# AMRC Exam Questions Answered 

Florian D.

September 2023

## 1 Regression / Linear Methods

Question 1: Explain Ridge and Lasso Regression. What are the differences? How do they differ from OLS? Show all formulas, explain the $\lambda$ parameter and also explain why Lasso sets coefficients exactly to zero and Ridge does not.

The ordinary least squares regression (OLS) is BLUE (best linear unbiased estimator) if we assume that the error terms $\varepsilon$ are normally distributed with a mean of zero and equal variance $\sigma^{2}$. It has the following form:

$$
y=\beta_{0}+\sum_{j=1}^{p} \beta_{j} x_{i j}
$$

The residual sum of squares is the minimization criterion:

$$
R S S(\beta)=\sum_{i=1}^{n}\left(y_{i}-\beta_{0}-\sum_{j=1}^{p} \beta_{j} x_{i j}\right)^{2}
$$

However it is not always the best idea to keep the model unbiased. We could reduce the sampling variance by increasing the bias. Ridge and Lasso penalize the parameter size.

$$
\hat{\beta}_{\text {Ridge }}=\underset{\beta}{\arg \max } \sum_{i=1}^{n}\left(y_{i}-\beta_{0}-\sum_{j=1}^{p} \beta_{j} x_{i j}\right)^{2}+\lambda \sum_{j=1}^{p} \beta_{j}^{2}
$$

We can see in the formula above that the size of the parameters $\beta_{j}$ is penalized by taking their square. This leads to a smoother model and prevents overfitting. How much the model is penalized for large betas depends on the regularization parameter $\lambda$.

$$
\hat{\beta}_{\text {Lasso }}=\underset{\beta}{\arg \max } \sum_{i=1}^{n}\left(y_{i}-\beta_{0}-\sum_{j=1}^{p} \beta_{j} x_{i j}\right)^{2}+\lambda \sum_{j=1}^{p}\left|\beta_{j}\right|
$$

For Lasso we use the L1 norm instead of the L2 norm. This means that the acceptable region is (visually speaking) diamond-shaped, rather than a circle. Thus we end up at zero values much easier.

## Question 2: Explain PCR and PLS.

PCR stands for Principal Component Regression. The idea is to reduce the dimensionality of the inputs by transforming the data into a new set of uncorrelated variables, which are ranked according to their variance size. These are the principal components. Here it is important to center and scale the data first. PCR is not scale-invariant.

$$
Z=X V
$$

Z are the principal components, which are the result of multiplying the inputs X by an eigenvector matrix $V$. The shape of $X$ is ( $n \times p$ ), the shape of $V$ is ( $\mathrm{p} \times \mathrm{p}$ ), which results in Z having the shape ( $\mathrm{n} \times \mathrm{p}$ ). It is important to mention that PCR does not take the latent variables $y_{i}$ into account.

$$
\begin{gathered}
y=X \beta+\varepsilon \\
=X V V^{\top} \beta+\varepsilon \\
=Z \theta+\tilde{\varepsilon}
\end{gathered}
$$

If we only use $q<p$ principal coponents:

$$
y=Z_{1: q} \theta_{1: q}+\tilde{\varepsilon}
$$

The estimator $\theta$ can be back-transformed to be interpreted in terms of the original variables:

$$
\tilde{\hat{\beta}}=V_{1: q} \hat{\theta}_{1: q}
$$

It is important to mention that $\tilde{\hat{\beta}}$ is no longer the original estimator unless the first $q$ principal components explain all information of X .

