



TRABAJO FIN DE GRADO

DOBLE GRADO INGENIERÍA INFORMÁTICA Y MATEMÁTICAS

# Detección de anomalías basada en técnicas de ensembles

---

Biblioteca de algoritmos

**Autor**

Ignacio Aguilera Martos

**Directores**

Francisco Herrera Triguero



ESCUELA TÉCNICA SUPERIOR DE INGENIERÍAS INFORMÁTICA Y DE  
TELECOMUNICACIÓN



FACULTAD DE CIENCIAS

Granada, 5 de Septiembre de 2019





# Detección de anomalías basada en técnicas de ensembles

---

Biblioteca de algoritmos

**Autor**

Ignacio Aguilera Martos

**Directores**

Francisco Herrera Triguero



# **Detección de anomalías basada en técnicas de ensembles: Biblioteca de algoritmos**

Ignacio Aguilera Martos

**Palabras clave:** anomalía, ensamblaje, python, hics, outres, loda, mahalanobis kernel, trinity, aprendizaje automático, estadística, probabilidad, multivariante

## **Resumen**

La detección de anomalías es un ámbito de estudio que está ganando relevancia por ser una parte interesante en el tratamiento de los datos. Actualmente hacemos un manejo y un uso de los datos cada vez más voraz y creciente, necesitando no sólo técnicas que nos permitan obtener información de ellos sino además preprocesamiento de los datos que haga que estas técnicas funcionen de forma más eficiente.

Las anomalías no sólo son útiles en el preprocesamiento de los datos, también son interesantes en detección de eventos atípicos en los mismos. Por ejemplo, podemos aplicar esta detección en casos como detección de fraude en compras con tarjetas bancarias o por ejemplo en predicción de fallos en sistemas como los frenos de un coche o un camión.

Para ello en el trabajo haremos un breve repaso de cuáles son las herramientas teóricas que hacen que el trabajo de nuestros algoritmos y modelos sea consistente y funcione así como herramientas estadísticas y del ámbito de la probabilidad que explican el funcionamiento de alguno de los modelos.

Finalmente el trabajo desembocará en la implementación de algunos de los modelos del estado del arte en el ámbito de la detección de anomalías y su comparativa con modelos considerados como clásicos o tradicionales. Es decir, pondremos en contraposición los modelos de ensamblaje con los tradicionales para estudiarlos comparativamente. Asimismo veremos algunas conclusiones sobre los modelos y una propuesta de trabajo futuro con la intención de mejorar la situación actual de los modelos de ensamblaje.





# Outlier detection based in ensemble methods: Library implementation

Ignacio Aguilera Martos

**Keywords:** outlier, ensemble, python, hics, outres, loda, mahalanobis kernel, trinity, machine learning, statistics, probability, multivariate

## Abstract

Nowadays it's being more and more important the analysis of outliers in the area of data preprocessing. The way we are using the data is more and more greedy and we need better ways of mining the knowledge from the data. The use of outlier detection can lead to better performance of the Machine Learning models as we can now detect the outliers and eliminate them or treat them separately. Another approach is the detection of certain events due to the appearance of outliers. For example we can have a record of a certain bank and the credit card users. If someone gets his card stolen the way the thief buys and where the payments occur can lead to a detection of an anomalous way of using this card and therefore to inform the person that he could have his card stolen.

The anomaly detection could be useful as well in various field as medicine or event detection. We could think and measure the failure of the brake system of a truck or an earthquake as an anomaly in our datasets and we could detect them or even predict them. In medicine we could see the problem as finding what's wrong on a set of patients. We could think for example on a set of blood tests. One of them is very bad in terms of some of the values. If it is posed against healthy people the anomaly detection algorithm could give us not only the fact that the person is ill but also where the anomalous values are coming from to make it easier for the doctor to discover the problem.

The aim of this project is the discussion of ensemble models against the conventional ones in the discussion of the dilemma of meta-algorithms versus simple algorithms. This study accomplishes the task of theoretical and practical discussion of the topic as well as further conclusions towards future work.

The way we introduced the outlier detection and study on this job has been preceded by a deep study on Machine Learning and the statistics it

involves. This previous study is due to the importance of understanding why the algorithms and models implemented in this job are suitable for their use and therefore we can know as well their limits. This section has a description and introduction of the Machine Learning area and it evolves on the study of ERM and the in sample and out sample dilemma in the field. A review on bias variance tradeoff is also given in this section. We need to consider that the problem we are handling is a non-supervised problem as in the general scenario we will not have the ground truth available, this is, the labels indicating which instance is an outlier and which isn't. That's why it is important to have a review and understand that variance and bias are put in a two hand balance, if we reduce variance we increase bias and viceversa.

After this study the first concept of outlier is given based on distances and quartiles. It is not only important the way we define the outliers but also why should we consider detecting them on our datasets before getting any further work done. Criteria and possibilities are described in this section as for example the Tukey's Fences criterion which is the most used one.

Probability, and even more multivariate probability, is very important in our study. Nearly all models implemented base their working principle on density or probability estimation. For this reason I've considered getting our hands first on a multivariate introduction with useful concepts for explaining and understanding the model. This does not mean that all concepts are going to be used in the study but, those included have been useful to me in my way understanding how the theory of the models is built around. This section gets some introduction concepts of random vectors taking into account the definition and properties of random variables. It also goes through the independence concept and some characterizations involving random vectors. The most useful and interesting part of this section from the mathematical point of view is the conditional probability and conditional expectation. These concepts are relevant because they have not been introduced during the course of the degree and they are very important and related with Stochastic Processes. These concepts can apply to dynamically generated data as time series or stream flow data.

Due to this probability introduction a new outlier definition is available to us through these concepts. A probability-based definition of outlier is given and then used in several models as HICS or OUTRES. This probability definition involves probability density expectation, marginal distribution and joint distribution. This definition is not put against the distance based one, but to complement of fulfill the first definition with non trivial outliers. This concept is drawn from the OUTRES and HICS papers.

All this theory gives us way to approach the model implementation. The concept of ensemble appears here as the algorithms used in this study

are no conventional ones. As the title says, the study goes around outlier ensembles. The concept is given here as the final goal is to make a reasonable comparison between the outlier detection algorithms, those called ensembles and what we could consider as traditional or conventional. We can consider a ensemble algorithm as an algorithm that makes use of simple algorithms combining them or algorithms that make a data transformation to study the dataset in a specific way. This includes not only doing projections to make for example histograms but also the study of the data in subspaces and applying different techniques or selection mechanisms depending on the subspace. The definition is made by giving the different types of ensembles based on Charu Aggarwal's book on outlier detection and outlier ensembles.

This portfolio contains the implementation and explanation of the five models chosen: HICS, OUTRES, Trinity, Mahalanobis Kernel and LODA. They are not chosen by coincidence but trying to cover most of the types of algorithms available in the state of art of outlier ensembles. HICS and OUTRES are of the subtype of ensembles called subspace miners of subspace based. The basic explanation of them is that they try to analyze the data in certain subspaces so they can measure the density in each one of them and compare it to the rest of the instances of the dataset. HICS maintaing the point of view of choosing the subspaces with no relation or conection with the instances of the dataset while OUTRES tries the other way around, this is choosing the subspace based on the instance we are considering. Mahalanobis Kernel is a PCA-based algorithm or at least PCA-influenced as it belongs to the same category. Trinity is a meta-model or meta-algorithm, this is a algorithm that combines simple models in order to obtain a more robust algorithm. Finally I have chosen a histogram-based algorithm which is LODA. The short explanation of this type of model is the use of histograms to study the frequency of appearance of a certain value in the data.

So now we have all set up for our experiments. For the implementation Python has been chosen for several reasons. First of all Python is a versatile flexible language giving a lot of possibilities on the libraries you can use. Second we can make the development usefull for more people as Python is one of the most used languages on data science. For this reason I've decided to make myself a library with the algorithms implemented so they can be easily used by Python users and furthermore the development is completely open and available in GitHub so that anyone can see the code, understand it and fix bugs or extend the library content with new models if necessary.

All models are put against the same set of datasets given from the Stony Brooks University. This University mantains a set of datasets for outlier detection with the ground truth available so practitioners can work with it. These datasets allow us to treat the problem as a semi-supervised problem as

we can obtain at the end a percentage of accuracy. The work first executes all models on these datasets to measure the performance of the ensemble models. To compare them with the classical ones we need the implementation of those classical. For this purpose the library PyOD is used. This library contains the implementation of a lot of models including some ensemble algorithms but not the ones I've chosen. With these implementations we can compare the accuracy and times of the models over the datasets. For a better understanding of the models they are analyzed individually if necessary.

So, I have ended up with a study of the state of art of ensemble algorithms putting them against the classical approach to see who outperforms whom. Future work is also discussed at the end of this portfolio as the possibilities of improvement are still there due to the difficulty of the problem and the novelty of the ensemble techniques.

# Agradecimientos

En primer lugar me gustaría agradecer a mi tutor, Francisco Herrera Triguero por su apoyo en el desarrollo de este trabajo. Ha sido un honor poder desarrollar este trabajo con su ayuda. Igualmente me gustaría agradecerle a Jacinto Carrasco Castillo su ayuda en el desarrollo del mismo y su dedicación conmigo.

Me gustaría agradecer el apoyo también de mis padres y mi hermana quienes me han acompañado durante estos 5 años y sin los cuales no podría haber completado este camino. Gracias por ser referentes para mí y no dejarme desistir en mis momentos más bajos. Nieves, nos veremos en tu exposición de TFG antes de que te des cuenta así que aprovecha y disfruta el camino.

A mis amigos y compañeros que han seguido el mismo camino que yo y que tanto apoyo me han dado para completar estas carreras. Luis, Pablo, Antonio, Diego, Darío, Iñaki y todos los que no puedo mencionar por no hacer estos agradecimientos infinitos. Gracias a todos por ser no sólo unos compañeros si no unos verdaderos amigos. También quiero agradecer a mis amigos fuera de la carrera. Alberto, Alex, Luismi, Pablo, Carmen, Elio y todos los que me dejo en el tintero, gracias por ayudarme y darme un empujón siempre que lo he necesitado.

A mi prima María y mi primo Fran quienes también me han servido de apoyo este tiempo. A mis abuelos, Ramiro, Vicenta y María. No he podido tener unos mejores referentes que vosotros. Espero llegar a poder ser así algún día. Espero también haber cumplido vuestras expectativas sobre mí.

Y a tí, María. Gracias por hacer este camino lo más fácil posible, por tus ánimos, tu cariño y comprensión. Me has enseñado lo que es verdadero trabajo duro, perseverancia y mejorar como persona. No puedo más que agradecerte estos años juntos y espero me dejes seguir acompañándote y formando un equipo.

Gracias a todos, os quiero.



# Índice general

<b>1. Introducción</b>	<b>1</b>
1.1. Contextualización . . . . .	2
1.2. Problema a abordar y técnicas empleadas . . . . .	3
1.3. Contenido básico y fuentes . . . . .	4
1.4. Objetivos . . . . .	5
 <b>I Machine Learning y concepto de anomalía basado en distancias</b>	 <b>7</b>
 <b>2. Machine Learning</b>	 <b>9</b>
2.1. Contextualización del aprendizaje . . . . .	9
2.1.1. Objetivo del aprendizaje . . . . .	10
2.1.2. Clases de aprendizaje . . . . .	11
2.2. Principios y adaptación del aprendizaje . . . . .	12
2.2.1. Principios inductivos . . . . .	14
2.3. Regularización . . . . .	17
2.3.1. Problema de la alta dimensionalidad . . . . .	17
2.3.2. Aproximación de funciones . . . . .	20
2.3.3. Penalización o control de la complejidad . . . . .	21

2.3.4. Equilibrio entre el sesgo y la varianza . . . . .	23
2.4. Teoría estadística del aprendizaje . . . . .	26
2.4.1. Condiciones para la convergencia y consistencia del ERM . . . . .	26
2.4.2. Función de crecimiento y dimensión de Vapnik-Chervonenkis	29
2.4.3. Límites de la generalización . . . . .	32
2.4.4. Principio de minimización del error estructural (SRM)	34
2.4.5. Aproximaciones de la dimensión VC . . . . .	35
2.4.6. Perspectiva . . . . .	36
<b>3. Concepto de anomalía</b>	<b>37</b>
3.1. Contextualización . . . . .	37
3.2. Criterios . . . . .	38
3.3. Qué hacer con las anomalías . . . . .	40
<b>II Introducción de Estadística Multivariante y concepto probabilístico de anomalía</b>	<b>41</b>
<b>4. Introducción de Estadística Multivariante</b>	<b>45</b>
4.1. Introducción . . . . .	45
4.1.1. Independencia . . . . .	47
4.1.2. Probabilidad y esperanza condicionada . . . . .	48
4.1.3. Desigualdades y fórmulas famosas . . . . .	53
<b>5. Concepto probabilístico de anomalía</b>	<b>57</b>



<b>III Explicación de los modelos y análisis de resultados</b>	<b>61</b>
<b>6. Modelos implementados</b>	<b>63</b>
6.1. Algoritmos de ensamblaje . . . . .	63
6.2. Mahalanobis Kernel . . . . .	64
6.3. TRINITY . . . . .	67
6.4. OUTRES . . . . .	71
6.5. HICS . . . . .	79
6.6. LODA . . . . .	86
6.7. Implementación . . . . .	90
<b>7. Experimentación y Resultados</b>	<b>93</b>
7.1. Conjuntos de datos . . . . .	93
7.2. Experimentación . . . . .	95
7.3. Resultados . . . . .	96
7.4. Conclusiones y trabajo futuro . . . . .	137
<b>Bibliografía</b>	<b>144</b>



# Capítulo 1

## Introducción

Antes de comenzar el objeto de estudio de este trabajo, lo primero que debemos hacer es contextualizar el mismo y establecer un marco de trabajo en cuanto a teoría que se empleará en la posterior experimentación y desarrollo del mismo.

El estudio realizado y plasmado en este trabajo se centra en la obtención de técnicas para la detección de anomalías en conjuntos de datos, concepto que introduciremos posteriormente. En concreto las técnicas que se van a desarrollar son las conocidas como técnicas ensemble o de ensamblaje que se basan en el estudio del problema o bien combinando modelos existentes o bien haciendo un estudio pormenorizado aplicando algún criterio por subespacios del conjunto de datos.

En primer lugar el trabajo desarrollará una introducción a la teoría de aprendizaje y resolución de problemas mediante datos y no por diseño así como la teoría matemática que esto involucra. Esta primera sección nos dará suficiente estructura al trabajo para poder definir en términos de distancias lo que significa que una instancia de un conjunto de datos sea una anomalía.

