EE-613: Machine Learning for Engineers

Feature extraction and selection
(and a bit of PAC)

François Fleuret

Dec 16th, 2015

Introduction
Dimension reduction

In many situation it makes sense to reduce the dimension of the original feature space. The objective is to:

- Reduce over-fitting
- Reduce the computational cost
- Facilitate the understanding of causal relations
- Facilitate the visualization of data

It can be combined with other procedures (supervised or not).
There are two main strategies to achieve dimension reduction:

- **Feature selection** finds a projection spanned by a subset of coordinates of the original space.

- **Feature extraction** (aka “feature learning”) builds a mapping from the original space into a space of lower dimension.

Feature selection is adequate if a subset of feature carries (all) the discriminating information.
Introduction
Feature selection vs. feature extraction

Feature extraction is required if none of the original feature carries the discriminating information, but it can be captured with a few quantities.

Feature selection
Introduction
Feature selection

The dimension reduction is achieved by selecting a subset of features, without re-combining them through a mapping.

In practice, if $X$ is our signal, r.v. on $\mathbb{R}^D$, given a target dimension $d$, we are looking for a list of coordinates

$$\nu(1), \ldots, \nu(d)$$

such that

$$X' = (X_{\nu(1)}, \ldots, X_{\nu(d)})$$

carries as much information as possible.

It is a simple way to achieve sparsity.

Some classes of predictors naturally achieve feature selection during training, for instance decision trees and Boosting.

Contrary to classical linear models (perceptron or SVM) or neural networks, the proportion of features they use is specified during training, and usually very small.
Introduction
Forward vs. backward selection

As usual in machine-learning, feature selection is defined by a criterion to optimize, and an optimization procedure.

The most common optimization schemes are:

- **Forward selection**: Features are added one after another, to increase the target score optimally at every iteration.
- **Backward selection**: Starting from all the feature, they are removed one at a time, to reduce the score the least.

Such a greedy optimization is not optimal, but usually tractable.

Introduction
Supervised vs. unsupervised

In an unsupervised setting, the objective is to keep as much of the information of the original signal $X$.

In the supervised case, the goal is to keep as much information *about the value to predict* $Y$. 
In the supervised case, features can be chosen specifically for a certain class of predictors, in which case it is called a *wrapper*.

The quality of a set of features is estimated by training a predictor and measuring empirically its performance.

This ties the definition of “information” to the predictor, avoiding to keep useless parts of the signal, but requires heavy computation and may lead to over-fitting.

The alternative is a *filter*, which is predictor-agnostic.

The standard supervised filter strategy consists in ranking features according to their individual information content, and selecting them in order.
Forward selection based on marginal information

Fisher score

The Fisher score provides an estimate of separability of the difference classes given a single features.

\[
S(X_j) = \frac{\sum_{i=1}^{C}(E(X_j | Y = i) - E(X_j))^2P(Y = i)}{\sum_{i=1}^{C} V(X_j | Y = i)P(Y = i)}
\]

Forward selection based on marginal information

Kolmogorov-Smirnov test

Another feature-selection score is based on the non-parametric Kolmogorov-Smirnov test

\[
S(X_j) = \max_x |P(X_j \leq x | Y = 0) - P(X_j \leq x | Y = 1)|
\]

This score does not depend on the cond. distributions if they are identical and as such is consistent to estimate if the distributions differ.
Forward selection based on marginal information

Mutual information

A fundamental concept that can be used directly in the case of discrete features and class is the mutual information

\[ I(A; B) = H(A) + H(B) - H(A, B) \]
\[ = H(A) - H(A | B) \]

It has some intuitive properties such as

\[ I(A; B) = I(B; A), \]

and

\[ I(A; A) = H(A). \]

Forward selection based on marginal information

Mutual information, relation with the error rate

If \( Y \) is a r.v. on \( \{1, \ldots, C\} \) standing for the label to predict, and \( f \) is a predictor of \( Y \) from \( X \), Fano's inequality implies

\[ P(f(X) \neq Y) \geq \frac{H(Y) - 1 - I(X; Y)}{\log C} \]

Hence, increasing the mutual information between \( X \) and \( Y \) lowers that lower bound, making accurate prediction feasible.