PLS on the other hand stands for partial least squares. Here we also construct a set of linear combinations of the input for regression but we also use y in addition to X for this.

$$
y_{i}=t_{i}^{\top} \gamma+\tilde{\varepsilon}_{i}
$$

The formula above shows the form on a PLS regression model. Here instead of using the inputs X, we have a score matrix $T$, which has the shape ( $n \times q$ ), where $q$ is less or equal to $p$. We don't know the content of T but we obtain each column of it sequentially by using the PLS criterion:

$$
w_{k}=\underset{w}{\arg \max } \operatorname{Cov}(y, X w)
$$

We obtain the columns of the matrix W by applying this criterion. Then the score matrix T is obtained by:

$$
T=X W
$$

It is important to mention that we have the following constraints:

$$
\left\|w_{k}\right\|=1 \text { to make sure these are just directions }
$$

$$
\operatorname{Cov}\left(X_{w_{k}}, X_{w_{j}}\right)=0
$$

to make sure that all directions are orthogonal. Our goal is to find the direction in which we can project X so that the covariance with the output y is maximized.

Question 3: Explain for multiple regression models the OLS solution, how to arrive at it and what to do in the case of near singularity of $X^{\top} X$

For the least squares regression model, we have the following solution for the estimator $\hat{\beta}$ :

$$
\hat{\beta}=\left(X^{\top} X\right)^{-1} X^{\top} y
$$

For the prediction $\hat{y}$ we can write:

$$
\begin{gathered}
\hat{y}=X \hat{\beta} \\
=X\left(X^{\top} X\right)^{-1} X^{\top} y
\end{gathered}
$$

So $X\left(X^{\top} X\right)^{-1} X^{\top}$ is called the hat matrix because it puts a hat on the y .
A problem that we have is that $X^{\top} X$ can become nearly singular when the input variables are highly correlated. This would mean the matrix would almost be not of full rank. And almost not invertible. Practically speaking, this makes the model extremely sensitive to changes in the input. The solution would be to use a regularized method like Ridge or Lasso.

## 2 Classification Methods

Question 4: Explain LDA, QDA and RDA. What is the idea of LDA? What is the Bayesian Theorem, what are its assumptions? Specify the $\varphi$ formula. Also provide the formula for LDA and QDA. What are the components of LDA and how do you estimate them? Why can you estimate them?

LDA stands for Linear Discriminant Analysis. The goal here is to find a linear combination of the input which best separates the two classes. The following formula gives us the conditional probability that given an observation x , the random variable G is k :

$$
P(G=k \mid x)=\frac{h_{k}(x) \pi_{k}}{\sum_{l=1}^{K} h_{l}(x) \pi_{l}}
$$

In this formula above, $h_{k}(x)$ is the density function of x in class $\mathrm{G}=\mathrm{k}$. The probability of any observation belonging to class k is $\pi_{k}$.

Oftentimes it is assumed that $h_{k}(x)$ is the density of a multivariate normal distribution:

$$
\varphi_{k}(x)=\frac{1}{\sqrt{(2 \pi)^{p}\left|\Sigma_{k}\right|}} e^{-\frac{\left(x-\mu_{k}\right)^{\top} \Sigma_{k}^{-1}\left(x-\mu_{k}\right)}{2}}
$$

LDA arises when we assume that all classess have a common covariance $\Sigma_{k}$.
Then the linear discriminant function is:

$$
\delta_{k}(x)=x^{\top} \Sigma^{-1} \mu_{k}-\frac{1}{2} \mu_{k}^{\top} \Sigma^{-1} \mu_{k}+\log \pi_{k}
$$

The decision rule is then:

$$
G(x)=\underset{k}{\arg \max } \delta_{k}(x)
$$

In QDA, which is quadratic discriminant analysis, we do not assume equal covariance matrices. Then the discriminant function becomes:

$$
\delta_{k}(x)=-\frac{1}{2} \log \left|\Sigma_{k}\right|-\frac{1}{2}\left(x-\mu_{k}\right)^{\top} \Sigma_{k}^{-1}\left(x-\mu_{k}\right)+\log \pi_{k}
$$

Finallyu there is the special case of the regularized discriminant analysis (RDA). Here we have a parameter $\alpha$, which provides are compromise between LDA and QDA.

$$
\hat{\Sigma}_{k}(\alpha)=\alpha \hat{\Sigma}_{k}+(1-\alpha) \hat{\Sigma}
$$

If $\alpha$ is 0 , we have LDA, if it is 1 we have QDA. Everything in between is a compromise.