Posteriormente se desarrollará brevemente algunos conocimientos estadísticos básicos de estadística multivariante para poder introducir el concepto de anomalía desde la perspectiva de las probabilidades condicionadas.

Tras esto podremos entrar en el terreno de la experimentación, desarrollo y explicación de técnicas y puesta en contraste con los algoritmos clásicos para comprobar el desempeño de las nuevas técnicas.

Por último se presentarán las conclusiones obtenidas tras todo este estudio.

## 1.1. Contextualización

En este contexto y sin haber comenzado la discusión del problema podríamos considerar el establecimiento de una solución al problema de detección de anomalías empleando un algoritmo preciso y óptimo, aunque costoso en tiempo, pero esta solución no es viable en este contexto. Pensemos por un momento en cómo detectar una anomalía en un conjunto de datos. Para poder dar un algoritmo concreto que resuelva siempre el problema de forma óptima tenemos que estar seguros de que somos capaces de definir de forma clara y para todo conjunto de datos cuándo estamos en presencia de un dato anómalo. Pero, ¿sabemos exactamente cuándo sobrepasamos la barrera de dato ligeramente desviado, ruido o una anomalía?

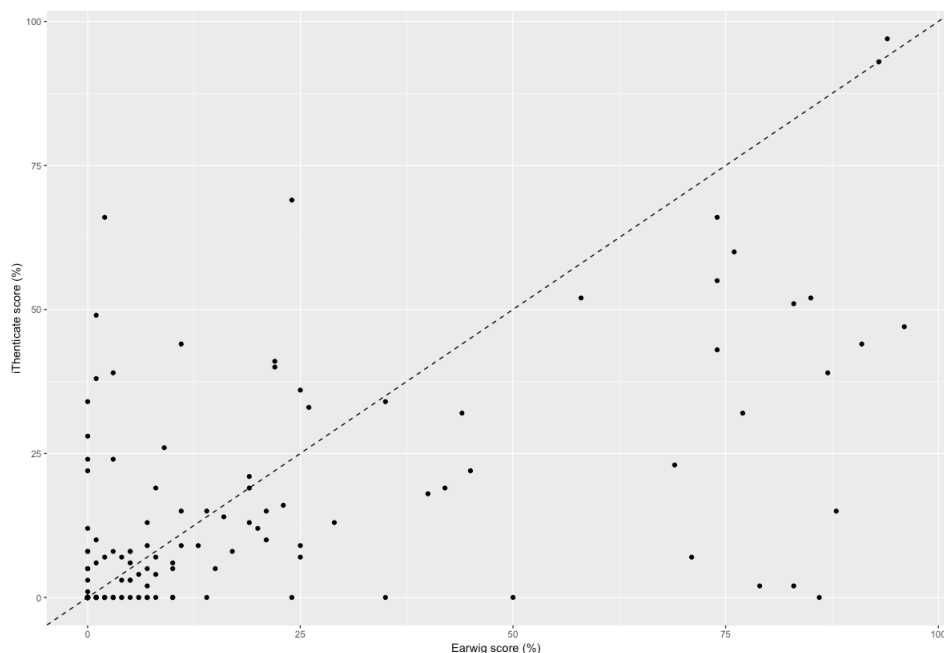


Figura 1.1: Ejemplo de conjunto de datos (Wikimedia)

Pensemos por ejemplo en este conjunto de datos. Tenemos un clúster muy bien definido en la esquina inferior izquierda y datos dispersos. ¿Podemos afirmar claramente cual es la línea que distingue los datos anómalos de los normales?

Esta discusión nos lleva a la primera barrera que tenemos que superar en este trabajo. El problema no es resoluble por diseño y por tanto debemos realizar una aproximación a través de los datos. Esto nos va a llevar a aprender de los mismos, valorar cada dato con una puntuación que nos acabará discriminando los datos normales y anómalos.

En el contexto de los problemas resueltos a través de los datos tenemos dos tipos: clasificación y regresión.

Podríamos pensar que estamos ante un problema de clasificación ordinario, es decir, aprender a través de los datos de entrenamiento cuáles son las anomalías y cuáles los datos normales pero no es así. Pensemos que no sabemos ni siquiera nosotros clasificar claramente estas anomalías salvo en algunos ejemplos prácticos. Por ejemplo si le diéramos a una persona un conjunto de datos ya establecido como el que hemos visto anteriormente ?? no sería nada fácil e incluso no podemos afirmar que sepamos hacer esta tarea. Por contra si el conjunto de datos es generado en un proceso de trabajo, por ejemplo un conductor de camiones haciendo su ruta, podemos saber cuándo hay una anomalía porque el trabajador la está viviendo y puede señalarla.

Por tanto este problema no es de clasificación al uso pues no es un problema supervisado. Esto significa que, en general no vamos a tener un conjunto etiquetado en el que poder probar cómo aprende nuestro modelo y tendremos que abordar otras técnicas para comprobar el desempeño.

Ahora que comprendemos el alcance del problema podemos intentar profundizar un poco más en la base teórica del mismo analizando las herramientas que el Machine Learning nos provee para abordarlo.

## 1.2. Problema a abordar y técnicas empleadas

Este trabajo va a estar enfocado en el estudio de las anomalías, en concreto, empleando lo que se conocen como técnicas de ensamblaje o algoritmos de ensamblaje. Para ello vamos a dar un marco inicial sobre aprendizaje automático, pues estos algoritmos se basan en los principios de funcionamiento del mismo.

El objetivo final de esta memoria será la implementación de cinco modelos de ensamblaje: HICS, OUTRES, Trinity, LODA y Mahalanobis Kernel. Estos algoritmos no han sido escogidos al azar, si no con la intención de cubrir el máximo de tipos posibles en cuanto a algoritmos de ensamblaje e intentando tomar aquellos que según la literatura obtienen el mejor resultado (estado del arte o “state of art”).

Con estos modelos podremos hacer una comparativa entre lo que se conoce como modelos clásicos y nuestros modelos implementados de ensamblaje, tanto en tiempo como en porcentaje de acierto sobre una serie de conjuntos de datos de los que se dispone información sobre las anomalías.

Con todo esto veremos que hay ideas interesantes en todos los modelos que pueden ser aprovechadas así como los tipos de algoritmos de ensamblaje que resultan ser más exitosos. Esto nos permitirá dar resultados robustos sobre los modelos y además recopilar una serie de ideas que podrían llevar al desarrollo de un modelo original propio que las aglomere.

Para el desarrollo de este trabajo se ha necesitado una base importante de aprendizaje automático. La base teórica de esta rama de la informática y de las matemáticas sustentará el éxito que podemos sacar de los modelos, así como marcar el límite que podemos obtener en cuanto al rendimiento de los mismos. Los modelos están ampliamente basados en técnicas probabilísticas de estadística multivariante por lo que será necesario una introducción de este campo incorporando sobre el temario de la carrera las nociones de vector aleatorio, esperanza condicionada a eventos y  $\sigma$ -álgebras y probabilidades condicionadas a eventos y  $\sigma$ -álgebras.

Para la implementación se ha empleado Python creando clases para cada modelo, por lo que se ha utilizado el conocimiento adquirido en asignaturas como Programación y Diseño Orientado a Objetos. Se ha utilizado para el desarrollo la librería NumPy, Sklearn y SciPy así como la librería PyOD que implementa los modelos clásicos de detección de anomalías.

### 1.3. Contenido básico y fuentes

El trabajo contiene una primera sección en la que se incluye una introducción de Aprendizaje Automático orientado específicamente a nuestro problema. Para ello primero se hace una contextualización del concepto de aprendizaje así como los principios inductivos que guían el mismo hacia un buen resultado como por ejemplo el ERM o minimización del error empírico. Se aportan también algunas reflexiones y conceptos en cuanto a la aproximación de funciones, que no es más que el objetivo del aprendizaje automático.

Todos estos conocimientos están basados en la teoría estadística de Vapnik y Chervonenkis que es brevemente repasada y en la que se dan cotas sobre el aprendizaje y su rendimiento. Esta introducción ha sido escrita basándose en tres libros: Learning from Data de Yaser Abu-Mostafa [7], Learning from Data de Cherkassky y Mulier [2] y Outlier Ensembles de Aggarwal y Sathe [43].

Este marco nos dirige hacia la primera definición del concepto de anomalía que está basada en distancias y rangos intercuartil que se describen en el libro Outlier Analysis [44].

Para dar una definición alternativa y una buena introducción para los modelos debemos hacer una breve introducción estadística. En esta introducción se define un vector aleatorio así como su función de densidad, su función característica y su función de distribución. Se refieren los conceptos de independencia y probabilidad y esperanza condicionada. Por último y aprovechando este contexto se enuncian y demuestran algunas desigualdades y fórmulas famosas. Este contenido viene dado por los apuntes de la asignatura Estadística Multivariante del grado en Matemáticas, los apuntes de la asignatura Procesos Estocásticos del grado en Matemáticas y el libro Probability Theory de M. Loève [49].

Tras esto puede ser introducido el concepto probabilístico y basado en densidad de una anomalía. Este concepto viene apoyado en el paper [4] que describe el algoritmo HICS.

Con los dos conceptos de probabilidad y el marco teórico ya planteado se introducen los modelos implementados y el concepto de algoritmos de ensamblaje. Estos conceptos sobre los algoritmos vienen de los libros Outlier Analysis [44] y Outlier Ensembles [43]. Se aporta en esta sección la explicación teórica de cada modelo así como la implementación desarrollada por mí mismo en Python. Los artículos en los que se basa cada algoritmo son [4], [43], [31] y [24].

Finalmente se analiza el comportamiento de todos los modelos en la sección de resultados frente a los algoritmos considerados como clásicos. Se aportan conclusiones tras todo el trabajo y, al haber margen de mejora, se aportan algunas ideas que podrían aplicarse en un futuro para desarrollar un modelo propio.

## 1.4. Objetivos

Por todo lo descrito anteriormente el trabajo tiene los siguientes objetivos claros:

- Desarrollar un marco teórico sobre el aprendizaje en problemas de clasificación y problemas no supervisados o semi-supervisados.
- Estudiar el estado del arte de los algoritmos de ensamblaje.
- Estudiar la teoría estadística que rodea los algoritmos de ensamblaje.
- Entender los fundamentos teóricos y el funcionamiento de los modelos implementados.

- Desarrollar una implementación de los modelos.
- Obtener una comparativa entre los modelos clásicos y los de ensamblaje.

Todos estos objetivos han sido alcanzados en el desarrollo de este estudio, obteniendo además algunas ideas nuevas que pudieran ser la base de un modelo propio.



## Parte I

# Machine Learning y concepto de anomalía basado en distancias



## Capítulo 2

# Machine Learning

En este capítulo vamos a hacer un repaso sobre los conceptos asociados al Machine Learning, el aprendizaje y la teoría matemática que involucra. Estas herramientas y conceptos los utilizaremos posteriormente para resolver el problema de detección de anomalías. El contenido de esta sección se ha basado en varios libros y artículos, pero principalmente el contenido ha sido extraído de los libros: Learning from Data de Yaser Abu-Mostafa [7], Learning from Data de Cherkassky y Mulier [2] y Outlier Ensembles de Aggarwal y Sathe [43].

### 2.1. Contextualización del aprendizaje

Para comenzar tenemos que empezar definiendo en que consiste el proceso de aprender sobre unos datos. Supongamos que tenemos un problema en el que tenemos una entrada y una salida, por ejemplo una entrada válida podría ser un vector  $x \in \mathbb{R}^d$  y una salida un valor real o un número natural. El problema de aprendizaje intenta estimar una estructura de tipo entrada-salida como la descrita usando únicamente un número finito de observaciones.

Podemos definirlo de forma más general empleando tres conceptos:

- **Generador:** El generador se encarga de obtener las entradas  $x \in \mathbb{R}^d$  mediante una distribución de probabilidad  $p(x)$  desconocida y fijada de antemano.
- **Sistema:** El sistema es el que produce la salida “y” (correcta) para cada entrada  $x \in \mathbb{R}^d$  mediante la distribución de probabilidad  $p(x|y)$

desconocida y fijada de antemano.

- Máquina de aprendizaje: esta es la que va a obtener información de las entradas y salidas conocidas para intentar predecir la salida correcta para una entrada nueva que se nos de. De forma abstracta esta máquina lo que hace es tomar una serie de funciones de un conjunto general de forma que para una entrada dada  $x$  la función  $f(x, \omega)$  con  $\omega \in \Omega$  nos de la salida que corresponde para  $x$  donde  $\omega$  es una forma de indexar las funciones tomadas para generalizar la salida del conjunto más general de funciones que hemos indicado.

El único cabo que hemos dejado sin atar en las definiciones que acabamos de ver es el conjunto de funciones del cual tomaremos algunas para adaptar la máquina de aprendizaje a los datos recibidos. Este conjunto de funciones, que notaremos como  $\mathcal{H}$ , es de momento la única forma que tenemos de aplicar un conocimiento a priori en la máquina de aprendizaje.

Para finalizar esta breve introducción y poder continuar profundizando vamos a exponer algunos ejemplos de clases de funciones para que podamos visualizar el contexto.

- Funciones lineales: En este caso la clase de funciones  $\mathcal{H}$  está formada por funciones de la forma  $h(x) = w_0 + \sum_{i=1}^d x_i w_i$  donde  $w \in \mathbb{R}^{d+1}$ . Este es el modelo de funciones más clásico.
- Funciones trigonométricas: Un ejemplo de una clase de funciones trigonométricas podría ser  $f_m(x, v_m, w_m) = \sum_{j=1}^{m-1} (v_j \sin(jx) + w_j \cos(jx)) + w_0$  donde en este caso la entrada es un único valor real. Este tipo de clases de funciones serán útiles en problemas de regresión que luego explicaremos con algo más de detalle.

### 2.1.1. Objetivo del aprendizaje

Cuando hablamos de aprendizaje nos referimos a que queremos obtener una cierta información a partir de los datos de que disponemos. Como ya se ha mencionado, intentamos obtener una función de una familia de funciones que aproxime o modele de buena manera la salida del sistema. Por tanto, ese es nuestro objetivo: obtener una función de la familia de funciones que minimice el error.

El problema que enfrentamos es que sólo disponemos de un número finito, por ejemplo  $n$ , de observaciones de datos y su correspondiente salida. Esto

nos va a hacer que no podamos tener una garantía de optimalidad a no ser que hagamos tender  $n$  a infinito.

Sin embargo si que podemos cuantificar cómo de buena es una aproximación con respecto a otra mediante la función pérdida o error que denotaremos como  $L(y, f(x, \omega))$ . Esta función nos va a medir la diferencia entre la salida real del sistema y la salida dada por la función  $f$  para la entrada  $x$  siendo siempre  $L(y, f(x, \omega)) \geq 0$ .