Hence, mutual information is often used as a score for feature selection

\[ S(X_j) = I(X_j; Y). \]
While these scores efficiently measure the information content of individual features, they do not avoid redundancy, nor account for joint informational content.

- If a very good feature is replicated multiple times, it will be picked again and again.

- If features are individually non-informative, and jointly informative, they will not be picked.

Consider $X_1, \ldots, X_D$ i.i.d. of distribution $B(0.5)$, and

$$Y = 1\{\sum_{i=1}^D X_i \in \mathbb{Z}\}.$$ 

Then

$$\forall i, \ I(X_i; Y) = 0$$

and

$$H(Y|X_1, \ldots, X_D) = 0.$$ 

Many (many!) feature selection schemes exist to take into account joint information, often through sampling of n-uplets, and redundancy with explicit penalty terms.
Selected features should be individually informative and weakly dependent.

CMIM selects features as follows:

\[ \nu(1) = \arg \max_n I(Y, X_n) \]

\[ \forall k, 1 \leq k < K, \quad \nu(k + 1) = \arg \max_n \left\{ \min_{l \leq k} I(Y, X_n | X_{\nu(l)}) \right\} \]

Face vs. non-face patches.
Forward selection based on marginal information
CMIM (cont.)

We apply this algorithm to a very noisy problem of drug efficiency prediction from molecular properties.

- 1,909 molecules.
- 139,351 binary features encoding three-dimensional properties.
- Provided by DuPont Pharmaceutical.
<table>
<thead>
<tr>
<th>Classifier</th>
<th>Error image</th>
<th>Error drug</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMIM feature selection + naive Bayesian</td>
<td>1.95%</td>
<td>11.72%</td>
</tr>
<tr>
<td>AdaBoost\textsubscript{reg} (optimized on test set)</td>
<td>3.06%</td>
<td>13.64%</td>
</tr>
<tr>
<td>MIM feature selection + naive Bayesian</td>
<td>8.59%</td>
<td>23.35%</td>
</tr>
<tr>
<td>CMIM feature selection + perceptron</td>
<td>9.32%</td>
<td>23.51%</td>
</tr>
<tr>
<td>Random feature selection + naive Bayesian</td>
<td>24.99%</td>
<td>40.13%</td>
</tr>
</tbody>
</table>

*(Fleuret, 2004)*

**Feature extraction**
Feature extraction is a good strategy for the visualization of data, and to control over-fitting when it is unsupervised.

However

- it may not reduce the computation, since the transformation may be expensive,

- the obtained features may be complex combinations of the original ones, hard to interpret.

PCA is the most classic unsupervised feature extraction procedure. It finds the best linear projection to minimize the $L^2$ norm between training points and their images.

Moreover, it ranks the extracted features according to the residual variance, hence it makes sense to take them in order until the target dimension is reached.
PCA may select directions of large variance which do not carry information about the class.

The Linear Discriminant Analysis (LDA) computes a linear transformation such that the means of the classes are pushed apart while each class is not dilated in the same directions.

It makes the assumption that the classes all follow Normal distributions of identical co-variance matrices.

Feature extraction
LDA (cont.)

Compute the with-class scatter matrix

$$S_w = \sum_{i=1}^{n} (x_i - \bar{x}_y)(x_i - \bar{x}_y)^T$$

and the between-class scatter matrix

$$S_b = \sum_{y=1}^{m} n_y (\bar{x}_y - \bar{x})(\bar{x}_y - \bar{x})^T$$

maximize the ratio between the two

$$\hat{w} = \arg \max_w \frac{w^T S_b w}{w^T S_w w}$$

which amounts to solving

$$S_b w = \lambda S_w w.$$ 

for the largest possible $\lambda$. This is the generalized Eigenvalue problem.
We consider the following population

We add 8 additional random dimensions $\sim \mathcal{U}[0, 10]$ and apply a random linear transformation.
After LDA, we retrieve two good directions

Unfortunately, the structure is often non-affine. This can be dealt with through kernelization, or with completely different methods.

The \( k \)-means procedure for instance can be seen as a crude discrete feature extraction method.