Question 5: Explain logistic regression. Provide all formulas, including the loglikelihood function.

Logistic regression is a classification algorithm. Its output also contains an inference statistic, which provides information about which variables are well suitable for separating the groups. The model looks like this (for two classes):

$$
\log \frac{P(G=1 \mid x)}{P(G=2 \mid x)}=\beta_{0}+\beta_{1}^{\top} x=z
$$

We can rewrite it like this:

$$
\begin{gathered}
\log \frac{P_{1}}{P_{2}}=z \\
\frac{P_{1}}{P_{2}}=\frac{P_{1}}{1-P_{1}}=e^{z} \\
P_{1}=e^{z}-P_{1} e^{z} \rightarrow P_{1}+P_{1} e^{z}=P_{1}\left(1+e^{z}\right)=e^{z} \\
P_{1}=\frac{e^{z}}{1+e^{z}}
\end{gathered}
$$

For $P_{2}$ we can say:

$$
P_{2}=1-P_{1}=1-\frac{e^{z}}{1+e^{z}}=\frac{1}{1+e^{z}}
$$

The log-likelihood function is:

$$
l(\beta)=\sum_{i=1}^{n} \log p_{g_{i}}\left(x_{i}, \beta\right)
$$

## 3 Basis Expansions / Splines

Question 6: Explain what splines are in general. What is the criterion to optimize and what are the solutions (provide formulas). How do you determine lambda and the degrees of freedom. What do degrees of freedom mean in this context? Why do we care about it? Talk about knots, penalization of curvature and how to minimize it.

In general splines are piecewise polynomials. A spline of order M with k knots $\xi_{i}$ where i goes from 1 to k is a piecewise polynomial of order M , which has continuous derivatives up to order M-2 (needed for curvature later on). The general form of the basis functions is:

$$
\begin{gathered}
h_{j}(x)=x^{j-1}, j=1, \ldots, M \\
h_{M+l}(x)=\left(x-\xi_{l}\right)_{+}^{M-1}, l=1, \ldots, \mathrm{k}
\end{gathered}
$$

Here it is important to notice that $\mathrm{M}=1$ means constant, $\mathrm{M}=2$ means linear, $\mathrm{M}=3$ means quadratic and $M=4$ means cubic splines.

For splines, we have to choose the order $M$ of the splines, the number of knots $|\xi|$ and the placement of the knots.

The polynomials we use for the regions tend to be erratic near the lower and upper data range. This can result in poor approximations. In natural cubic splines we thus also add an extra condition that the function has to be linear beyound the boundary knots. By doing this we also win back 4
degrees of freedom (since cubic and now linear in both boundary regions).
With smoothing splines we can avoid to choose the number and placement of knots. We do this by controlling the complexity of the fit through regularization. We minimize the following residual sum of squares:

$$
R S S(f, \lambda)=\sum_{i=1}^{n}\left\{y_{i}-f\left(x_{i}\right)\right\}^{2}+\lambda \int f^{\prime \prime}(t)^{2} d t
$$

The first term measures the closeness to the data and the second term penalizes curvature of the function. We basically sum up the squared curvatures of the function at all points. By setting $\lambda$ to 0 , f can be any function that interpolates the data. By setting $\lambda$ to $\infty$ we get the simple least square fit, where no second derivative can be tolerated.

The solution to this minimization problem is a unique minimizer, which is a natural cubic spline with knots at the values $x_{i}$ with i going from 1 to n . It seems like this solution is over-parameterized, since n knots correspond to n degrees of freedom. However, these degrees of freedom are reduced by the penalty term, since the spline coefficients are shrunk towards the linear fit.