Recordemos además que el Generador obtiene datos mediante una distribución desconocida pero fijada de antemano y que son independientes e idénticamente distribuidos con respecto a la distribución conjunta, es decir:

$$p(x, y) = p(x)p(y|x)$$

Una vez definido todo esto podemos obtener el valor esperado de pérdida o error mediante el funcional

$$R(\omega) = \int L(y, f(x, \omega))p(x, y)dxdy$$

Ahora podemos concretar un poco más lo que entendemos como objetivo del aprendizaje. El objetivo será encontrar una función  $f \in \mathcal{H}$  que nos minimice el valor del funcional  $R(\omega)$ . Pero recordemos que  $p(x, y)$  es desconocida para nosotros, por lo que no podemos saber cómo se distribuyen los datos y por tanto el valor del funcional no es calculable para nosotros y por tanto la solución puramente de cálculo no es accesible.

Por tanto, la única forma realmente potente y útil de encontrar una buena aproximación será incorporar el conocimiento a priori que tenemos del sistema. En la sección anterior hemos visto que una forma de incorporar dicho conocimiento es mediante la selección de la clase de funciones, pero además será muy relevante el hecho de cómo los datos son empleados en el proceso de aprendizaje. En este apartado de decisión tendremos que resolver primero la codificación de los datos, el algoritmo empleado y el uso de técnicas como la regularización que veremos después para incorporar nuestro conocimiento en el camino que nos lleve a la solución.

### 2.1.2. Clases de aprendizaje

El problema de aprendizaje puede ser subdividido a su vez en cuatro clases distintas y que se suelen abordar de forma independiente. Estos tipos

de problemas de aprendizaje son:

- **Clasificación:** El problema de clasificación consiste en identificar y separar instancias de datos según su clase. Por ejemplo podemos dividir a la población mundial en dos clases: sanos y enfermos. Un problema de clasificación podría ser saber identificar estas clases para un conjunto de personas. Los problemas de clasificación más sencillos son aquellos en los que se usan dos únicas clases aunque se puede generalizar la definición del problema a  $k$ -clases.
- **Regresión:** El problema de regresión consiste en estimar una función  $f : \mathbb{R}^n \rightarrow \mathbb{R}$  a partir de una serie de muestras previas con los valores de  $f$ . Un problema de regresión podría ser determinar la función que, dados los datos de altura y dimensiones corporales sea capaz de darnos el peso aproximado de la persona.
- **Estimación de la función de densidad:** en este caso no nos interesa la salida que proporciona el sistema, ya sea el valor de una clase o una función real como en el caso de la regresión. En este caso el objetivo del aprendizaje es conseguir la función de densidad  $f(x, \omega)$ , con  $\omega \in \Omega$  los parámetros necesarios de la función de densidad, con la que se distribuyen los datos de entrada del sistema.
- **Agrupamiento y cuantificación vectorial:** El problema de cuantificación vectorial consiste en intentar explicar la distribución de los vectores de entrada mediante puntos clave llamados centroides. De esta forma se podría reducir la complejidad de los datos expresándolos en función de un sistema de generadores menor. El problema de agrupamiento tiene también relación por utilizar la idea de centroide, pero el objetivo es completamente distinto. El objetivo del problema de agrupamiento es intentar conseguir agrupar los datos en clústeres, es decir, regiones del espacio en las que se concentran un conjunto de datos. De esta forma intentamos agrupar los datos que mantienen una relación entre sí. Un ejemplo de un problema de cuantificación vectorial podría ser un problema de reducción de dimensionalidad y un ejemplo de problema de agrupamiento podría ser identificar instancias de datos con características comunes.

## 2.2. Principios y adaptación del aprendizaje

Según Vapnik [1] la predicción mediante el aprendizaje se puede dividir en dos fases:

1. Aprendizaje o estimación a partir de una muestra.
2. Predicción a partir de las estimaciones obtenidas.

Estas dos fases se corresponden con los dos tipos de inferencia clásica que conocemos, esto es, inducción y deducción. Traído a este caso el proceso de inducción es aquel que a partir de los datos de aprendizaje o los datos de la muestra que tenemos con la salida que corresponde podemos estimar un modelo. Es decir, estamos sacando el conocimiento de los datos para generar el modelo. El proceso de deducción es aquel que, una vez obtenido el modelo estimado (la generalización) obtenemos una predicción de la salida sobre un conjunto de datos.

Por contra, Vapnik propone un paso que resuelve estas dos fases directamente y que él denomina transducción. Este paso consiste en, dados los datos de entrenamiento obtenemos directamente los valores de salida sin tener que hacer la generalización a un modelo. De esta forma, según Vapnik, podríamos reducir el error que cometemos en la predicción. Este razonamiento tiene sentido, pues estamos omitiendo el paso más complejo del proceso de inducción-deducción.

En resumen esta idea se puede resumir en la siguiente figura:

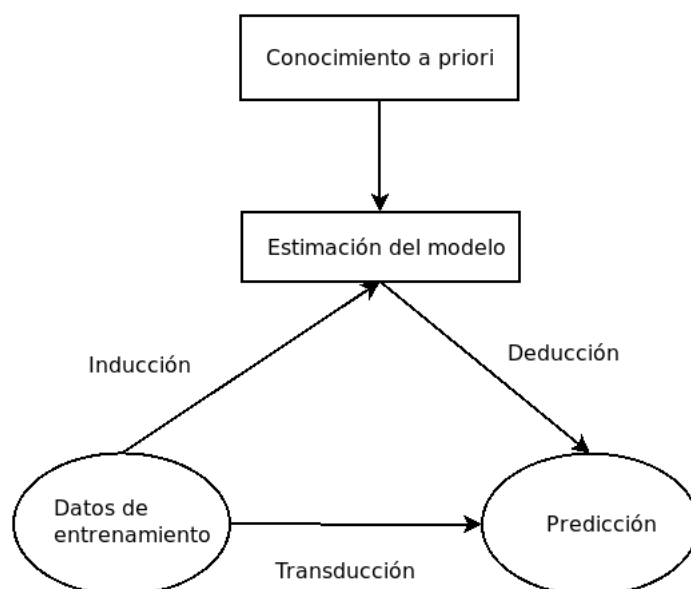


Figura 2.1: Tipos de inferencia y transducción [2, p. 41]

Podemos ver que el conocimiento a priori que tenemos del problema se manifiesta una vez se crea el modelo general, de forma que se emplearía en

el paso de la inducción. Ya hemos hablado previamente del conocimiento a priori y cómo incorporarlo al modelo, pero por concretar un poco más podemos añadirlo básicamente de dos formas:

- Escogiendo un conjunto de funciones para aproximar la salida del sistema
- Añadiendo restricciones o penalizaciones adicionales a dicho conjunto de funciones.

En resumen, para poder crear la generalización del modelo de forma única necesitamos:

1. Un conjunto de funciones para aproximar la salida.
2. Conocimiento a priori.
3. Un principio inductivo, que no es más que una indicación de cómo emplear los datos para llegar a la generalización del modelo.
4. Un método de aprendizaje, es decir, una implementación del principio inductivo.

En secciones posteriores revisaremos algunos de los principios inductivos más usados pero es importante reseñar la diferencia entre principio inductivo y método de aprendizaje. Para un mismo principio inductivo podemos tener varios métodos de aprendizaje, pues podemos escoger diferentes formas de llevarlo a la práctica. Por ejemplo, uno de los principios inductivos más empleados es el ERM o Empirical Risk Minimization, es decir, minimización del error empírico. Podríamos pensar en diferentes formas de utilizar este principio, por ejemplo sólo avanzamos en la creación del modelo si a cada paso que demos minimizamos el error, o por ejemplo vamos avanzando varios modelos a la vez hasta obtener un número de modelos finales de entre los cuales escogeremos aquel que mejor minimice dicho error.

### 2.2.1. Principios inductivos

Una vez introducido el concepto como hemos hecho en la sección anterior vamos a hacer un breve repaso de los principios más usados y en qué consiste cada uno de ellos.



## Penalización o Regularización

Imaginemos que tenemos una clase de funciones muy flexible, esto es con un gran número de parámetros libres  $f(x, \omega)$  con  $\omega \in \Omega$ . Vamos a partir de la base del ERM, es decir, minimizar el error empírico. La penalización lo que va a hacer es añadir un factor a la función a minimizar:

$$R_{pen}(\omega) = R_{emp}(\omega) + \lambda \phi[f(x, \omega)]$$

Donde  $R_{emp}(\omega)$  es el error empírico con los parámetros  $\omega$  y  $\phi[f(x, \omega)]$  es un funcional no negativo asociado a cada estimación  $f(x, \omega)$ . El parámetro  $\lambda > 0$  es un escalar que controla el peso de la penalización.

El funcional  $\phi[f(x, \omega)]$  puede medir lo que creamos conveniente que debemos añadir, es decir, aquí podemos añadir a la minimización algún tipo de medida que nos diga cómo de bien funciona el ajuste de los datos y cómo de bien funciona la información a priori que hemos incluido en el modelo. Pensemos por ejemplo que  $\lambda$  fuera un parámetro con un valor muy alto. En este caso la penalización por un mal ajuste de los datos no sería de gran importancia pues lo más conveniente sería minimizar el valor del funcional para no obtener una gran penalización. De esta forma podemos ajustar y dar un poco más de información al error empírico. Por ejemplo, en función del problema, es posible medir la complejidad de la solución mediante el funcional  $\phi$  y de esta forma no sólo vamos a obtener una función que ajuste bien los datos, si no que también mantenga una cierta simplicidad para evitar por ejemplo el sobreajuste.

## Reglas de parada anticipada

Pensemos en un método que vaya aprendiendo de los datos de forma iterativa intentando a cada iteración reducir el error cometido, por ejemplo el ERM. Los métodos o reglas de parada anticipada pueden verse como penalizaciones sobre el algoritmo conforme se va ejecutando. Las reglas de parada anticipada, como su nombre indica lo que prevén es la parada del algoritmo antes de obtener su objetivo teórico. Por ejemplo un algoritmo intenta que el error sea menor que  $10^{-6}$  pero para reducirlo desde  $10^{-4}$  hasta  $10^{-5}$  está consumiendo millones de iteraciones. Si queremos que el tiempo de cómputo penalice lo que podemos hacer es fijar por ejemplo un número máximo de iteraciones que detenga el método aunque no se haya alcanzado esa barrera de error que se preveía.

### Minimización del riesgo estructural o SRM

Para entender esta filosofía nos ponemos en la situación de que ya sabemos la clase de funciones con la que vamos a aproximar la salida del sistema, por ejemplo hemos escogido la clase de funciones polinómicas. Bajo esta clase de funciones podemos ordenar las funciones por complejidad, entendiendo por complejidad el número de parámetros de la función. Por ejemplo los polinomios de grado  $m$  son de menor complejidad que los de grado  $m + 1$ . De esta forma podemos pensar en una estructura de la clase de funciones de la forma:

$$S_0 \subset S_1 \subset S_2 \subset \dots$$

Este parámetro de complejidad también puede ser un principio a minimizar para intentar conseguir una solución adecuada pero también simple. La generalización de la medida de complejidad para las clases de funciones es la conocida como dimensión VC o dimensión de Vapnik-Chervonenkis.

### Inferencia Bayesiana

Este principio inductivo se utiliza en el problema de estimación de la función de densidad. El principio es utilizar la conocida fórmula de Bayes para hacer una estimación de la función de densidad empleando el conocimiento a priori que disponemos del problema. La forma en la que se emplea esta fórmula es de la siguiente:

$$P[\text{modelo}|\text{datos}] = \frac{P[\text{datos}|\text{modelo}] \cdot P[\text{modelo}]}{P[\text{datos}]}$$

, donde  $P[\text{modelo}]$  es la probabilidad a priori,  $P[\text{datos}]$  es la probabilidad de los datos de entrenamiento y  $P[\text{datos}|\text{modelo}]$  es la probabilidad de que los datos estén generados por el modelo.

### Descripción de mínima longitud

La idea de este principio es la minimización de la longitud que se necesita emplear para describir un modelo y la correspondiente salida. Llamamos  $l$  a la longitud total:

$$l = L(\text{modelo}) + L(\text{datos}|\text{modelo}).$$

Esta medida puede ser vista como una medida de complejidad conjunta de todo el modelo.

## 2.3. Regularización

Por la importancia de este principio inductivo vamos a desarrollarlo un poco más, junto con el concepto de penalización, la selección de los modelos y la relación entre sesgo y varianza. Este último es un concepto muy relevante en cuanto al aprendizaje y que en nuestro caso, al no poseer la clasificación real tendremos que tenerlo en cuenta.

### 2.3.1. Problema de la alta dimensionalidad

Sabemos que cuando estamos ante un problema de aprendizaje nuestro objetivo es conseguir estimar una función con un número finito de instancias de una muestra ya con la salida. Al tener un número finito de elementos en la muestra ya sabemos que no podemos garantizar que la respuesta sea la óptima o correcta, pero además debemos pensar que a mayor regularidad del conjunto de funciones empleado debemos tener una densidad suficiente de puntos para compensar dicha regularidad. Este problema es conocido como la maldición de la dimensionalidad (curse of dimensionality). El problema es que cuanto mayor sea la dimensionalidad considerada más difícil es poder tener esa alta densidad de datos que se requieren para funciones muy regulares.

Este problema que conlleva la alta dimensionalidad proviene de la geometría de los espacio con alta dimensionalidad. A medida que incrementamos la dimensionalidad el espacio se ve cada vez con más aristas o picos. Podemos pensar en un cubo para el espacio tridimensional y a medida que aumentamos la dimensión incorporamos más aristas y vértices. Podemos resumir en 4 propiedades de los espacio con alta dimensionalidad que causan este problema:

1. La densidad disminuye exponencialmente al aumentar el número de dimensiones. Supongamos que tenemos una muestra de  $n$  puntos en  $\mathbb{R}$ . Para poder tener la misma densidad en un espacio  $d$ -dimensional  $\mathbb{R}^d$  necesitamos  $n^d$  puntos.