Given

\[
x_n \in \mathbb{R}^D, \quad n = 1, \ldots, N
\]

and a target cardinality \( C \), it finds an set of centroids \( \alpha_1, \ldots, \alpha_C \) minimizing

\[
\sum_n \min_c \| x_n - \alpha_c \|^2
\]

The extracted discrete feature is

\[
\arg \min_c \| x_n - \alpha_c \|^2.
\]
Feature extraction
Isomap

A more sophisticated algorithm to deal with non-affine structures is isomap.

It consists of approximating the geodesic distance with the euclidean distance in a space of small dimension.

Feature extraction
Isomap (cont.)

Given $x_1, \ldots, x_n \in \mathbb{R}^d$, Isomap first built a graph by connecting all points to its $k$ nearest neighbors.

Then, it approximates the geodesic distance between points with the length $\Delta$ of the shortest path in that graph.
The second step consists of finding $y_1, \ldots, y_n$ in $\mathbb{R}^r$ such that
\[
\forall i, j, \Delta(i, j) \simeq \|y_i - y_j\|
\]
This is done using the multi-dimensional scaling (MDS), which minimizes
\[
\sum_{i \neq j} (\|y_i - y_j\| - \Delta(i, j))^2
\]
Hence we finally have associated one $y_i$ in $\mathbb{R}^r$ to every $x_i$.
Note that we have not provided a way to generalize to other $x$. 

(J. B. Tenenbaum, V. de Silva and J. C. Langford, 2000)
Feature extraction
Isomap (cont.)


Isomap
Digits

Neural networks
Multi-task learning for NLP

There are not many supervised feature extraction procedures. The most popular are ANNs, whose early layers can be trained on one task, and re-used on another.

(Collober & Weston, 2008)

Neural networks
Multi-task learning for NLP

Without language model:

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>france</td>
<td>454</td>
<td>jesus</td>
<td>1973</td>
<td>xbox</td>
<td>6909</td>
</tr>
<tr>
<td>persuasion</td>
<td>thickets</td>
<td>decadent</td>
<td>widescreen</td>
<td>odd</td>
<td>ppa</td>
</tr>
<tr>
<td>faw</td>
<td>savary</td>
<td>verus</td>
<td>antica</td>
<td>anchieta</td>
<td>uddin</td>
</tr>
<tr>
<td>blackstock</td>
<td>sympathetic</td>
<td>oxide</td>
<td>shabby</td>
<td>emigration</td>
<td>biologically</td>
</tr>
<tr>
<td>giorgi</td>
<td>jfk</td>
<td>urbina</td>
<td>awe</td>
<td>marking</td>
<td>kayak</td>
</tr>
<tr>
<td>shaheed</td>
<td>khwarazm</td>
<td>eglinton</td>
<td>thud</td>
<td>heuer</td>
<td>mclarens</td>
</tr>
<tr>
<td>rumelia</td>
<td>stationery</td>
<td>epos</td>
<td>occupant</td>
<td>sambhaji</td>
<td>gladwin</td>
</tr>
<tr>
<td>planum</td>
<td>ilias</td>
<td>edging</td>
<td>revised</td>
<td>worshippers</td>
<td>centrally</td>
</tr>
<tr>
<td>goa’uld</td>
<td>gsNUMBER</td>
<td>frg</td>
<td>leavened</td>
<td>ritsuko</td>
<td>indonesia</td>
</tr>
<tr>
<td>collation</td>
<td>operator</td>
<td>namsos</td>
<td>pandionidae</td>
<td>lifeless</td>
<td>moneo</td>
</tr>
<tr>
<td>bacha</td>
<td>w.j.</td>
<td>shirt</td>
<td>biological</td>
<td>mahan</td>
<td>nilgiris</td>
</tr>
</tbody>
</table>
With language model:

<table>
<thead>
<tr>
<th>france</th>
<th>jesus</th>
<th>xbox</th>
<th>reddish</th>
<th>scratched</th>
<th>megabits</th>
</tr>
</thead>
<tbody>
<tr>
<td>454</td>
<td>1973</td>
<td>6909</td>
<td>11724</td>
<td>29869</td>
<td>87025</td>
</tr>
<tr>
<td>austria</td>
<td>god</td>
<td>amiga</td>
<td>greenish</td>
<td>nailed</td>
<td>octets</td>
</tr>
<tr>
<td>belgium</td>
<td>sati</td>
<td>playstation</td>
<td>bluish</td>
<td>smashed</td>
<td>mb/s</td>
</tr>
<tr>
<td>germany</td>
<td>christ</td>
<td>msx</td>
<td>pinkish</td>
<td>punched</td>
<td>bit/s</td>
</tr>
<tr>
<td>italy</td>
<td>satan</td>
<td>ipod</td>
<td>purplish</td>
<td>popped</td>
<td>baud</td>
</tr>
<tr>
<td>greece</td>
<td>kali</td>
<td>sega</td>
<td>brownish</td>
<td>cramped</td>
<td>carats</td>
</tr>
<tr>
<td>sweden</td>
<td>indra</td>
<td>psNUMBER</td>
<td>greyish</td>
<td>scraped</td>
<td>kbit/s</td>
</tr>
<tr>
<td>norway</td>
<td>vishnu</td>
<td>hd</td>
<td>grayish</td>
<td>screwed</td>
<td>megahertz</td>
</tr>
<tr>
<td>europe</td>
<td>ananda</td>
<td>dreamcast</td>
<td>whitish</td>
<td>sectioned</td>
<td>megapixels</td>
</tr>
<tr>
<td>hungary</td>
<td>parvati</td>
<td>geforce</td>
<td>silvery</td>
<td>slashed</td>
<td>gbit/s</td>
</tr>
<tr>
<td>switzerland</td>
<td>grace</td>
<td>capcom</td>
<td>yellowish</td>
<td>ripped</td>
<td>amperes</td>
</tr>
</tbody>
</table>

Regularization and sparsity
We have seen that for linear regression one minimize

\[ L(\alpha) = \sum_n \left( \sum_d \alpha_d x_n^d - y_n \right)^2 \]

and that we can add a \( L^2 \) penalty on the coefficients (aka “Ridge regression”)

\[ L(\alpha) = \sum_n \left( \sum_d \alpha_d x_n^d - y_n \right)^2 + \lambda \sum_d \alpha_d^2 \]

such a penalty favor smaller and more homogeneous weights. It also makes finding the optimal parameters properly conditioned for small data sets.

Regularization and sparsity

LASSO

Using a \( L^1 \) penalty

\[ L(\alpha) = \sum_n \left( \sum_d \alpha_d x_n^d - y_n \right)^2 + \lambda \sum_d |\alpha_d| \]

leads the least important model parameters to zero, since the improvement they bring has to be greater than \( \lambda \) for their optimal value to be non-zero.

This is still convex!
We consider
\[ \beta = (1, 2, 3, 4, 5, 0, 0, 0, 0, 0) \]
and \( \forall n = 1, \ldots, N \)
\[ x_n \sim \mathcal{N}(0, 1) \]
and
\[ y_n = \langle \beta, x_n \rangle + \mathcal{N}(0, 1). \]

We estimate
\[ \hat{\beta} = \arg \min_{\beta} \sum_n (y_n - \langle \beta, x_n \rangle)^2 + \lambda_2 \sum_d \beta_d^2 + \lambda_1 \sum_d |\beta_d|. \]
Regularization and sparsity

Toy example (cont.)