Since the solution is a natural cubic spline, we can write it as:

$$
f(x)=\sum_{j=1}^{n} N_{j}(x) \theta_{j}
$$

where $N_{j}$ is the j-th spline basis function.
So the criterion is reduced to:

$$
R S S(\theta, \lambda)=(y-N \theta)^{\top}(y-N \theta)+\lambda \theta^{\top} \Omega_{N} \theta
$$

with $\{N\}_{i j}=N_{j}\left(x_{i}\right)$ and $\left\{\Omega_{N}\right\}_{j k}=\int N_{j}^{\prime \prime}(t) N_{k}^{\prime \prime}(t) d t$
The solution is:

$$
\hat{\theta}=\left(N^{\top} N+\lambda \Omega_{N}\right)^{-1} N^{\top} y
$$

This is a generalized form of the ridge regression. Choosing $\lambda$ can be done using cross-validation.

## 4 Generalized Additive Models (GAMs)

Question 7: What are GAMs? What does the model look like? What is the minimization criterion? How do we find a solution?

Instead of having a weighted sum (linear combination) of regressor variables in GAMs we have a weighted sum (linear combination) of transformed regressor variables. The general form of a GAM looks like this:

$$
g[\mu(x)]=\alpha+f_{1}\left(x_{1}\right)+\ldots+f_{p}\left(x_{p}\right)
$$

In general, we have a conditional expectation of the target value $y$, given the corresponding data. This expectation is $\mu(x)$. We take this expectation and feed it into a so-called link function $g$ on the left side. Examples are the identity link, the logit function or just the log.

We can also write the model like this:

$$
y_{i}=\alpha+\sum_{j=1}^{p} f_{j}\left(x_{i j}\right)+\varepsilon_{i}
$$

To find the functions $f_{j}$, we minimize the penalized residual sum of squares criterion:

$$
\operatorname{PRSS}\left(\alpha, f_{1}, \ldots, f_{p}\right)=\sum_{i=1}^{n}\left\{y_{i}-\alpha-\sum_{j=1}^{p} f_{j}\left(x_{i j}\right)\right\}^{2}+\sum_{j=1}^{p} \lambda_{j} \int f_{j}^{\prime \prime}\left(t_{j}\right)^{2} d t
$$

Here $t_{j}$ is the domain along which the smoothing is applied. Independent of the choice of the smoothing parameters $\lambda_{j}$ an additive model with cubic splines minimizes the PRSS. The solution can be found using the backfitting algorithm.

The general idea is to start with an initial guess for each component (smoothed function) of the model. Then we pick one of the components and keep all others fixed. We fit this component to the residuals from the other components. We update our guess based on the information that the other components have not explained yet. We repeat this process for all components. We do all of this until the estimates stop changing (or change very little). Once, converged, our GAM is estimated.

## 5 Tree-Based Methods

Question 8: What are regression and classification trees? Explain the general idea and provide the criterion to be minimized for both cases. Also explain the different measures of node impurity. Furthermore, explain how trees are split (splitting criteria and formula), how to grow a tree, when to stop and how to prevent overfitting?

In general, tree-based methods partition the feature space into rectangular regions. The goal is for them to be as homogeneous as possible. In the context of the lecture, we limited the decision rules and thus the splits to binary splits, meaning we always only have two branches. The split is based on a split variable (which feature to look at) and a split point (what is the cutoff value for the split).