2. Cuanto mayor dimensionalidad tenga el conjunto de datos mayor lado se necesita para que un hipercubo contenga el mismo porcentaje del conjunto que con una menor dimensionalidad. Imaginemos que tenemos un conjunto  $d$ -dimensional en el que tenemos la muestra dentro de un hipercubo unidad. Si quisiéramos abarcar un porcentaje  $p \in [0, 1]$  necesitaríamos un cubo de lado  $e_d(p) = p^{1/d}$ . Como se puede observar a mayor dimensionalidad y  $p$  constante el lado es cada vez mayor. Esta idea es fácilmente entendible si observamos la siguiente figura:

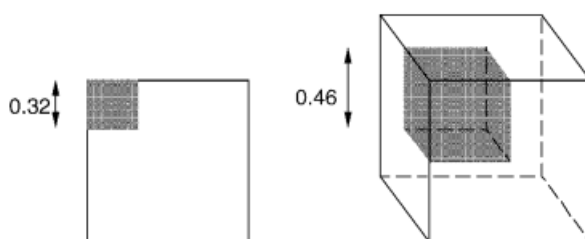


Figura 2.2: Para 2 dimensiones necesitamos menor lado que para 3 dimensiones. [2, p. 64]

3. Casi todo punto está más cerca de un borde que de otro punto. Pensemos en un conjunto de datos con  $n$  puntos distribuidos de forma uniforme en una bola  $d$ -dimensional de radio unidad. Para este conjunto de datos, según Hastie [3], la distancia media entre el centro de la distribución y los puntos más cercanos a dicho centro se mide bajo la fórmula:

$$D(d, n) = \left(1 - \frac{1}{2}^{1/n}\right)^{1/d}$$

Si en esta fórmula tomamos por ejemplo  $n = 200$  y  $d = 10$  el resultado es  $D(10, 200) \approx 0.57$ . Esto significa que los puntos más cercanos al centro de la distribución están más cerca de los bordes que del centro.

4. Casi todo punto es una anomalía sobre su propia proyección. Si pensamos de nuevo en la idea de los vértices y aristas en espacio de alta dimensionalidad y pensamos en que, según el punto anterior, cada vez que aumenta la dimensionalidad los puntos están más cerca de los bordes entonces no es extraño pensar que los puntos a medida que aumenta la dimensionalidad están más distantes del resto de puntos. Esto intuitivamente (ya que aún no hemos visto la definición formal de anomalía) nos guía a pensar que vistos los puntos en sus propios entornos éstos serán anomalías comparados con el resto.



Figura 2.3: Forma conceptual de un espacio de alta dimensionalidad.[2, p. 64]

Conceptualmente podemos imaginarlo con esta forma de picos, con lo que si tenemos los datos apiñados en dichos picos o extremos el resto de datos que estén en picos diferentes distan tanto del que estamos considerando que no podemos afirmar que tengan ninguna relación entre sí.

Estos puntos hemos de recordar que van referidos al conjunto de datos y no a las funciones que estamos considerando para representar la salida del sistema. Si estamos considerando la complejidad de las funciones la dimensionalidad no es una buena medida. Sabemos de la existencia de teoremas de aproximación de funciones como por ejemplo el Teorema de Superposición de Kolmogorov-Arnold.

### **Teorema 2.1 (Teorema de Superposición de Kolmogorov-Arnold)**

Sea  $f$  una función continua de varias variables  $f : X_1 \times \dots \times X_n \rightarrow \mathbb{R}$ , entonces existen funciones  $\Phi_q : \mathbb{R} \rightarrow \mathbb{R}$  y  $\phi_{q,p} : X_p \rightarrow [0, 1]$  tales que  $f$  se puede expresar como:

$$f(x) = f(x_1, \dots, x_n) = \sum_{q=0}^{2n} \Phi_q \left( \sum_{p=1}^n \phi_{q,p}(x_p) \right)$$

Este Teorema argumenta perfectamente que la complejidad que le damos a los datos por tener una alta dimensionalidad no es transferible a las funciones pues podemos expresar funciones de varias variables como combinación de funciones de una sola variables. En otras palabras no podemos argumentar que la complejidad de funciones univariantes sea mayor o menor que la de funciones multivariantes.

### 2.3.2. Aproximación de funciones

Como ya hemos dicho en la introducción queremos aproximar una función salida del sistema dentro de una familia de funciones. Este campo no es nuevo, tenemos como herramientas una serie de Teoremas relacionados con la aproximación de funciones como el Teorema de Kolmogorov enunciado anteriormente o el Teorema de aproximación de Weierstrass.

La versión más simple del Teorema de Weierstrass es la de funciones reales definidas en intervalos cerrados, veamos un repaso de estos Teoremas para hacer un esquema de la aproximación de funciones.

**Teorema 2.2 (Teorema de aproximación de Weierstrass)** *Supongamos que  $f : [a, b] \rightarrow \mathbb{R}$  es una función continua. Entonces  $\forall \epsilon > 0$ ,  $\exists p$  un polinomio tal que  $\forall x \in [a, b]$  tenemos que  $|f(x) - p(x)| < \epsilon$ .*

En otras palabras, podemos aproximar las funciones continuas reales definidas en un intervalo cerrado con el error que queramos en un punto mediante polinomios. Además tenemos versiones más generales aún como el Teorema de Stone-Weierstrass para funciones reales, para espacios localmente compactos y para el espacio de los complejos.

Estas aproximaciones son más sencillas en términos de la complejidad de la clase de funciones, pero tenemos aproximaciones muy famosas, como por ejemplo la serie de Fourier.

**Definición 2.1 (Serie de Fourier)** *Si tenemos una función  $f : \mathbb{R} \rightarrow \mathbb{R}$  integrable en el intervalo  $[t_0 - \frac{T}{2}, t_0 + \frac{T}{2}]$  entonces se puede obtener el desarrollo en serie de Fourier de  $f$  en dicho intervalo. Si  $f$  es periódica en toda la recta real la aproximación será válida en todos los valores en los que esté definida.*

$$f(t) \approx \frac{a_0}{2} + \sum_{n=1}^{\infty} [a_n \cos(\frac{2n\pi}{T}t) + b_n \sin(\frac{2n\pi}{T}t)]$$

Donde  $a_0, a_n$  y  $b_n$  son los coeficientes de la serie de Fourier que tienen la forma:

$$a_0 = \frac{2}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} f(t) dt$$

$$a_n = \frac{2}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} f(t) \cos\left(\frac{2n\pi}{T}t\right) dt$$

$$b_n = \frac{2}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} f(t) \sin\left(\frac{2n\pi}{T}t\right) dt$$

Como podemos ver hemos introducido dos conocidas formas de aproximar funciones, una con funciones polinómicas y otra con funciones trigonométricas. Vamos a dividir en dos los tipos de aproximación que podemos tener para el problema de aprendizaje.

1. Aproximaciones universales: son aquellas en las que se establece que cualquier función continua puede ser aproximada por otra función de otra clase con el error que queramos. En este grupo podríamos meter a los dos teoremas que hemos dado previamente. Dentro de este grupo podemos tener diferentes tipos de aproximaciones en función de la familia de funciones que escojamos como aproximaciones. Por ejemplo en los dos teoremas previos hemos cogido las clases de funciones polinómicas y trigonométricas pero podríamos haber tomado otras clases diferentes.
2. Aproximaciones inexactas: son aquellas en las que no podemos tener una aproximación como las que hemos dado en los teoremas previos, si no que proveen de una aproximación de peor calidad.

### 2.3.3. Penalización o control de la complejidad

Ya hemos discutido brevemente en la sección de principios inductivos la complejidad y cómo penalizarla. Vamos a ver qué elementos queremos controlar con la penalización:

1. La clase de funciones con la que vamos a hacer la aproximación. Tenemos que decidir si escoger una clase tan amplia que nos aseguremos que abarque la solución seguro pero penalicemos la complejidad de la elección o queremos una clase de funciones más ajustada.
2. Tipo de funcional de penalización. Tenemos que escoger entre los distintos tipos de penalización que queremos. Esto se reduce a escoger entre dos tipos de penalización: paramétrica y no paramétrica. La primera de ellas se basa en estudiar la suavidad del ajuste junto con el

número de parámetros que requiere la aproximación mientras que la segunda intenta estudiar lo mismo, es decir la suavidad del ajuste, sin medir los parámetros de la clase de funciones. En este punto se puede incorporar el conocimiento a priori del problema.

3. Método con el que queremos minimizar la penalización. Este apartado está relacionado con los métodos que tenemos de aprender de los datos y el objetivo será intentar hallar una forma eficiente de minimizar tanto el error de la aproximación como la propia penalización.
4. Control de la complejidad. Como hemos dicho antes el control de la complejidad no es algo sencillo y habrá que escoger la mejor manera de medir dicha complejidad. En secciones posteriores veremos medidas de complejidad como la dimensión de Vapnik-Chervonenkis.

Veamos brevemente la distinción que hemos hecho entre la penalización paramétrica y no paramétrica.

### Penalización paramétrica

Supongamos que tenemos un conjunto de funciones  $f(x, \omega)$  con  $\omega \in \Omega$  donde  $\Omega$  es el conjunto de parámetros de la forma  $\omega = (\omega_0, \dots, \omega_m)$ . Como la aproximación viene definida por el parámetros  $\omega$  entonces podemos definir también la penalización asociada a dicha selección de parámetros.

Vamos a ver los ejemplos de las penalizaciones más empleadas de este tipo.

- Ridge:  $\phi_r(\omega_m) = \sum_{i=0}^m \omega_i^2$
- Selección de subconjunto:  $\phi_s(\omega_m) = \sum_{i=0}^m \chi(\omega_i \neq 0)$
- Bridge:  $\phi_p(\omega_m) = \sum_{i=0}^m |\omega_i|^p$
- Decaimiento de peso:  $\phi_q(\omega_m) = \sum_{i=0}^m \frac{(\omega_i/q)^2}{1+(\omega_i/q)^2}$

### Penalización no paramétrica

En primer lugar vamos a definir la transformada de Fourier de una función para poder definir el funcional de penalización.



**Definición 2.2 (Transformada de Fourier)** Sea  $f$  una función integrable Lebesgue,  $f \in L(\mathbb{R})$ . Se define la transformada de Fourier de  $f$  como la función:

$$\mathcal{F}\{f\} : \xi \rightarrow \hat{f}(\xi) := \int_{-\infty}^{\infty} f(x) e^{-2\pi i \xi x} dx$$

Recordemos brevemente las propiedades de la transformada de Fourier.

- La transformada de Fourier es un operador lineal:  $\mathcal{F}\{a \cdot f + b \cdot g\} = a\mathcal{F}\{f\} + b \cdot \mathcal{F}\{g\}$
- $\mathcal{F}\{f(at)\}(\xi) = \frac{1}{|a|} \cdot \mathcal{F}\{f\}(\frac{\xi}{a})$
- $\mathcal{F}\{f(t-a)\}(\xi) = e^{-\pi i \xi a} \cdot \mathcal{F}\{f\}(\xi)$
- $\mathcal{F}\{f\}(\xi - a) = \mathcal{F}\{e^{\pi i a t} f(t)\}(\xi)$
- $\mathcal{F}\{f'\}(\xi) = 2\pi i \xi \mathcal{F}\{f\}(\xi)$
- $\mathcal{F}\{f'\}(\xi) = \mathcal{F}\{(-it) \cdot f(t)\}(\xi)$

Habiendo recordado esto podemos definir el funcional de penalización no paramétrica. Este funcional mide la suavidad del ajuste de la función gracias a que se puede medir, mediante la transformada de Fourier, la ondulación de la función. Por tanto el funcional no paramétrico que se propone es:

$$\phi[f] = \int_{\mathbb{R}^d} \frac{|\hat{f}(s)|^2}{\hat{G}(s)} ds$$

Donde  $\hat{f}$  indica la transformada de Fourier de la función  $f$  y  $\frac{1}{\hat{G}}$  es la transformada de Fourier de una función de filtro de paso alto. Es en esta proposición de filtro donde se añade el conocimiento a priori del problema. Por ejemplo pudiera ser interesante en alguna aplicación práctica tener un funcional invariante frente a rotaciones de funciones.

#### 2.3.4. Equilibrio entre el sesgo y la varianza

Este enfoque es muy utilizado en el estudio del error, dividiéndolo en sesgo y varianza para hacer un mejor estudio del mismo y poder enfrentar ambos con varios métodos. Este estudio del caso clásico no es válido (o al

menos no del todo) para problemas no supervisados como es nuestro caso. Vamos a hacer una adaptación de esta teoría para que pueda encajar en nuestro caso de estudio.

Tenemos que tener en cuenta que no conocemos la salida real del sistema en el caso de detección de anomalías, es decir, no sabemos estimar con certeza el sesgo y la varianza y por tanto el error que cometemos. En primer lugar vamos a ver una pequeña adaptación de la notación al caso de detección de anomalías para poder hacer un estudio enfocado en nuestro problema.

Vamos a notar por  $X_1, \dots, X_n$  los datos de test y  $\mathcal{D}$  como conjunto de datos de entrenamiento. Además vamos a considerar que existe una función  $f$  que nos da la etiqueta real de un dato, esto es, si es o no una anomalía. Por tanto podemos decir que la auténtica etiqueta de un dato es  $y_i = f(X_i)$ . Además nosotros estaremos usando un modelo ya escogido por nosotros para predecir la etiqueta de un dato de test, esto es  $g(X_i, \mathcal{D}) \approx y_i + \beta$  donde  $\beta$  es un cierto error.

Una vez conocida esta notación podemos definir el error medio al cuadrado como:

$$MSE = \frac{1}{n} \sum_{i=1}^n \{y_i - g(X_i, \mathcal{D})\}^2$$

Y podemos definir también el valor esperado del error medio al cuadrado como:

$$E[MSE] = \frac{1}{n} \sum_{i=1}^n E[\{y_i - g(X_i, \mathcal{D})\}^2]$$

Una vez definido el  $MSE$  esperado podemos desarrollar un poco el cálculo para poder obtener el error y la varianza que esperamos.