<table>
<thead>
<tr>
<th>$\lambda_1$</th>
<th>$\lambda_2$</th>
<th>$\hat{\beta}_1$</th>
<th>$\hat{\beta}_2$</th>
<th>$\hat{\beta}_3$</th>
<th>$\hat{\beta}_4$</th>
<th>$\hat{\beta}_5$</th>
<th>$\hat{\beta}_6$</th>
<th>$\hat{\beta}_7$</th>
<th>$\hat{\beta}_8$</th>
<th>$\hat{\beta}_9$</th>
<th>$\hat{\beta}_{10}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>-</td>
<td>1.037</td>
<td>2.033</td>
<td>2.999</td>
<td>3.995</td>
<td>5.041</td>
<td>0.039</td>
<td>-0.002</td>
<td>-0.055</td>
<td>0.005</td>
<td>0.084</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>2.000</td>
<td>1.035</td>
<td>2.027</td>
<td>2.992</td>
<td>3.987</td>
<td>5.029</td>
<td>0.040</td>
<td>-0.002</td>
<td>-0.054</td>
<td>0.005</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>4.000</td>
<td>1.033</td>
<td>2.024</td>
<td>2.987</td>
<td>3.978</td>
<td>5.020</td>
<td>0.040</td>
<td>-0.002</td>
<td>-0.054</td>
<td>0.004</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>8.000</td>
<td>1.028</td>
<td>2.017</td>
<td>2.975</td>
<td>3.962</td>
<td>5.003</td>
<td>0.040</td>
<td>-0.003</td>
<td>-0.054</td>
<td>0.003</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>16.000</td>
<td>1.020</td>
<td>2.002</td>
<td>2.951</td>
<td>3.932</td>
<td>4.964</td>
<td>0.041</td>
<td>-0.004</td>
<td>-0.053</td>
<td>0.001</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>32.000</td>
<td>1.003</td>
<td>1.973</td>
<td>2.903</td>
<td>3.871</td>
<td>4.895</td>
<td>0.043</td>
<td>-0.007</td>
<td>-0.052</td>
<td>-0.004</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>64.000</td>
<td>0.972</td>
<td>1.918</td>
<td>2.814</td>
<td>3.756</td>
<td>4.758</td>
<td>0.046</td>
<td>-0.011</td>
<td>-0.050</td>
<td>-0.012</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>128.000</td>
<td>0.913</td>
<td>1.818</td>
<td>2.651</td>
<td>3.542</td>
<td>4.500</td>
<td>0.050</td>
<td>-0.018</td>
<td>-0.046</td>
<td>-0.026</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>256.000</td>
<td>0.814</td>
<td>1.644</td>
<td>2.377</td>
<td>3.182</td>
<td>4.067</td>
<td>0.056</td>
<td>-0.027</td>
<td>-0.040</td>
<td>-0.046</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>512.000</td>
<td>0.670</td>
<td>1.380</td>
<td>1.968</td>
<td>2.644</td>
<td>3.404</td>
<td>0.061</td>
<td>-0.037</td>
<td>-0.032</td>
<td>-0.067</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>1024.000</td>
<td>0.493</td>
<td>1.045</td>
<td>1.463</td>
<td>1.975</td>
<td>2.571</td>
<td>0.058</td>
<td>-0.040</td>
<td>-0.022</td>
<td>-0.077</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>2048.000</td>
<td>0.323</td>
<td>0.703</td>
<td>0.966</td>
<td>1.310</td>
<td>1.724</td>
<td>0.047</td>
<td>-0.035</td>
<td>-0.014</td>
<td>-0.069</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>4096.000</td>
<td>0.191</td>
<td>0.424</td>
<td>0.573</td>
<td>0.781</td>
<td>1.037</td>
<td>0.032</td>
<td>-0.024</td>
<td>-0.008</td>
<td>-0.050</td>
</tr>
<tr>
<td>1.000</td>
<td>-</td>
<td>1.037</td>
<td>2.032</td>
<td>2.999</td>
<td>3.994</td>
<td>5.040</td>
<td>0.039</td>
<td>-0.001</td>
<td>-0.054</td>
<td>0.005</td>
<td>0.083</td>
</tr>
<tr>
<td>2.000</td>
<td>-</td>
<td>1.037</td>
<td>2.031</td>
<td>2.998</td>
<td>3.993</td>
<td>5.040</td>
<td>0.038</td>
<td>-0.001</td>
<td>-0.053</td>
<td>0.004</td>
<td>0.083</td>
</tr>
<tr>
<td>4.000</td>
<td>-</td>
<td>1.036</td>
<td>2.028</td>
<td>2.997</td>
<td>3.992</td>
<td>5.039</td>
<td>0.037</td>
<td>-0.052</td>
<td>0.003</td>
<td>0.081</td>
<td></td>
</tr>
<tr>
<td>8.000</td>
<td>-</td>
<td>1.034</td>
<td>2.027</td>
<td>2.995</td>
<td>3.991</td>
<td>5.035</td>
<td>0.035</td>
<td>-0.050</td>
<td>0.001</td>
<td>0.079</td>
<td></td>
</tr>
<tr>
<td>16.000</td>
<td>-</td>
<td>1.031</td>
<td>2.023</td>
<td>2.991</td>
<td>3.986</td>
<td>5.029</td>
<td>0.032</td>
<td>-0.046</td>
<td>-0.075</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32.000</td>
<td>-</td>
<td>1.023</td>
<td>2.016</td>
<td>2.984</td>
<td>3.978</td>
<td>5.024</td>
<td>0.024</td>
<td>-0.038</td>
<td>-0.066</td>
<td></td>
<td></td>
</tr>
<tr>
<td>64.000</td>
<td>-</td>
<td>1.008</td>
<td>2.003</td>
<td>2.965</td>
<td>3.961</td>
<td>5.010</td>
<td>0.008</td>
<td>-0.022</td>
<td>-0.048</td>
<td></td>
<td></td>
</tr>
<tr>
<td>128.000</td>
<td>-</td>
<td>0.978</td>
<td>1.975</td>
<td>2.930</td>
<td>3.929</td>
<td>4.983</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0.014</td>
<td></td>
</tr>
<tr>
<td>256.000</td>
<td>-</td>
<td>0.917</td>
<td>1.916</td>
<td>2.865</td>
<td>3.864</td>
<td>4.925</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>512.000</td>
<td>-</td>
<td>0.793</td>
<td>1.800</td>
<td>2.734</td>
<td>3.734</td>
<td>4.802</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1024.000</td>
<td>-</td>
<td>0.546</td>
<td>1.564</td>
<td>2.474</td>
<td>3.471</td>
<td>4.570</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2048.000</td>
<td>-</td>
<td>0.051</td>
<td>1.093</td>
<td>1.952</td>
<td>2.941</td>
<td>4.092</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4096.000</td>
<td>-</td>
<td>-</td>
<td>0.090</td>
<td>0.876</td>
<td>1.947</td>
<td>3.149</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Some remarks