Our tree partitions our feature space into $M$ Regions $R_{1}, \ldots, R_{M}$ and we model the response for each region as a constant $c_{m}$ (meaning every input combination that lies in this region will produce the same result). This can be written as:

$$
f(x)=\sum_{m=1}^{M} c_{m} I\left(x \in R_{m}\right)
$$

Here $I$ is the indicator function, which returns 1 if x is part of $R_{m}$ and 0 otherwise. If our minimization criterion is the sum of squares, the best choice of $\hat{c}_{m}$ is just the average of the $y_{i}$ values within each region.

$$
\hat{c}_{m}=\operatorname{ave}\left(y_{i} \mid x_{i} \in R_{m}\right)
$$

Finding the best partition for this problem is computationally infeasible, thus we approximate a solution. For this we consider a split variable $x_{j}$ and a split point s. A split based on these is defined by two half planes:

$$
R_{1}(j, s)=\left\{x \mid x_{j} \leq s\right\} ; \quad R_{2}(j, s)=\left\{x \mid x_{j}>s\right\}
$$

We then define the following minimization criterion and search for the splitting variable $x_{j}$ and the split point $s$ that solve it:

$$
\min _{j, s}\left[\min _{c_{1}} \sum_{x_{i} \in R_{1}(j, s)}\left(y_{i}-c_{1}\right)^{2}+\min _{c_{2}} \sum_{x_{i} \in R_{2}(j, s)}\left(y_{i}-c_{2}\right)^{2}\right]
$$

Put into words, we are basically looking for a splitting variable and a split point so that the sum of the errors of the two resulting regions are minimized. The inner part of this problem is easily solved because:

$$
\hat{c}_{1}=\operatorname{ave}\left(y_{i} \mid x_{i} \in R_{1}(j, s) \text { and } \hat{c}_{2}=\operatorname{ave}\left(y_{i} \mid x_{i} \in R_{2}(j, s)\right.\right.
$$

Because this is so trivial, we can scan through all the inputs to determine the best pair $(j, s)$.
To avoid overfitting here, we use a tuning parameter, which tries to regulate the model's complexity. First we grow a large tree $T_{0}$. We stop growing this tree when a minimum node size is reached. Then we prune this tree using cost complexity pruning. By doing this, we get a sub-tree $T$.

For the cost complexity criterion we index the leaf nodes by $m$ representing the Region $R_{m} .|T|$ denotes the number of leaf nodes in our sub-tree $T$ and

$$
\hat{c}_{m}=\frac{1}{n_{m}} \sum_{x_{i} \in R_{m}} y_{i}
$$

(this is just the average of the region since $n_{m}$ is the number of observations in $R_{m}$ )
as well as

$$
Q_{m}(T)=\frac{1}{n_{m}} \sum_{x_{i} \in R_{m}}\left(y_{i}-\hat{c}_{m}\right)^{2}
$$

(which just denotes the impurity of the node).
With this, we can now define the cost complexity criterion as

$$
c_{\alpha}(T)=\sum_{m=1}^{|T|} n_{m} Q_{m}(T)+\alpha|T|
$$

We want to minimize this criterion, which means that we want to reduce the impurity as well as the size of the tree as much as possible. To find the optimal sub-tree $T_{\alpha}$ for a given $\alpha$, we eliminate the internal node which yields the smallest increase of $\sum_{m} n_{m} Q_{m}(T)$ per node. We do this until no node is left. This sequence of sub-trees must include $T_{\alpha}$.

For classification, we partition the x -variables into K classes based on their y -values, which range from 1 to K . In a node m representing a region $R_{m}$ with $n_{m}$ observations, we define the proportion of the class k in this node like this:

$$
\hat{p}_{m k}=\frac{1}{n_{m}} \sum_{x_{i} \in R_{m}} I\left(y_{i}=k\right)
$$

Every node $m$ is assigned a class like this:

$$
k(m)=\underset{k}{\arg \max } \hat{p}_{m k}
$$

In other words, we assign the most common class in a node to this node.

Three example measures that can be used for the impurity measure $Q_{m}(T)$ are:

- Misclassification error: $\frac{1}{n_{m}} \sum_{x_{i} \in R_{m}} I\left(y_{i} \neq k(m)\right)=1-\hat{p}_{m} k$
- Gini Index: $\Sigma_{k \neq k^{\prime}} \hat{p}_{m k} \hat{p}_{m k^{\prime}}=\sum_{k=1}^{K} \hat{p}_{m k}\left(1-\hat{p}_{m k}\right)$
- Cross-entropy: $\sum_{k=1}^{K} \hat{p}_{m k} \log \hat{p}_{m k}$

Question 9: What are Random Forests? What is the basic idea behind them? Explain the algorithm step-by-step.