En primer lugar podemos escribirlo como:

$$E[MSE] = \frac{1}{n} \sum_{i=1}^n E[\{(y_i - f(X_i)) + (f(X_i) - g(X_i, \mathcal{D}))\}^2]$$

Aquí solo hemos restado y sumado  $f(X_i)$ , ahora si recordamos que  $y_i = f(X_i)$  entonces podemos igualar el primero de los paréntesis a 0 y por tanto nos queda:

$$E[MSE] = \frac{1}{n} \sum_{i=1}^n E[\{f(X_i) - g(X_i, \mathcal{D})\}^2]$$

Si seguimos descomponiendo podemos sumar y restar  $E[g(X_i, \mathcal{D})]$  con lo que nos quedaría:

$$\begin{aligned} E[MSE] &= \frac{1}{n} \sum_{i=1}^n E[\{f(X_i) - E[g(X_i, \mathcal{D})]\}^2] \\ &\quad + \frac{2}{n} \sum_{i=1}^n \{f(X_i) - E[g(X_i, \mathcal{D})]\} \cdot \{E[g(X_i, \mathcal{D})] - E[g(X_i, \mathcal{D})]\} \\ &\quad + \frac{1}{n} E[\{E[g(X_i, \mathcal{D})] - g(X_i, \mathcal{D})\}^2] \end{aligned}$$

Como es claro, el segundo término da cero por lo que nos queda al final:

$$\begin{aligned} E[MSE] &= \frac{1}{n} \sum_{i=1}^n E[\{f(X_i) - E[g(X_i, \mathcal{D})]\}^2] + \frac{1}{n} \sum_{i=1}^n E[\{E[g(X_i, \mathcal{D})] - g(X_i, \mathcal{D})\}^2] \\ &= \frac{1}{n} \sum_{i=1}^n \{f(X_i) - E[g(X_i, \mathcal{D})]\}^2 + \frac{1}{n} \sum_{i=1}^n E[\{E[g(X_i, \mathcal{D})] - g(X_i, \mathcal{D})\}^2] \end{aligned}$$

Si reconocemos cada uno de los términos, en primer lugar el primero de ellos es el sesgo al cuadrado y el segundo la varianza, por lo que finalmente lo que hemos obtenido es:

$$E[MSE] = \text{sesgo}^2 + \text{varianza}$$

El dilema que se nos plantea es el siguiente: si tomamos modelos con un bajo sesgo en la estimación de los parámetros entonces tendremos una alta varianza y viceversa. Esto significa que no podemos con el conocimiento del que disponemos disminuir tanto el sesgo como la varianza a la vez. Es esta propiedad la que se conoce como la compensación entre sesgo y varianza.

## 2.4. Teoría estadística del aprendizaje

En esta sección vamos a hacer un repaso por la teoría del aprendizaje, en concreto la teoría desarrollada por Vapnik-Chervonenkis. Esta teoría se basa o tiene como pilares cuatro puntos:

1. Condiciones para la consistencia del principio ERM o minimización del error empírico.
2. Cotas en la capacidad de generalización de las máquinas de aprendizaje.
3. Principios de inferencia sobre muestras finitas.
4. Métodos constructivos para implementar los principios inductivos ya expuestos.

Durante el desarrollo de esta sección haremos un repaso de estos cuatro puntos para dar el broche final a esta sección y poder realizar la primera de las definiciones de anomalía.

### 2.4.1. Condiciones para la convergencia y consistencia del ERM

En el problema de aprendizaje disponemos de una muestra en la que tenemos los propios datos de entrada y la salida del sistema. Denotemos a estos elementos por  $z = (x, y)$  donde  $x$  son los datos de entrada e  $y$  la salida del sistema. Por tanto la muestra que se nos da es un conjunto  $Z_n = \{z_1, \dots, z_n\}$ . Estos datos están generados como ya sabemos mediante una función de densidad desconocida  $p(z)$ . Sobre este esquema tenemos una serie de funciones de pérdida y un funcional de pérdida. El objetivo es encontrar dicha función de pérdida  $Q(z, \omega)$  que minimice dicho funcional:

$$R(\omega) = \int Q(z, \omega) p(z) dz$$

Por tanto si tenemos la función de pérdida podemos definir el error empírico como:

$$R_{emp}(\omega) = \sum_{i=1}^n Q(z_i, \omega)$$

Donde  $\omega$  son los parámetros escogidos para el modelo.

Para poder estudiar la consistencia del ERM primero debemos definir formalmente dicha propiedad. Denotamos por  $R_{emp}(\omega_n^*)$  el valor del error empírico con la función de pérdida  $Q(z, \omega_n^*)$  que minimiza el error empírico para el conjunto de entrenamiento  $Z_n$ . Denotemos además por  $R(\omega_n^*)$  el verdadero valor (desconocido) del error para la función de pérdida. Como se puede ver estos valores dependen del tamaño del conjunto de entrenamiento  $n$ , podemos por tanto estudiar cómo se comportan estos errores cuando aumentamos el tamaño del conjunto de entrenamiento. Es aquí donde entra la definición de consistencia del ERM. Decimos que es consistente si la sucesión de errores reales y empíricos convergen en probabilidad al mismo límite  $R(\omega_0) = \min_{\omega} R(\omega)$ . Es decir:

$$\begin{aligned} R(\omega_n^*) &\rightarrow R(\omega_0) \text{ cuando } n \rightarrow \infty \\ R_{emp}(\omega_n^*) &\rightarrow R(\omega_0) \text{ cuando } n \rightarrow \infty \end{aligned}$$

Para poder asegurar esta propiedad sobre el ERM tenemos el conocido como Teorema Clave de la Teoría del Aprendizaje de Vapnik y Chervonenkis.

**Teorema 2.3 (Teorema Clave de la Teoría del Aprendizaje)** *Para funciones de pérdida acotadas el principio inductivo de minimización del error empírico es consistente si y sólo si el error empírico converge uniformemente al valor real del error en el siguiente sentido:*

$$\lim_{n \rightarrow \infty} P[\sup_{\omega} |R(\omega) - R_{emp}(\omega)| > \epsilon] = 0, \quad \forall \epsilon > 0$$

Cabe recalcar que estas condiciones de consistencia dependen de las propiedades de la clase de funciones elegida. No podemos pretender escoger como clase de aproximación una muy general y seguir manteniendo las condiciones de consistencia del ERM. Aún así el teorema nos está dando condiciones generales para la consistencia del ERM pero son abstractas y no fácilmente aplicables en la práctica. Para ello vamos a estudiar las condiciones de convergencia de ERM que sí serán aplicables en la implementación de algoritmos.

Vamos ahora a particularizar el estudio en el caso de clasificación binaria por ser la materia de estudio que nos ocupa, pues al final tendremos que clasificar instancias en anómalas o no anómalas. Ahora las funciones de pérdida  $Q(z, \omega)$  son funciones de pérdida indicadoras. Vamos a notar por  $N(Z_n)$  el número de dicotomías que se pueden tener con la clase de funciones

elegidas. Esto es el número de formas de clasificar los datos en las dos clases existentes.

Una vez actualizada nuestra notación podemos definir la entropía aleatoria como  $H(Z_n) = \ln N(Z_n)$ . Esta cantidad es una variable aleatoria dependiente de los valores de entrenamiento  $Z_n$ , podemos definir ahora la entropía de Vapnik-Chervonenkis como el valor medio o esperado de la entropía aleatoria:

$$H(n) = E[\ln N(Z_n)]$$

Esta medida es una cuantificación de la diversidad del conjunto de funciones indicadoras que nos pueden separar los datos en ambas clases.

Por último vamos a definir la función de crecimiento que nos va a permitir hacer cotas y llegar a la condición necesaria y suficiente para la convergencia del ERM. Definimos la función de crecimiento como:

$$G(n) = \ln \max_{Z_n} N(Z_n)$$

Donde aquí estamos notando el máximo número de dicotomías sobre todas las posibles muestras existentes de tamaño  $n$ . Es más, como el máximo número de formas de dividir un conjunto de tamaño  $n$  en dos clases es  $2^n$  entonces podemos afirmar que  $G(n) \leq n \ln(2)$ .

Por último y para completar la cadena de desigualdades que buscamos vamos a definir la entropía reforzada de Vapnik-Chervonenkis:

$$H_{ann}(n) = \ln(E[N(Z_n)])$$

Haciendo uso de la conocida desigualdad de Jensen,

$$\sum_{i=1}^n a_i \ln(x_i) \leq \ln\left(\sum_{i=1}^n a_i x_i\right)$$

,

podemos ver claramente que  $H(n) \leq H_{ann}(n)$ . Por tanto obtenemos la cadena de desigualdades:

$$H(n) \leq H_{ann}(n) \leq G(n) \leq n \ln(2)$$

La condición necesaria y suficiente de Vapnik-Chervonenkis para la convergencia del ERM que hallaron fue que:

$$\lim_{n \rightarrow \infty} \frac{H(n)}{n} = 0$$

Pero esta condición no asegura una convergencia rápida asintóticamente al error real. Se dice que el ratio de convergencia es rápido asintóticamente en la Teoría de Vapkin-Chervonenkis si:

$$\forall n > n_0 \quad P(R(\omega) - R(\omega^*) < \epsilon) = e^{-cn\epsilon^2} \text{ con } c > 0$$

Para poder cumplir esta condición se dio la condición suficiente para la convergencia rápida:

$$\lim_{n \rightarrow \infty} \frac{H_{ann}(n)}{n} = 0$$

Estas condiciones son dependientes de la distribución de los datos  $Z_n$  como es claro al depender de la esperanza de una variable aleatoria dependiente de  $Z_n$ . Es por tanto que esta condición no es del todo general. Para solventar esto se tiene la consistencia y convergencia del ERM con la condición necesaria y suficiente de que:

$$\lim_{n \rightarrow \infty} \frac{G(n)}{n}$$

Por tanto este estudio nos ha dado las condiciones de convergencia y consistencia del ERM.

### 2.4.2. Función de crecimiento y dimensión de Vapnik-Chervonenkis

El objetivo que perseguimos es obtener cotas para la capacidad de generalización de las máquinas de aprendizaje. Para dar el primer paso según hemos visto necesitamos una forma de evaluar la función de crecimiento vista en el apartado anterior, cosa que no es sencilla de llevar a la práctica.

Para continuar avanzando en este camino lo primero que vamos a presentar es el concepto de dimensión de Vapnik-Chervonenkis o dimensión VC. Cuando discutimos cómo medir la complejidad de un modelo ya hablamos

de que la dimensión VC podría ser una buena herramienta para este fin, la introducimos a continuación.

Vapnik y Chervonenkis probaron que la función de crecimiento estaba acotada por una función logarítmica en función del tamaño de la muestra. El punto en el que se tiene  $n = h$  donde  $h$  es un valor fijo se tiene que el crecimiento de la función de crecimiento empieza a ralentizarse, esta es la conocida como dimensión VC. Si  $h$  es un número finito entonces tenemos que la función de crecimiento no va a crecer de forma lineal para muestras de tamaño grande y de hecho se tiene la cota:

$$G(n) \leq h(1 + \ln(\frac{n}{h}))$$

La dimensión de Vapnik-Chervonenkis es intrínseca a la elección del conjunto de funciones y además nos da condiciones sobre la convergencia rápida del ERM. Ya hemos visto antes que la cota más grande de la función de crecimiento es:

$$G(n) \leq n \ln(2)$$

Si comparamos las dos cotas en función de  $n$  tenemos la siguiente gráfica:

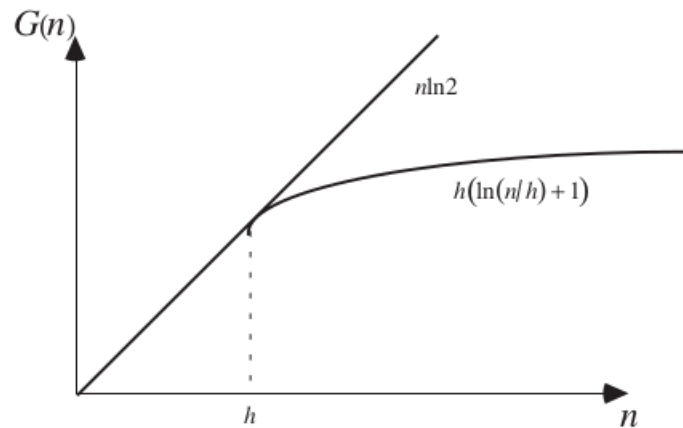


Figura 2.4: Comportamiento de la función de crecimiento [2, p. 107]

Como podemos ver el comportamiento una vez que el tamaño de la muestra alcanza la dimensión VC converge de forma mucho más rápida.



Hasta ahora no hemos definido formalmente la dimensión VC pero hemos dado una característica de la misma que nos garantiza una buena convergencia. Decimos que un conjunto de funciones indicadoras tiene dimensión VC  $h$  si existe una muestra de puntos de tamaño  $h$  que puede ser dividida pero no existe una muestra de tamaño  $h + 1$  que cumpla dicha condición. Es decir, podemos decir que la dimensión VC es la máxima dimensión para la que existe una solución óptima a nuestro problema de dividir el conjunto de datos entre datos anómalos y normales.

Veamos esto con un ejemplo gráfico:

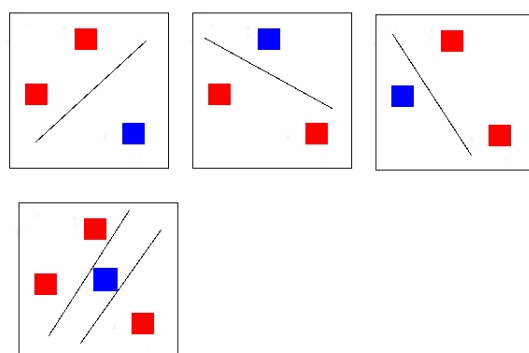


Figura 2.5: Ejemplo de cálculo de dimensión VC Wikimedia

Como podemos ver si estamos considerando funciones lineales para aproximar podemos dividir todas las posibilidades con tamaño de muestra 3, pero no con tamaño de muestra 4 por lo que en este caso concreto la dimensión VC será 3.

Ahora podemos volver a la cadena de desigualdades que hemos visto en la sección anterior y actualizarla con la nueva mejor cota que hemos desarrollado con la dimensión VC:

$$H(n) \leq H_{ann}(n) \leq G(n) \leq h(1 + \ln(\frac{n}{h}))$$

La definición que hemos dado es para funciones indicadoras pero no para funciones reales en general, vamos a generalizar por tanto la definición de la dimensión de Vapnik-Chervonenkis para el caso de funciones reales.

Consideramos como hemos hecho anteriormente funciones de pérdida del tipo  $Q(z, \omega)$  pero acotadas superior e inferiormente por constantes:

$$A \leq Q(z, \omega) \leq B$$

Para este caso podemos pensar en una función indicadora que nos diga si  $Q(z, \omega)$  está por encima o por debajo de un cierto valor  $\beta$  con  $A \leq \beta \leq B$ . Podemos por tanto generalizar la dimensión VC para el caso de funciones de pérdida reales como la dimensión VC de este tipo de funciones indicadoras dependientes del parámetro  $\beta$ .

### 2.4.3. Límites de la generalización

Venimos de discutir las propiedades de convergencia y consistencia del principio inductivo ERM. Ahora bajo este principio vamos a intentar ir un paso mas allá en la generalización e intentar responder a las siguientes dos preguntas:

1. ¿Cómo de cerca están el error real  $R(\omega^*)$  y el mínimo error empírico  $R_{emp}(\omega^*)$ ?
2. ¿Cómo de cerca están el error real  $R(\omega^*)$  y el mínimo error posible  $R(\omega_0) = \min_{\omega} R(\omega)$ ?