- The $L^1$ and $L^2$ penalty terms can be combined (elastic net)
- It can be shown that LASSO is equivalent to SVM
- All these regularization can be interpreted in a Bayesian framework with the proper priors on the parameters
- As for feature selection, these methods can be used both as a regularizer to mitigate over-fitting and reduce the computational cost, or as a mean to interpret the data
The usual setting for learning for classification:

- A training set,
- a family of classifiers,
- a test set.

Learning means to choose a classifier according to its performances on the training set to get good performances on the test set.
We will use the following notation:

- $\mathcal{X}$ the space of the objects to classify (for instance images)
- $\mathcal{C}$ the family of classifiers
- $S = ((X_1, Y_1), \ldots, (X_{2N}, Y_{2N}))$ a random variable on $(\mathcal{X} \times \{0, 1\})^{2N}$ standing for the training and test samples.
- $F$ a random variable on $\mathcal{C}$ standing for the learned classifier. It can be a deterministic function of $S$ or not.

(1) The set $\mathcal{C}$ contains all the classifiers obtainable with the learning algorithm.

For an ANN for instance, there is one element of $\mathcal{C}$ for every single configuration of the synaptic weights.

(2) The variable $S$ is not one sample, but a family of $2N$ samples with their labels. It contains both the training and the test set.
Gap between training and test error

One fixed $f$

For every $f \in \mathcal{C}$, let $\xi(f, S)$ denote the difference between the training and the test errors of $f$.

$$\xi(f, S) = \frac{1}{N} \sum_{i=1}^{N} 1\{f(X_{N+i}) \neq Y_{N+i}\} - \frac{1}{N} \sum_{i=1}^{N} 1\{f(X_i) \neq Y_i\}$$

Where $1\{t\}$ is equal to 1 if $t$ is true, and 0 otherwise. Since $S$ is random, this is a random quantity.

Gap between the test and the training error

Data-dependent $f$

Given $\eta \geq 0$, we want to bound the probability that the test error is less than the training error plus $\eta$.

$$P(\xi(F, S) \leq \eta) \geq ?$$

Not that here $F$ is not constant anymore and is a function of the samples $X_1, \ldots, X_{2N}$ and the $Y_1, \ldots, Y_N$. 
Where we see that for any fixed $f$, the test and training errors are likely to be similar . . .