Decision trees are very sensitive to small changes in the data. A small change in the data can lead to a completely different tree. What random forests do is they train many trees in an ensemble. These trees are generated randomly by using only bootstrapped samples and by only using a random selection of variables to be available for splitting at each knot.

The algorithm works as follows:

- Step 1: Bootstrap Sampling (random sample with replacement of size n)
- Step 2: Grow tree based on this first sample
- At each knot choose a random selection of p variables to be available for splitting
- For classification choose $\sqrt{p}$ variables and for regression choose $\frac{p}{3}$ variables
- Step 3: Use the OOB data (not used for training, i.e. not part of the bootstrapped sample) to compute feature importance
- Compute the impurity of the whole tree $T_{b}$ as $\pi_{b}=\sum_{m=1}^{\left|T_{b}\right|} Q_{m}\left(T_{b}\right)$ (sum of impurity of all nodes)
- Shuffle each variable $x_{j}$ randomly and compute how impure the tree is after this as $\pi_{b_{j}}$
- The feature importance is $\delta_{b_{j}}=\pi_{b}-\pi_{b_{j}}$
- Step 4: Repeat steps 1-3 for $B$ number of trees and combute for each the feature importances $\delta_{b_{j}}$ for all $b$ and all $j$
- Step 5: Compute the overall feature importance score for the j -th variable as follows:

$$
\hat{\theta}_{j}=\frac{1}{B} \sum_{b=1}^{B} \delta_{b_{j}}
$$

To make decisions with the random forest we just take the average of all tree responses for regression and the majority for classification.

## 6 Support Vector Machines (SVMs)

Question 10: What are SVMs? How do they work? What is the criterion for the linearly separable case and for the non-separable case? Explain the optimization formula and how you get there for both. Explain $L_{p}$ and $L_{d}$ with constraints.

Support Vector Machines aim to separate groups of data using hyperplanes. In the lectore we focused on the two class case ( $\mathrm{K}=2$ ). The classification returns a sign (positive or negative) for the group membership.

In general a hyperplane $\mathcal{L}$ is defined by:

$$
f(x)=\beta_{0}+\beta^{\top} x=0
$$

As a distance measure for any point x to $\mathcal{L}$ we can use the following:

$$
\beta^{* \top}\left(x-x_{0}\right)=\frac{1}{\|\beta\|}\left(\beta^{\top} x+\beta_{0}\right)=\frac{1}{\left\|f^{\prime}(x)\right\|} f(x)
$$

Here $x_{0}$ is a point on $\mathcal{L}$ and $x$ is any point. By subtracting them, we get a distance vector and then we project it onto the direction of $\beta^{*}$.

If all points are completely separable by a hyperplane we can always find a function $f: \mathbb{R}^{p} \rightarrow \mathbb{R}$ so that $g_{i} f\left(x_{i}\right)>0$ for all i. In other words all instances will be classified correctly. The product of the class $g_{i} \in\{-1,1\}$ and the function result will always be positive.

We define the distance $M$ as the minimal distance of a point to the hyperplane taken over all observations. So the distance to the closest point from the hyperplane.

$$
M=\min _{i=1, \ldots, n} g_{i} f\left(x_{i}\right)
$$

Our goal is to find a hyperplane that maximizes the margin, which is $2 M$ wide (one $M$ on each side). So we end up with the following maximization problem:

$$
\max _{\beta, \beta_{0},\|\beta\|=1} M
$$

so that

$$
g_{i}\left(x_{i}^{\top} \beta+\beta_{0}\right) \geq M
$$

Put into words, we are just aiming so maximize the margin under the condition that all points are on or beyond the margin. Nothing is within it. We can re-write this further as a minimization problem to remove the constraint that $\beta$ has to be normed.