Estas preguntas las vamos a resolver en el marco que hemos introducido, con todos los conceptos anteriores de la teoría de Vapnik-Chervonenkis en el caso del problema de clasificación binaria que es el que más se ajusta a nuestro problema.

Según Vapnik-Chervonekis se puede acotar el error real cometido por el error empírico con una probabilidad de al menos  $1 - \eta$  usando el principio inductivo ERM. La cota que hallaron es la siguiente:

$$R(\omega) \leq R_{emp}(\omega) + \frac{\epsilon}{2} \left( 1 + \sqrt{1 + \frac{4 \cdot R_{emp}(\omega)}{\epsilon}} \right)$$

donde:

$$\epsilon = a_1 \cdot \frac{h(\ln(\frac{a_2 n}{h}) + 1) - \ln(\frac{\eta}{4})}{n}$$

cuando el conjunto de funciones de pérdida  $Q(z, \omega)$  contiene un número infinito de elementos, en caso contrario:

$$\epsilon = 2 \frac{\ln(N) - \ln(\eta)}{n}$$

y los valores  $a_1, a_2$  son constantes sobre los que se exigen condiciones.

Para empezar según la demostración de Vapnik, los valores  $a_1$  y  $a_2$  deben estar en los rangos  $0 < a_1 \leq 4$  y  $0 < a_2 \leq 2$  siendo la pareja de valores  $a_1 = 4$  y  $a_2 = 2$  la correspondiente al peor de los casos, dando en como resultado el siguiente valor de  $\epsilon$ :

$$\epsilon = 4 \frac{h(\ln(\frac{2n}{h})) - \ln(\frac{\eta}{4})}{n}$$

Con esta desigualdad estamos dando la cota de cómo se comporta el error real con respecto al error empírico. Podemos ver que, en el mejor de los casos el error real y el error empírico se van a diferenciar en al menos  $\frac{\epsilon}{2}$ .

Además, para resolver la segunda de las preguntas la teoría de Vapnik-Chervonenkis nos da la siguiente cota con probabilidad al menos  $1 - 2\eta$ :

$$R(\omega_n^*) - \min_{\omega} R(\omega) \leq \sqrt{\frac{-\ln(\eta)}{2n}} + \frac{\epsilon}{2} \left( 1 + \sqrt{1 + \frac{4}{\epsilon}} \right)$$

En este caso podemos ver que la cota es aún mayor que en el caso anterior, teniéndose tanto en esta cota como en la anterior que a mayor nivel de confianza (menor valor de  $\eta$ ) mayor es la cota y por tanto menos información tenemos. Es decir, no podemos conocer una buena cota con un nivel de confianza alto. Este hecho no debería de sorprendernos pues seguimos trabajando con un número finito de datos y ya sabemos que no podemos obtener una aproximación todo lo buena que queramos con un número finito de datos de entrenamiento.

Este hecho también se refleja en los valores analíticos que hemos dado. Pensemos en un escenario con  $\eta \rightarrow 0$ , es decir un alto nivel de confianza. Entonces si miramos la expresión de  $\epsilon$  podemos observar que  $-\ln(\frac{\eta}{4}) \rightarrow \infty$  y por tanto  $\epsilon \rightarrow \infty$  con lo que la cota no nos aportaría ninguna información en ninguno de los dos casos.

Por otro lado si lo que crece es el tamaño de la muestra, es decir,  $n \rightarrow \infty$ , estamos aumentando el conocimiento que tenemos sobre el problema y por tanto lo razonable sería que ambas cotas tendieran al valor óptimo. En efecto si observamos el valor de  $\epsilon$  cuando  $n \rightarrow \infty$  vemos que tiende a 0 por lo que el error empírico y real están muy cerca y de igual forma el error real y el

mínimo error posible. Por tanto podemos decir que nuestro nivel de certeza depende del tamaño de la muestra. Este hecho fue visto por Vapnik en su teoría y propuso como valor aproximado de la confianza de la desigualdad aquel que lleva asociado el valor:

$$\eta = \min\left(\frac{4}{\sqrt{n}}, 1\right)$$

#### 2.4.4. Principio de minimización del error estructural (SRM)

Hemos visto una construcción en base al principio inductivo ERM y hemos razonado que funciona bien para casos en los que la proporción  $\frac{n}{h}$ , es decir la proporción del tamaño de la muestra y la dimensión VC, es grande. En este caso quiere decir que tenemos muchos datos comparado con la dimensión VC y por tanto  $\epsilon \approx 0$ . Por contra cuando tenemos que  $\frac{n}{h}$  es pequeño no tenemos mucha información de la cota. Por tanto, al estar el número de datos fijo por el problema, tenemos que buscar un conjunto de funciones para aproximar la salida del sistema que nos den una dimensión VC controlable para hacerla más o menos grande.

El principio inductivo que pretende plasmar esta idea es el principio de minimización del error estructural o SRM. Bajo este principio se le otorga a la clase de funciones de pérdida de una estructura, es decir, tenemos subconjuntos de la forma  $S_k = \{Q(z, \omega), \omega \in \Omega_k\}$  de forma que:

$$S_1 \subset S_2 \subset \dots \subset S_k \subset \dots$$

donde cada subconjunto de funciones de pérdida tiene asociada una dimensión VC  $h_k$  teniéndose el orden:

$$h_1 \leq h_2 \leq \dots \leq h_k \leq \dots$$

Al igual que en el Teorema clave de la Teoría del Aprendizaje de Vapnik-Chervonenkis se exigía que las funciones de pérdida estuvieran acotadas en este caso vamos a pedir que las funciones contenidas en cada uno de los  $S_k$  o bien estén acotadas o si no que cumplan que:

$$\sup_{\omega \in \Omega_k} \frac{(\int Q^p(z, \omega) dp(z))^{\frac{1}{p}}}{\int Q(z, \omega) dp(z)} \leq \tau_k, \quad p > 2$$

para alguna pareja  $(p, \tau_k)$ .

En cuanto a la definición del SRM hay dos estrategias prácticas que se llevan a cabo para su implementación que son:

1. Mantener la dimensión VC fija y minimizar el error empírico.
2. Mantener el error empírico constante y pequeño y minimizar la dimensión VC.

Estas implementaciones realmente quedan muy libres en la práctica y se proponen por tanto diferentes estructuras de minimización del error empírico y la dimensión VC que se saben que funcionan bien.

Por tanto este principio no se basa meramente en el buen ajuste de los datos, si no que además pretende hacer una minimización de la complejidad del modelo propuesto.

#### 2.4.5. Aproximaciones de la dimensión VC

Como hemos estado viendo las cotas que hemos expuesto y desarrollado dependen en mayor o menor medida de la dimensión VC. Como es lógico este valor no es fácil de calcular, y de hecho sólo se sabe para unos cuantos conjuntos de funciones de aproximación. Vapnik propuso una método para poder estimar este valor y así poder obtener unas cotas aproximadas.

El procedimiento propuesto por Vapnik consiste en, dadas dos muestras  $Z_n^1, Z_n^2$  de tamaño  $n$  de pares  $z_i = (x, y)$  de datos de entrada y salida del sistema vamos a medir el error empírico con nuestro modelo que cometemos observando la máxima desviación de los ratios de error de estas dos muestras independientes, es decir:

$$\xi(n) = \max_{\omega} (|Error(Z_n^1) - Error(Z_n^2)|)$$

donde  $Error(Z_n^i)$  es la tasa de error empírico cometido por el modelo. De acuerdo con la teoría desarrollada por Vapnik-Chervonenkis tenemos que  $\xi(n)$  está acotada:

$$\xi(n) \leq \Phi\left(\frac{n}{h}\right)$$

donde  $h$  es la dimensión VC y:

$$\Phi(\tau) = \begin{cases} 1 & \text{si } \tau < 0.5 \\ a^{\frac{\ln(2\tau)+1}{\tau-k}} \left( \sqrt{1 + \frac{b(\tau-k)}{\ln(2\tau)+1}} + 1 \right) & \text{en otro caso} \end{cases}$$

donde  $\tau = \frac{n}{h}$  y las constantes  $a = 0.16$  y  $b = 1.2$  son constantes estimadas empíricamente por Vapnik y  $k = 0.14928$  tomada así para que  $\Phi(0.5) = 1$  de forma que la cota sea muy ajustada.

Por tanto describió con esto el siguiente esquema de obtención de la aproximación de la dimensión VC:

1. Generamos una muestra de tamaño  $2n$  etiquetada  $z_{2n}$
2. Dividimos la muestra en dos del mismo tamaño  $Z_n^1$  y  $Z_n^2$
3. Invertir las etiquetas de  $Z_n^2$
4. Mezclar los dos conjuntos de nuevo y entrenar el modelo
5. Separar el conjunto en dos de nuevo e invertir las etiquetas del segundo, volver a mezclarlos y entrenar de nuevo el modelo
6. Medir la diferencia de los errores  $\xi(n) = |Error(Z_n^1) - Error(Z_n^2)|$

Como hemos dicho antes la desigualdad  $\xi(n) \leq \Phi(\frac{n}{h})$  es muy ajustada y por tanto, podemos obtener la aproximación de  $h$  como:

$$h^* = \arg \min_h [\xi(n) - \Phi(\frac{n}{h})]$$

Es decir, el valor que haga dicha diferencia menor, es decir que más acerque los valores  $\xi(n)$  y  $\Phi(\frac{n}{h})$ .

#### 2.4.6. Perspectiva

Tras este desarrollo teórico hemos dado un marco sobre el cuál podremos cimentar el resto del trabajo y modelos empleados. Con este capítulo hemos hecho un repaso por toda la teoría básica de Machine Learning y la teoría desarrollada por Vapnik y Chervonenkis.

El siguiente paso que debemos dar es introducir la definición clásica de anomalía basada en distancias y dar algunas reflexiones sobre ella para poder proseguir en el estudio.

## Capítulo 3

# Concepto de anomalía

En esta sección vamos a estudiar la idea de anomalía, fundamentalmente propuesta en el libro Outlier Analysis [44].

### 3.1. Contextualización

Ya hemos discutido previamente una idea intuitiva del concepto de anomalía. Un dato decimos que es anómalo cuando se distancia del resto de los datos lo suficiente como para no tener características comunes con ellos.

Este hecho puede ser por distintos motivos. Puede que la anomalía venga del hecho de que se está produciendo un evento en nuestros experimentos que no sea nada frecuente. Por ejemplo podemos estar midiendo datos meteorológicos y que en un momento dado se den una serie de fenómenos que no sea frecuente ver juntos, o incluso que no se hayan visto nunca ocurrir simultáneamente. Otra forma de tener una anomalía en nuestro conjunto de datos pudiera ser errores de medición. Por ejemplo si seguimos con este símil de los datos meteorológicos imaginemos que nuestra estación dispone de un termómetro. Este sensor se ha roto y empieza a marcar datos superiores a  $100\text{ }^{\circ}\text{C}$ , claramente son datos muy desviados de las temperaturas normales con lo que no tendrían relación con el resto y presentaría una desviación muy importante con respecto al resto de los datos.

### 3.2. Criterios

Esta idea intuitiva que estamos dando de anomalía no refleja todos los posibles escenarios. Los ejemplos que estamos dando suponen una desviación muy grande de los datos normales, tanto que no se pueden comparar con el resto porque difieren mucho numéricamente. Vamos a plantear un escenario para dar una mejor forma al concepto de anomalía. Pensemos en una serie de datos muy agrupados en dos clústeres por ejemplo:

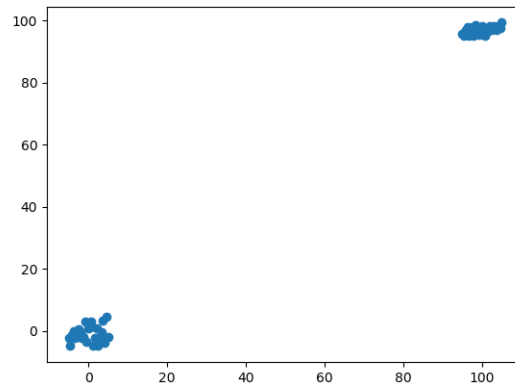


Figura 3.1: Clústeres alejados

Como podemos comprobar que tenemos dos clústeres no sólo alejados entre sí, si no con los elementos muy concentrados para poner un caso extremo. Ahora no vamos a proponer un valor que se aleje de los dos clústeres, si no uno que esté a medio camino entre los dos:



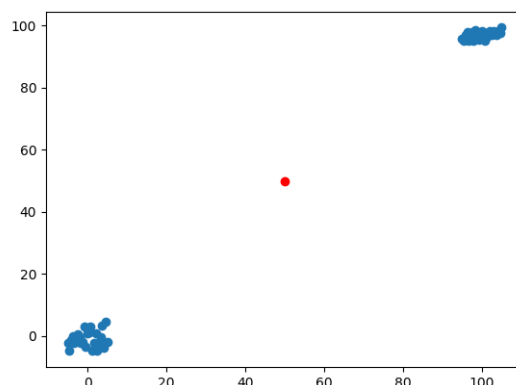


Figura 3.2: Clústeres alejados con una anomalía en rojo

Si los datos del clúster de abajo a la izquierda fueran datos de temperatura con valores entorno a 0 y los de arriba a la derecha fueran de datos de temperatura entorno a 100 grados nuestro datos anómalo tendría una temperatura de unos 50 grados. Esta temperatura no se aleja radicalmente de los valores normales, es decir, no son -1000 grados ni 1000 grados. Aún así estamos describiendo una situación anómala.

No podemos dar una definición formal o que podamos decir que abarca todos los casos para definir lo que es una anomalía, aún así vamos a intentar dar dos puntos de vista: uno basado en distancias y otro en probabilidades.

El criterio más usado en la definición o detección de anomalías es el llamado “Tukey’s Fences”. Para introducirlo vamos a ver su definición en una única dimensión para luego extender el concepto. Pensemos en un conjunto de datos 1-D. Sobre sus valores podemos calcular los cuartiles  $Q_1$ ,  $Q_2$  y  $Q_3$ . Un valor anómalo es aquel que no cae dentro del intervalo  $[Q_1 - k(Q_3 - Q_1), Q_3 + k(Q_3 - Q_1)]$  donde  $k$  es una constante. El valor propuesto para  $k$  por Tukey fue de  $k = 1.5$  aunque algunos autores más restrictivos proponen  $k = 3$ .

Este criterio puede ser extendido al caso de mayor dimensionalidad si realizamos este mismo test sobre todos los valores de todas las características y comprobar si alguno o todos se salen del rango en función de cómo de restrictivo queremos que sea el criterio.

