecting a machine learning model:

- **Classification**:
  - Random Forest
  - GBM
  - Logistic Regression
  - Naive Bayes
  - Support Vector Machines
  - k-Nearest Neighbors

- **Regression**
  - Random Forest
  - GBM
  - Linear Regression
  - Ridge
  - Lasso
  - SVR

Which parameters should I optimize? How do I choose parameters closest to the best ones? These are a couple of questions people come up with most of the time. One cannot get answers to these questions without experience with different models + parameters on a large number of datasets. Also people who have experience are not willing to share their secrets. Luckily, I have quite a bit of experience too and I’m willing to give away some of the stuff.
Let’s break down the hyperparameters, model wise:

<table>
<thead>
<tr>
<th>Model</th>
<th>Parameters to optimize</th>
<th>Good range of values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linear Regression</td>
<td>• fit_intercept • normalize</td>
<td>• True / False</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• True / False</td>
</tr>
<tr>
<td>Ridge</td>
<td>• alpha • Fit_intercept • Normalize</td>
<td>• 0.01, 0.1, 1.0, 10, 100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• True/False</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• True/False</td>
</tr>
<tr>
<td>k-neighbors</td>
<td>• N_neighbors • p</td>
<td>• 2, 4, 8, 16 ....</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2, 3</td>
</tr>
<tr>
<td>SVM</td>
<td>• C • Gamma • class_weight</td>
<td>• 0.001, 0.01...10...100...1000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 'Auto', RS*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 'Balanced', None</td>
</tr>
<tr>
<td>Logistic Regression</td>
<td>• Penalty • C</td>
<td>• L1 or l2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0.001, 0.01...10...100</td>
</tr>
<tr>
<td>Naive Bayes (all variations)</td>
<td>NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>Lasso</td>
<td>• Alpha • Normalize</td>
<td>• 0.1, 1.0, 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• True/False</td>
</tr>
<tr>
<td>Random Forest</td>
<td>• N_estimators • Max_depth • Min_samples_split • Min_samples_leaf • Max_features</td>
<td>• 120, 300, 500, 800, 1200</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 5, 8, 15, 25, 30, None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1, 2, 5, 10, 15, 100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1, 2, 5, 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Log2, sqrt, None</td>
</tr>
<tr>
<td>Xgboost</td>
<td>• Eta • Gamma • Max_depth • Min_child_weight • Subsample •Colsample_bytree • Lambda • alpha</td>
<td>• 0.01,0.015, 0.025, 0.05, 0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0.05-0.1,0.3,0.5,0.7,0.9,1.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3, 5, 7, 9, 12, 15, 17, 25</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1, 3, 5, 7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0.6, 0.7, 0.8, 0.9, 1.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0.6, 0.7, 0.8, 0.9, 1.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0.01-0.1, 1.0, RS*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0, 0.1, 0.5, 1.0 RS*</td>
</tr>
</tbody>
</table>

RS* = Cannot say about proper values, go for Random Search in these hyperparameters.

In my opinion, and strictly my opinion, the above models will out-perform any others and we don’t need to evaluate any other models.
Once again, remember to save the transformers:

And apply them on validation set separately:

The above rules and the framework has performed very well in most of the datasets I have dealt with. Of course, it has also failed for very complicated tasks. Nothing is perfect and we keep on improving on what we learn. Just like in machine learning.

Get in touch with me with any doubts: abhishek4 [at] gmail [dot] com
How to automatically identify whether a variable is ordinal, nominal or interval?

Abhishek Thakur
Senior Data Scientist @ Searchmetrics Inc.

I will soon publish an advanced version which should answer your question and several others about feature engineering.

Arnab Biswas
Software Engineer at Cisco Systems

Two questions:

1. "Please remember to convert categories to numbers first using LabelEncoder before applying OneHotEncoder on it" - As per my understanding, if I have ordinal features, I will use LabelEncoder. For nominal features, I will use OneHotEncoder. For nominal features, do I need apply LabelEncoder first and then OneHotEncoder. If yes, could you please explain the reason?

2. One popular way to apply "OneHotEncoder" is to use "get_dummies". How is it different from the recommended approach above (code snip from your blog).

Thanks a lot!