$$
\min _{\beta, \beta_{0}}\|\beta\|
$$

so that

$$
g_{i}\left(x_{i}^{\top} \beta+\beta_{0}\right) \geq 1
$$

In our distance measure before we had $\|\beta\|$ in the denominator. It has an inversely proportional relationship to the margin. The smaller $\beta$, the larger the margin. Keeping $g_{i}\left(x_{i}^{\top} \beta+\beta_{0}\right)$ greater or equal to one ensures that the instances are all on the correct side of the hyperplane.

This minimization problem is a convex optimisation problem. This means that we are looking for the minimum of a function that looks like a bowl. We cannot get stuck in a local minimum. We can use the Lagrange method to solve it. For this we have to minimize the Lagrange Primal Function:

$$
L_{p}=\frac{1}{2}\|\beta\|^{2}-\sum_{i=1}^{n} \alpha_{i}\left[g_{i}\left(x_{i}^{\top} \beta+\beta_{0}\right)-1\right]
$$

Here we minimize $\frac{1}{2}\|\beta\|^{2}$ due to mathematical convenience. Derivation is easier like this. The second part is the inequality condition which we bring into the objective function using the Lagrange multipliers $\alpha_{i}$.

Setting the derivatives of this function with respect to $\beta$ and $\beta_{0}$ to zero, results in the Lagrange dual function:

$$
L_{d}=\sum_{i=1}^{n} \alpha_{i}-\frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{i} \alpha_{j} g_{i} g_{j} x_{i}^{\top} x_{j}
$$

This now results in the final maximization problem:

$$
\max _{\alpha_{i}}\left[\sum_{i=1}^{n} \alpha_{i}-\frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{i} \alpha_{j} g_{i} g_{j} x_{i}^{\top} x_{j}\right]
$$

so that $\alpha_{i} \geq 0$ for all i.
To be optimal, we also need to satisfy the Karush-Kuhn-Tucker conditions:

$$
\begin{array}{r}
\sum_{i=1}^{n} \alpha_{i} g_{i} x_{i}=\beta \\
\sum_{i=1}^{n} \alpha_{i} g_{i}=0 \\
\alpha_{i}\left[g_{i}\left(x_{i}^{\top} \beta+\beta_{0}\right)-1\right]=0 \quad \text { for all i }
\end{array}
$$

In the non-separable case, where the data points of the two classes overlap, we introduce a so-called slack variable $\xi_{i} \geq 0$ for each side condition. Its value is the violation of the corresponding side condition. When it is positive it means that the point x is on the wrong side of the margin by the amount $M \xi_{i}$. For correctly classified points $x_{j}$ the slack variables $\xi_{j}$ are zero.

We can formulate the following minimization problem:

$$
\min _{\beta, \beta_{0}}\left[\frac{1}{2}\|\beta\|^{2}+C \sum_{i=1}^{n} \xi_{i}\right]
$$

so that

$$
\left\{\begin{array}{l}
g_{i}\left(x_{i}^{T} \beta+\beta_{0}\right) \geq 1-\xi_{i} \quad \text { for all } \mathrm{i}  \tag{1}\\
\xi_{i} \geq 0 \text { for all } \mathrm{i}
\end{array}\right.
$$

We again maximize the margin as before by minimizing $\frac{1}{2}\|\beta\|^{2}$. Then we also penalize misclassified observations by adding $C \sum_{i=1}^{n} \xi_{i}$ to the problem. Here $C$ is the cost parameter. For this problem we again have a Lagrange primal function:

$$
L_{p}=\frac{1}{2}\|\beta\|^{2}+C \sum_{i=1}^{n} \xi_{i}-\sum_{i=1}^{n} \alpha_{i}\left[g_{i}\left(x_{i}^{T} \beta+\beta_{0}\right)-\left(1-\xi_{i}\right)\right]-\sum_{i=1}^{n} \lambda_{i} \xi_{i}
$$