Esta extensión es muy vaga, por lo que se propone un criterio un poco más fijado. Imaginemos los datos agrupados por clústeres, entonces podemos fijar un centroide de dicho clúster. Sobre cada clúster podemos medir cuál

es la mayor distancia dentro del clúster de los datos al centroide. Podemos extender el criterio de Tukey diciendo que un dato anómalo es aquel que se distancia más de 1.5 veces de la mayor distancia dentro del clúster al centroide.

Esta generalización ya si abarca el ejemplo que hemos propuesto. Al estar muy apiñados los datos entorno al centroide la mayor distancia dentro del clúster es muy pequeña, de hecho en el ejemplo construido es menor que 5. Por tanto el dato (50, 50) está alejado más de  $1.5 \cdot 5 = 7.5$  unidades del centroide y por tanto lo podemos considerar una anomalía.

### 3.3. Qué hacer con las anomalías

Estamos estudiando cómo podemos detectar anomalías pero una vez que las hayamos detectado en nuestros conjuntos de datos en un problema real, ¿qué debemos hacer con ellas? Este problema es algo muy general, puede que estemos seguros en nuestro caso de que las anomalías se han debido a un problema de medición porque nuestros instrumentos estaban rotos y por tanto deberíamos descartarlos. Puede que sean datos reales pero estén tan separados del resto que debamos estudiarlos de forma separada. Vamos a dar unas cuantas alternativas a lo que podemos hacer una vez que hemos detectados las anomalías dentro de nuestro conjunto de datos:

- Dejarlos: puede que nuestro conjunto de datos tenga un número de datos muy elevado y por tanto aparezcan en él anomalías. Estas anomalías no deben ser eliminadas, es más debemos escoger modelos que aprendan o utilicen los datos teniendo en cuenta estas anomalías y siendo robustos ante su aparición.
- Exclusión: una opción es eliminar directamente las anomalías. Esto en general no está justificado y de hecho no se recomienda pues perdemos riqueza del conjunto de datos al eliminar instancias del mismo. Aún así, si decidimos eliminar los datos tenemos dos formas de hacerlo. Podemos eliminarlos directamente y prescindir de esos datos o podemos sustituirlos por datos cercanos que no sean anómalos.
- Estudiarlos por separado: puede que tengamos un número suficientemente elevado de las mismas y que enseñen algunos patrones o tengan explicación en nuestro ejemplo del mundo real. En este caso quizás deberíamos considerarlas y estudiarlas a parte para darles un sentido y emplear el conocimiento que les subyace.

## Parte II

# Introducción de Estadística Multivariante y concepto probabilístico de anomalía



Para poder proseguir en el estudio debemos hacer un repaso breve de conceptos de estadística multivariante. El contenido de esta sección se ha sacado básicamente de apuntes de la asignatura Estadística Multivariante del grado en Matemáticas, los apuntes de la asignatura Procesos Estocásticos del grado en Matemáticas y el libro Probability Theory de M. Loève [49].



## Capítulo 4

# Introducción de Estadística Multivariante

Vamos a dar otra definición de anomalía que no coincide con la que hemos visto basada en distancias, pero antes de dar esa definición debemos hacer un breve repaso de estadística multivariante y probabilidad para poder comprender y enmarcar dicha definición.

### 4.1. Introducción

En primer lugar vamos a describir conceptos básicos sobre los que poder construir los conceptos que necesitamos para la definición de anomalía basada en probabilidades.

En primer lugar vamos a definir el concepto de variable aleatoria.

**Definición 4.1** *Una variable aleatoria es una función  $X : \Omega \rightarrow E$  que parte de un espacio de probabilidad  $(\Omega, \mathcal{F}, \mathcal{P})$  y llega a un espacio medible  $(E, \mathcal{B})$ , donde  $X$  además es una función medible.*

Normalmente ya sabemos que  $E \subseteq \mathbb{R}$  y además cabe recordar que  $\mathcal{F}$  es una  $\sigma$ -álgebra. Además cabe recordar la definición de función medible:

**Definición 4.2** *Decimos que una función  $X : (\Omega, \mathcal{F}, \mathcal{P}) \rightarrow (E, \mathcal{B})$  es medible si  $X^{-1}(B) \in \mathcal{F}$ ,  $\forall B \in \mathcal{B}$ .*

Esta definición puede extenderse al caso vectorial, introduciendo con esto la noción de vector aleatorio:

**Definición 4.3** *Un vector aleatorio  $\underline{X} = (X_1, \dots, X_p)$  es una aplicación medible  $\underline{X} : (\Omega, \mathcal{F}, \mathcal{P}) \rightarrow (E, \mathcal{B}^p)$  donde  $E \subseteq \mathbb{R}^p$ .*

Se puede demostrar además la caracterización:

**Proposición 4.1** *Un vector  $\underline{X} = (X_1, \dots, X_p)$  es un vector aleatorio si y sólo si  $X_i : (\Omega, \mathcal{F}, \mathcal{P}) \rightarrow (\mathbb{R}, \mathcal{B})$  es una función medible.*

Con este vector aleatorio podemos estudiar o definir la distribución de probabilidad del mismo sobre  $(\mathbb{R}^p, \mathcal{B}^p)$   $P_{\underline{X}}$  como:

$$P_{\underline{X}}[B] := P[\underline{X}^{-1}(B)] \quad \forall B \in \mathcal{B}$$

con lo que el espacio  $(\mathbb{R}^p, \mathcal{B}^p, P_{\underline{X}})$  es un espacio de probabilidad o probabilístico.

Sobre los conocimientos de la definición de la función de distribución univariante podemos hacer una definición análoga para el caso multivariante.

**Definición 4.4** *Se define la función de distribución asociada a la probabilidad inducida como:*

$$F_{\underline{X}}(\underline{x}) = P_{\underline{X}}[X_1 \leq x_1, \dots, X_p \leq x_p] \quad , \quad \forall \underline{x} = (x_1, \dots, x_p) \in \mathbb{R}^p$$

De igual forma podemos caracterizar la función de densidad como aquella  $f_{\underline{X}}$  que, de existir, cumple que:

$$F_{\underline{X}}(\underline{x}) = \int_{-\infty}^{x_1} \int_{-\infty}^{x_2} \dots \int_{-\infty}^{x_p} f_{\underline{X}}(u_1, \dots, u_p) du_1 \dots du_p$$

Otra forma de determinar de forma única la distribución de un vector aleatorio es mediante la función característica, lo que nos va a dar además una caracterización de la independencia que introduciremos seguidamente.



**Definición 4.5** Dado un vector aleatorio  $X = (X_1, \dots, X_p)$  se define la función característica como  $\Phi_{\underline{X}}(\underline{t}) = E[e^{i\underline{t}X}]$  con  $\underline{t} = (t_1, \dots, t_p) \in \mathbb{R}^p$  donde la función  $E[\cdot]$  denota la esperanza, por lo que:

$$\Phi_{\underline{X}}(\underline{t}) = \int_{\mathbb{R}^p} e^{i\underline{t}X} P_{\underline{X}}(d\underline{x})$$

Con esto ya podemos introducir el concepto de independencia en varias variables.

#### 4.1.1. Independencia

**Definición 4.6** Dados dos vectores aleatorios  $\underline{X} = (X_1, \dots, X_p)$ ,  $\underline{Y} = (Y_1, \dots, Y_p)$  se dice que son independientes si:

$$F_{\underline{X}, \underline{Y}}(\underline{x}, \underline{y}) = F_{\underline{X}}(\underline{x}) \cdot F_{\underline{Y}}(\underline{y})$$

Podemos también definir la independencia entre las variables de un vector aleatorio como:

**Definición 4.7**  $X = (X_1, \dots, X_p)$  se dice que está compuesto de variables independientes si  $\forall B = B_1 \times \dots \times B_p$  con  $B_i \in \mathcal{B}$  se tiene que:

$$P_{\underline{X}}(B) = P_{X_1}[B_1] \cdot \dots \cdot P_{X_p}[B_p]$$

En cuanto a la independencia de sucesos podemos dar dos definiciones de independencia:

**Definición 4.8** Decimos que los eventos  $B = (B_1, \dots, B_p)$  son independientes dos a dos si para todos  $m \neq k$  se tiene que  $P(B_m \cap B_k) = P(B_m)P(B_k)$

**Definición 4.9** Se dice que los eventos  $B = (B_1, \dots, B_p)$  son independientes mutuamente si para todo  $k \leq p$  se tiene que  $P(\bigcap_{i=1}^k B_i) = \prod_{i=1}^k P(B_i)$

En cuanto a la definición de independencia entre las variables aleatorias que definen un vector aleatorio podemos dar dos caracterizaciones basadas en la función característica.

**Proposición 4.2** *Si las componentes del vector aleatorio  $X = (X_1, \dots, X_p)$  son independientes entonces:*

$$\Phi_{\underline{X}}(t) = E[e^{it\underline{X}}] = \prod_{j=1}^p E[e^{it_j X_j}]$$

**Proposición 4.3** *Si las componentes del vector aleatorio  $X = (X_1, \dots, X_p)$  son independientes entonces la función característica de la variable  $Y = \sum_{j=1}^p X_j$  es:*

$$\Phi_Y(t) = E[e^{itY}] = E[e^{it \sum_{j=1}^p X_j}] = \prod_{j=1}^p \Phi_{X_j}(t)$$

#### 4.1.2. Probabilidad y esperanza condicionada

En esta sección vamos a describir la probabilidad y esperanza condicionada de una variable aleatoria y no de un vector aleatorio. Este hecho es sencillo de deducir, pues como hemos introducido previamente la distribución de probabilidad de un vector aleatorio viene determinada por una distribución de probabilidad de una variable aleatoria. Por tanto el estudio de la probabilidad y esperanza condicionada en el caso univariante se hace válido para el caso multivariante.

En primer lugar debemos introducir el concepto de probabilidad condicionada tal y cómo la conocemos hasta ahora de Bayes. Partimos de un espacio de probabilidad  $(\Omega, \mathcal{A}, \mathcal{P})$ .

**Definición 4.10** *Definimos la probabilidad condicionada a un suceso  $B \in \mathcal{A}$  con  $P(B) > 0$  como:*

$$P(\cdot|B) : \mathcal{A} \rightarrow [0, 1], \quad P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Esta es una función de probabilidad, por lo que nos lleva a pensar en el espacio de probabilidad que genera, es más podemos pensar en el espacio de probabilidad en el que la probabilidad condicionada no se anula, es decir:

$$\mathcal{A}_B = \{C = A \cap B, A \in \mathcal{A}\}$$

Por tanto solemos considerar como espacio de probabilidad condicionada al espacio  $(B, \mathcal{A}_B, P(\cdot|B))$ .

Partiendo de este espacio de probabilidad podemos considerar una variable aleatoria  $X : (\Omega, \mathcal{A}, \mathcal{P}(\cdot|B)) \rightarrow (\mathbb{R}, \mathcal{B})$ .

**Definición 4.11** Definimos la esperanza de esta variable aleatoria condicionada a  $B$  como:

$$E[X|B] = \int_{\Omega} X dP(\cdot|B) = \int_{\Omega} X dP(\cdot|B) = \frac{1}{P(B)} \int_B X dP = \frac{E[X1_B]}{P(B)}$$

Donde  $1_B$  representa la función indicadora del conjunto  $B$ .

No sólo podemos estudiar la probabilidad y esperanzas condicionadas a un evento, si no que también las podemos estudiar condicionadas a una  $\sigma$ -álgebra. En este terreno vamos a distinguir dos posibilidades: condicionamiento a una  $\sigma$ -álgebra generada por una partición numerable de sucesos de probabilidad no nula y condicionamiento a una  $\sigma$ -álgebra arbitraria.

**Definición 4.12** Definimos la esperanza condicionada a una  $\sigma$ -álgebra  $\mathcal{A}$  generada por  $\{B_n\} \subset \mathcal{A}$  con  $B_i \cap B_j = \emptyset$ ,  $i \neq j$ ,  $\bigcup_{n=1}^{\infty} B_n = \Omega$  y  $P(B_i) > 0$ ,  $\forall i$ . Siendo la  $\mathcal{U} = \sigma(\{B_n\})$  la  $\sigma$ -álgebra generada por  $\{B_n\}$ . Con este marco, definimos la esperanza de una variable aleatoria  $X : (\Omega, \mathcal{A}, P) \rightarrow (\mathbb{R}, \mathcal{B})$  condicionada a la  $\sigma$ -álgebra  $\mathcal{U}$  como:

$$E[X|\mathcal{U}](\omega) = \sum_{n=1}^{\infty} E[X|B_n]1_{B_n}(\omega)$$

**Propiedades 4.1** 1.  $E[X|\mathcal{U}] : (\Omega, \mathcal{U}) \rightarrow (\mathbb{R}, \mathcal{B})$  es  $\mathcal{U}$ -medible.

2.  $E[E[X|\mathcal{U}]] = \sum_{n=1}^{\infty} E[X|B_n]P(B_n) = \sum_{n=1}^{\infty} E[X1_{B_n}] = E[X]$

De igual forma podemos definir la probabilidad condicionada a una  $\sigma$ -álgebra generada por una partición numerable de sucesos no nulos.

**Definición 4.13** Definimos la probabilidad de un suceso  $A \in \mathcal{A}$  condicionada a la  $\sigma$ -álgebra  $\mathcal{U}$  como:

$$P(A|\mathcal{U}) = E[1_A|\mathcal{U}] = \sum_{n=1}^{\infty} E[1_A|B_n]1_{B_n} = \sum_{n=1}^{\infty} P(A|B_n)1_{B_n}$$

casi seguramente.

Podemos también dar unas propiedades inmediatas de la probabilidad condicionada tomando como base las de la esperanza.

**Propiedades 4.2** 1.  $P(A|\mathcal{U})$  es  $\mathcal{U}$ -medible.

2.  $E[P(A|\mathcal{U})] = P(A)$

Una vez visto esto podemos hacer una definición con una  $\sigma$ -álgebra arbitraria. Cabe decir que en este caso no vamos a poder dar una definición constructiva y fácil de calcular como sí hemos hecho en el caso particular anterior. Lo que sí vamos a tener con esta definición más general es el mantenimiento de las propiedades que hemos visto en primera instancia tanto de la probabilidad como de la esperanza condicionada. Sobra decir además que esta definición coincide con la anterior en el caso particular de una  $\sigma$ -álgebra generada por una partición numerable de sucesos no nulos.

**Definición 4.14** Definimos la esperanza de una variable aleatoria  $X$  en el marco dado condicionada a una  $\sigma$ -álgebra  $\mathcal{U} \subset \mathcal{A}$  como la única función  $\mathcal{U}$ -medible tal que:

$$\forall u \in \mathcal{U} \quad \int_{\mathcal{U}} E[X|\mathcal{U}] P_{\mathcal{U}} = \int_{\mathcal{U}} X dP$$

casi seguramente  $P_{\mathcal{U}}$ . Donde  $\forall u \in \mathcal{U} \quad P_{\mathcal{U}}(u) = P(u)$ .