Concentration Inequality
Hoeffding's inequality (1963)

Given a family of independent random variables $Z_1, \ldots, Z_N$, bounded $\forall i, Z_i \in [a_i, b_i]$, if $S$ denotes $\sum_i Z_i$, then $\forall t \geq 0$ we have Hoeffding's inequality (1963)

$$P(S - E(S) > t) \leq \exp \left( -\frac{2t^2}{\sum_i (b_i - a_i)^2} \right)$$

This is an concentration result: It tells how much $S$ is concentrated around its average value.
Note that the $\{f(X_i) \neq Y_i\}$ are i.i.d Bernoulli, and we have

$$\xi(f, S) = \frac{1}{N} \sum_{i=1}^{N} 1\{f(X_{N+i}) \neq Y_{N+i}\} - \frac{1}{N} \sum_{i=1}^{N} 1\{f(X_i) \neq Y_i\}$$

$$= \frac{1}{N} \sum_{i=1}^{N} \frac{1\{f(X_{N+i}) \neq Y_{N+i}\} - 1\{f(X_i) \neq Y_i\}}{\Delta_i}$$

Thus $\xi$ is the averaged sum of the $\Delta_i$, which are i.i.d random variables on $\{-1, 0, 1\}$ of zero mean.

Concentration Inequality
Application to the error

Hence, when $f$ is fixed we have (Hoeffding):

$$\forall f, \forall \eta \geq 0, \; P(\xi(f, S) > \eta) \leq \exp\left(-\frac{1}{2} \eta^2 N\right)$$
Where we realize that the probability the chosen $F$ fails is lower than the probability that there exists an $f$ that fails . . .

We have

$$P(\xi(F, S) > \eta) = \sum_f P(F = f, \xi(F, S) > \eta)$$
$$= \sum_f P(F = f, \xi(f, S) > \eta)$$
$$\leq \sum_f P(\xi(f, S) > \eta)$$
$$\leq \|C\| \exp\left(-\frac{1}{2} \eta^2 N\right)$$

This is our first generalization bound!
Union bound  
We can fix the probability

We can conversely express the gap as a function of the probability we want.

If we define

\[ \epsilon^* = \|C\| \exp\left(-\frac{1}{2} \eta^2 N\right) \]

We have

\[ \sqrt{2 \frac{\log \|C\| - \log \epsilon^*}{N}} = \eta \]

Hence from

\[ P(\xi(F, S) > \eta) \leq \|C\| \exp\left(-\frac{1}{2} \eta^2 N\right) \]

we get

\[ P\left(\xi(F, S) > \sqrt{2 \frac{\log \|C\| + \log \frac{1}{\epsilon^*}}{N}}\right) \leq \epsilon^* \]

Thus, with probability \(1 - \epsilon^*\), the gap between the train and test errors grows as the square root of the log of the nb. of classifiers.
Proving a bound with “real” predictors is in general a bit technical.

However, if we fix the number of weak learners to $N$, impose that their coefficients take only the values $\pm 1$, and bound the number of Boosting rounds to $M$, we know that we have a total of $(2N)^M$ possible predictors, and we can use our bound directly.

For decision trees, we can do something similar.

If we have $N$ possible Boolean decisions to put at the nodes, and the depth is bounded by $D$, then there are at most $N^{2^{D-1}}$ trees.
Where we realize that we can arbitrarily distribute allowed errors on the $f$s before looking at the training data . . .

Until now, the only quantity we control is $||C||$: If we know that certain mappings can be removed without hurting the train error, we can remove them and get a better bound.

Can we do something better than that?

We introduce $\eta(f)$ as the control we want between the train and test error if $f$ is chosen. Until now, this was constant.

Now we want to bound the probability that the gap between the training and the test error for $f$ is lower than
Prior on $\mathcal{C}$  
Let make $\eta$ depend on $F$

Let $\epsilon(f)$ denote the (bound on the) probability that the constraint is not verified for $f$:

\[
P(\xi(F, S) > \eta(F)) \leq P(\exists f \in \mathcal{C}, \xi(f, S) > \eta(f)) \leq \sum_f P(\xi(f, S) > \eta(f)) \leq \sum_f \epsilon(f)
\]

and we have

\[
\forall f, \eta(f) = \sqrt{2 \frac{\log \frac{1}{\epsilon(f)}}{N}}
\]

Prior on $\mathcal{C}$  
Let make $\eta$ depend on $F$

Let define $\epsilon^* = \sum_f \epsilon(f)$ and $\rho(f) = \frac{\epsilon(f)}{\epsilon^*}$. The later is a distribution on $\mathcal{C}$.