Again we put our minimization problem first and then we add the side conditions with Lagrange multipliers $\alpha_{i}$ and $\lambda_{i}$. After taking the derivatives with respect to $\beta, \beta_{0}$ and $\xi_{i}$, we get the following Lagrange dual function:

$$
L_{d}=\sum_{i=1}^{n} \alpha_{i}-\frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{i} \alpha_{j} g_{i} g_{j} x_{i}^{\top} x_{j}
$$

This leads to the maximization problem:

$$
\max _{\alpha_{i}}\left[\sum_{i=1}^{n} \alpha_{i}-\frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{i} \alpha_{j} g_{i} g_{j} x_{i}^{\top} x_{j}\right]
$$

so that $0 \leq \alpha_{i} \leq C$ for all i.
To be optimal, we also need to satisfy the Karush-Kuhn-Tucker conditions:

$$
\begin{gathered}
\sum_{i=1}^{n} \alpha_{i} g_{i} x_{i}=\beta \\
\sum_{i=1}^{n} \alpha_{i} g_{i}=0 \\
C=\alpha_{i}+\lambda_{i} \\
\lambda_{i} \xi_{i}=0 \\
\alpha_{i}\left[g_{i}\left(x_{i}^{\top} \beta+\beta_{0}\right)-\left(1-\xi_{i}\right)\right]=0 \\
g_{i}\left(x_{i}^{\top} \beta+\beta_{0}\right)-\left(1-\xi_{i}\right) \geq 0
\end{gathered}
$$

for all i.

## Question 11: Explain the kernel trick and kernel functions.

We can use transformations of our original data and then fit a linear model on these transformed inputs. Let $h_{m}(x)$ be the $m^{t h}$ transformation of x for M transformations. A linear basis expansion of x is defined as:

$$
H(x)=\sum_{m=1}^{M} \alpha_{m} h_{m}(x)
$$

Instead of using the function $f$ as before, we re-define it as follows:

$$
f(x)=h(x)^{T} \beta+\beta_{0}
$$

This is still a linear model in the variables $h(x)$ but these variables themselves can be non-linear transformations. The Lagrangian dual function can be written as:

$$
L_{d}=\sum_{i=1}^{n} \alpha_{i}-\frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{i} \alpha_{j} g_{i} g_{j}\left\langle h\left(x_{i}\right), h\left(x_{j}\right)\right\rangle
$$

Here $\left\langle h\left(x_{i}\right), h\left(x_{j}\right)\right\rangle$ denotes the inner product. It is important to notice that the transformations $h(x)$ only occur as an inner product. This means that there is no need to actually evaluate them. It is enough if we know a symmetric positive (semi-) definite function K , the so-called kernel function:

$$
K(u, v)=\langle h(u), h(v)\rangle
$$

The kernel function K computes the inner product in the transformed feature space without us having to first compute the transformations. The following kernel functions are important:

Linear kernel:

$$
K(u, v)=\langle u, v\rangle=u^{\top} v
$$

Polynomial kernel (degree d):

$$
K(u, v)=\left(c_{0}+\gamma\langle u, v\rangle\right)^{d} \quad \text { for constant } c_{0} \text { and with } \gamma>0
$$

Radial Basis kernel (RBF):

$$
K(u, v)=e^{-\gamma\|u-v\|^{2}} \quad \text { with } \gamma>0
$$

Sigmoid kernel:

$$
K(u, v)=\tanh \left(\gamma\langle u, v\rangle+c_{0}\right) \quad \text { for constant } c_{0} \text { and with } \gamma>0
$$

This is what the kernel trick is about. We don't choose transformations $h(x)$, which we then use in a linear model. Instead we work with the kernel functions, which directly compute the inner product in the transformed feature space.