Note that both can be fixed arbitrarily, and we have

\[
\forall f, \eta(f) = \sqrt{2 \frac{\log \frac{1}{\rho(f)} + \log \frac{1}{\epsilon^*}}{N}}
\]
Prior on $C$
Let’s put everything together

Our final result is that, if

- we choose a distribution $\rho$ on $C$ arbitrarily,
- we choose $0 < \epsilon^* < 1$ arbitrarily,
- we sample a pair $S$ training set / test set each of size $N$,
- we choose a $F$ after looking at the training set.

Then, we have with probability greater than $1 - \epsilon^*$:

$$\xi(F, S) \leq \sqrt{2 \frac{\log \frac{1}{\rho(F)} + \log \frac{1}{\epsilon^*}}{N}}$$

where $\xi(F, S)$ is the difference between the test and train errors.

Prior on $C$
This is a philosophical theorem!

If we see $-\log \rho(f)$ as the “description” length of $f$ (think Huffman). Our result (true with probability $1 - \epsilon^*$)

$$\xi(F, S) \leq \sqrt{2 \frac{\log \frac{1}{\rho(F)} + \log \frac{1}{\epsilon^*}}{N}}$$

says that picking a classifier with a long description leads to a bad control on the test error.

*Entities should not be multiplied unnecessarily.*

Principle of parsimony of William of Occam (1280 – 1349). Also known as Occam’s Razor.
Practical session

Random vs. wrapper vs. filter

If you type

```
wget http://www.idiap.ch/˜fleuret/files/EE613/EE613-pw14.tgz
.tar zxfv EE613-pw14.tgz
.cd EE613/pw14
wget http://www.idiap.ch/˜fleuret/files/EE613/mnist.tgz
.tar zxfv mnist.tgz
./do.sh demo
```

you should obtain after a few seconds a printout ending with

```
Training the decision tree ... done.
********************************************************************
Using 784 questions.
Train error 0 %
Test error 0.83 %
********************************************************************
```
We re-use the classes we had for decision trees, and will try to find good subsets of questions to train them.

```cpp
class DecisionTree : public Classifier {
public:
    DecisionTree(QuestionSet *question_set);
    virtual ~DecisionTree();
    virtual void train(VignetteSet *train_set);
    virtual int predict(VignetteSet *vs, int n_vignette);
};
```

```cpp
class QuestionSet {
public:
    virtual int nb_questions() = 0;
    virtual bool response(int n_question,
                           VignetteSet *vs, int n_vignette) = 0;
};
```

We have a new class which models a subset of an original set of questions:

```cpp
class SubQuestionSet : public QuestionSet {
public:
    SubQuestionSet(QuestionSet *source, int *selected);
    ~SubQuestionSet();
    virtual int nb_questions();
    virtual bool response(int n_question,
                           VignetteSet *vs, int n_vignette);
};
```
Practical session
Random vs. wrapper vs. filter

So for instance, if we want to train a tree using the 10 first questions of a PixelQuestionSet, we would write:

```c
PixelQuestionSet qs(train_image_set->width(),
                   train_image_set->height());

int selected[qs.nb_questions()];
for(int k = 0; k < qs.nb_questions(); k++) {
    if(k < 10) {
        selected[k] = 1;
    } else {
        selected[k] = 0;
    }
}

SubQuestionSet sqs(&qs, selected);
print_errors_for_question_set(train_image_set, test_image_set,
                              &sqs);
```

Practical session
Random vs. wrapper vs. filter

We have the three following functions to help us:

```c
scalar_t mutual_information(int nb, int *x, int *y);

void tag_subset(int nb_total, int nb_to_tag,
                 int *tagged);

void tag_the_top_ones(int nb_total, scalar_t *scores, int nb_to_tag,
                       int *tagged);
```
François Fleuret
IDIAP Research Institute
francois.fleuret@idiap.ch
http://www.idiap.ch/~fleuret