Igualmente podemos dar una definición de la probabilidad condicionada a una  $\sigma$ -álgebra arbitraria tomando como base la definición de esperanza condicionada.

**Definición 4.15** Definimos la probabilidad de  $A \in \mathcal{A}$  condicionada a la  $\sigma$ -álgebra  $\mathcal{U}$  como:

$$P(A|\mathcal{U}) = E[1_A|\mathcal{U}]$$

casi seguramente  $P_{\mathcal{U}}$ .

Por último antes de dar unas propiedades que nos den un poco más de conocimiento y herramientas de trabajo vamos a ver el concepto de probabilidad y esperanza condicionada a una variable aleatoria y no a un suceso o una  $\sigma$ -álgebra como hemos visto previamente.

Partimos igualmente del marco  $(\Omega, \mathcal{A}, P)$  con dos variables aleatorias  $X, Y$ .

**Definición 4.16** Definimos la  $\sigma$ -álgebra generada por la variable aleatoria  $Y$  como la menor  $\sigma$ -álgebra que hace medible a la variable aleatoria  $Y$  y la notaremos como  $\sigma(Y)$ .

Ahora si podemos definir la esperanza de una variable aleatoria condicionada a otra.

**Definición 4.17** Definimos la esperanza de la variable aleatoria  $X$  condicionada a la variable aleatoria  $Y$  como:

$$E[X|Y] = E[X|\sigma(Y)]$$

Como anotación cabe decir que esta esperanza condicionada es una función dependiente de la variable aleatoria  $Y$ , es decir podemos expresarla como:

$$g(y) = E[X|Y = y]$$

Ahora que tenemos la definición de la esperanza condicionada a una variable aleatoria podemos usar el concepto como hemos hecho anteriormente para definir la probabilidad de un suceso condicionado a una variable aleatoria.

**Definición 4.18** Para todo  $A \in \mathcal{A}$  definimos la probabilidad de  $A$  condicionada a la variable aleatoria  $Y$  como:

$$P(A|Y) = E[1_A|\sigma(Y)]$$

*casi seguramente*  $P_{\sigma(Y)}$

Ahora estamos en condiciones de dar una propiedades elementales y de suavizamiento que nos van a dar herramientas con las esperanzas condicionadas. En este punto ya hemos visto que, al haber hecho las definiciones de esperanza y probabilidades usándolas indistintamente las propiedades que vamos a dar para la esperanza se pueden emplear para las probabilidades utilizando sus definiciones que impliquen el uso de esperanzas.

Sobre estas propiedades vamos a realizar algunas de las demostraciones de las propiedades elementales y de las de suavizamiento que vamos a dar para poner de relieve cómo podemos hacer uso de la probabilidad y esperanza condicionada.

**Propiedades 4.3 (Propiedades elementales)** *Partimos de un espacio de probabilidad  $(\Omega, \mathcal{A}, P)$ ,  $\mathcal{U}$  una  $\sigma$ -álgebra contenida en  $\mathcal{A}$  y  $X, Y$  variables aleatorias integrables.*

1.  $E[cte|\mathcal{U}] = cte$  casi seguramente  $P_{\mathcal{U}}$
2. Sean  $a, b \in \mathbb{R}$   $E[aX + bY|\mathcal{U}] = aE[X|\mathcal{U}] + bE[Y|\mathcal{U}]$  casi seguramente  $P_{\mathcal{U}}$ , es decir, la esperanza condicionada cumple la propiedad de linealidad.
3.  $X \geq Y$  casi seguramente  $P \Rightarrow E[X|\mathcal{U}] \geq E[Y|\mathcal{U}]$  casi seguramente  $P_{\mathcal{U}}$ .
4.  $|E[X|\mathcal{U}]| \leq E[|X||\mathcal{U}]$

**Demostración 4.1** *Vamos a demostrar la propiedad 1 para ver como trabajar con las igualdades casi seguras.*

1. Como la igualdad es casi seguramente podemos aplicar integrales en la misma con lo que obtenemos lo siguiente:

$$\forall u \in \mathcal{U} \int_u E[cte|\mathcal{U}] dP_{\mathcal{U}} = \int_u cte dP = cte P(u) = cte P_{\mathcal{U}}(u) = \int_u cte dP_{\mathcal{U}}$$

Como la igualdad es con integrales, podemos decir por tanto que  $E[cte|\mathcal{U}] = cte$  casi seguramente  $P_{\mathcal{U}}$ .

**Propiedades 4.4 (Propiedades de suavizamiento)** *Partimos del marco del espacio probabilístico  $(\Omega, \mathcal{A}, P)$  con una  $\sigma$ -álgebra  $\mathcal{U} \subset \mathcal{A}$ .*

1. Si  $X$  es una variable aleatoria integrable y  $\mathcal{U}$ -medible entonces se tiene que  $E[X|\mathcal{U}] = X$  casi seguramente  $P_{\mathcal{U}}$
2. Sean  $X, Y$  variables aleatorias con  $X$   $\mathcal{U}$ -medible,  $Y$  integrable y  $XY$  integrable, entonces se tiene que  $E[XY|\mathcal{U}] = X E[Y|\mathcal{U}]$  casi seguramente  $P_{\mathcal{U}}$ .
3. Se dice que  $X$  es independiente de  $\mathcal{U}$  si  $X$  y  $1_{\mathcal{U}}$  son independientes. Si  $X$  es independiente de  $\mathcal{U}$  entonces  $E[X|\mathcal{U}] = E[X]$  casi seguramente  $P_{\mathcal{U}}$ .
4. Sean  $\mathcal{U}_1 \subset \mathcal{U}_2 \subset \mathcal{A}$  y  $X$  una variable aleatoria integrable, entonces:

$$E[X|\mathcal{U}_1] = E[E[X|\mathcal{U}_1]|\mathcal{U}_2] = E[E[X|\mathcal{U}_2]|\mathcal{U}_1]$$

casi seguramente  $P_{\mathcal{U}}$ .

Vamos a hacer la demostración de las 4 propiedades para dar así una pincelada de cómo aplicar los conceptos vistos hasta ahora.

**Demostración 4.2** *Demostremos las propiedades de suavizamiento:*

4. Sabemos que  $E[X|\mathcal{U}_1] = Z$  es  $\mathcal{U}_1$ -medible y por tanto es  $\mathcal{U}_2$ -medible, por lo que  $E[Z|\mathcal{U}_2] = Z$  casi seguramente  $P_{\mathcal{U}_2}$ .

Vamos a utilizar ahora el hecho de que las igualdades son casi seguramente y por tanto vamos a ver si aplicando integrales en ambos lados de la igualdad obtenemos el mismo resultado y confirmamos la igualdad.

$$\forall u \in \mathcal{U}_1 \subset \mathcal{U}_2 \text{ tenemos } \int_u E[E[X|\mathcal{U}_1]|\mathcal{U}_2]dP_{\mathcal{U}_2} = \int_u E[X|\mathcal{U}_1]dP_{\mathcal{U}_1} = \int_u XdP$$

Veamos ahora desarrollando el otro término.

$$\int_u E[E[X|\mathcal{U}_2]|\mathcal{U}_1]dP_{\mathcal{U}_1} = \int_u E[X|\mathcal{U}_2]dP_{\mathcal{U}_2} = \int_u XdP$$

Al haber llegado a la misma igualdad en integrales tenemos por tanto la igualdad casi seguramente que buscábamos.

1. Como  $X$  es  $\mathcal{U}$ -medible entonces tenemos que  $\forall u \in \mathcal{U} \int_u E[X|\mathcal{U}]dP_{\mathcal{U}} = \int_u XdP = \int_u XdP_{\mathcal{U}}$  pues al ser  $\mathcal{U}$ -medible tenemos que  $E[X] = \int_{\Omega} XdP = \int_{\Omega} XdP_{\mathcal{U}}$ .
3.  $\forall u \in \mathcal{U} \int_u E[X|\mathcal{U}]dP_{\mathcal{U}} = \int_u XdP = \int_{\Omega} 1_u XdP = E[1_u X] = E[1_u]E[X] = P(u)E[X] = P_{\mathcal{U}}(u)E[X] = \int_u E[X]dP_{\mathcal{U}}$

Ya hemos dado las definiciones y propiedades de probabilidad y esperanza condicionadas, para finalizar vamos a ver algunas desigualdades famosas que utilizaremos y sus demostraciones.

#### 4.1.3. Desigualdades y fórmulas famosas

**Teorema 4.1 (Desigualdad de Markov)** *Sea  $X$  una variable aleatoria que toma valores no negativos. Entonces para cualquier constante  $\alpha$  satisfaciendo  $E[X] < \alpha$  se cumple que:*

$$P(X > \alpha) \leq \frac{E[X]}{\alpha}$$

**Demostración 4.3** *Denotemos como  $f_X(x)$  la función de densidad de la variable aleatoria  $X$ . Entonces tenemos:*

$$\begin{aligned}
E[X] &= \int_x x f_X(x) dx = \int_{0 \leq x \leq \alpha} x f_X(x) dx + \int_{x > \alpha} x f_X(x) dx \\
&\geq \int_{x > \alpha} x f_X(x) dx \geq \int_{x > \alpha} \alpha f_X(x) dx
\end{aligned}$$

La primera de las desigualdades se sigue de la no negatividad de  $X$  y la segunda se sigue de que la integral está definida sobre los puntos en los que  $x > \alpha$ , de hecho:

$$\int_{x > \alpha} \alpha f_X(x) dx = \alpha P(X > \alpha)$$

Con lo que tenemos finalmente que:

$$E[X] \geq \alpha P(X > \alpha) \Leftrightarrow P(X > \alpha) \leq \frac{E[X]}{\alpha}$$

■

**Teorema 4.2 (Desigualdad de Chebychev)** Sea  $X$  una variable aleatoria arbitraria. Entonces para cualquier constante  $\alpha$  se tiene que:

$$P(|X - E[X]| > \alpha) \leq \frac{\text{Var}[X]}{\alpha^2}$$

**Demostración 4.4** Sabemos que la desigualdad  $|X - E[X]| > \alpha$  es cierta si y sólo si  $|X - E[X]|^2 > \alpha^2$

Vamos a definir la variable aleatoria  $Y = (X - E[X])^2$  es es no negativa. Con esta definición se tiene que  $E[Y] = \text{Var}[X]$  por la propia definición de la variable aleatoria  $Y$ .

Entonces la parte izquierda de la desigualdad del teorema se puede expresar como  $P(|X - E[X]| > \alpha) = P(Y > \alpha^2)$ . Aplicando aquí la desigualdad de Markov obtenemos que:

$$P(Y > \alpha^2) \leq \frac{E[Y]}{\alpha^2} = \frac{\text{Var}[X]}{\alpha^2}$$

■



**Teorema 4.3 (Cota inferior de Chernoff)** Sea  $X$  una variable aleatoria que se puede expresar como la suma de  $N$  variables aleatorias independientes de Bernoulli, cada una tomando el valor 1 con probabilidad  $p_i$ .

$$X = \sum_{i=1}^N X_i$$

Entonces para todo  $\delta \in (0, 1)$  tenemos que:

$$P(X < (1 - \delta)E[X]) < e^{-E[X]\delta^2/2}$$

**Teorema 4.4 (Cota superior de Chernoff)** Sea  $X$  una variable aleatoria que se puede expresar como la suma de  $N$  variables aleatorias independientes de Bernoulli, cada una tomando el valor 1 con probabilidad  $p_i$ .

$$X = \sum_{i=1}^N X_i$$

Entonces para todo  $\delta \in (0, 2 \cdot e - 1)$  tenemos que:

$$P(X > (1 + \delta)E[X]) < e^{-E[X]\delta^2/2}$$

Ambas cotas disponen de una demostración que no es constructiva, por lo que no es relevante su demostración para el estudio. Como ejemplo de una demostración de un estilo similar haremos la demostración de la siguiente desigualdad.

**Teorema 4.5 (Desigualdad de Hoeffding)** Sea  $X$  una variable aleatoria que se puede expresar como suma de  $N$  variables aleatorias independientes acotadas en intervalos  $[l_i, u_i]$ .

$$X = \sum_{i=1}^N X_i$$

Entonces para todo  $\theta > 0$  se tienen las cotas:

$$P(X - E[X] > \theta) \leq e^{-\frac{2\theta^2}{\sum_{i=1}^N (u_i - l_i)^2}}$$

$$P(E[X] - X > \theta) \leq e^{-\frac{2\theta^2}{\sum_{i=1}^N (u_i - l_i)^2}}$$

**Demostración 4.5** *Sólo haremos la demostración de la primera desigualdad de forma resumida y sin entrar en los detalles más complejos que se alejan del interés del estudio.*

*En primer lugar debemos probar que para todo  $t \geq 0$  se cumple la desigualdad:*

$$P(X - E[X] > \theta) = P(e^{t(X-E[X])} > e^{t\theta})$$

*Usando la desigualdad de Markov podemos probar que  $P(e^{t(X-E[X])} > e^{t\theta})$  es como mucho  $E[e^{t(X-E[X])}]e^{-t\theta}$ .*

*Además al ser variables aleatorias independientes las que componen la variable aleatoria  $X$  podemos descomponer el término teniendo la desigualdad:*

$$P(X - E[X] > \theta) \leq e^{-t\theta} \prod_i E[e^{t(X_i - E[X_i])}]$$

*Cada uno de los términos de este producto se puede probar que vale como mucho  $e^{t^2(u_i - l_i)/8}$  usando argumentos de convexidad y el Teorema de Taylor.*

*Por tanto se cumple:*

$$P(X - E[X] > \theta) \leq e^{-t\theta} \prod_i e^{t^2(u_i - l_i)^2/8}$$

*Nos interesa hallar el valor de  $t = t^*$  que ajusta la desigualdad. Puede demostrarse que ese valor es:*

$$t^* = \frac{4\theta}{\sum_{i=1}^N (u_i - l_i)^2}$$

*Sustituyendo en la desigualdad con este valor de  $t$  tenemos el resultado que queríamos probar.* ■

## Capítulo 5

# Concepto probabilístico de anomalía

Tras la introducción dada de estadística multivariante ya tenemos los conceptos necesarios para dar la definición alternativa de anomalía basada en probabilidades. Esta definición cabe decir que no es alternativa a la basada en distancias, si no complementaria y propuesta en el artículo que describe el modelo HICS [4].

En primer lugar cabe decir que esta definición, al igual que el criterio ya explicado no engloba todas las anomalías y por tanto es algo difícil de medir. Esta definición hace referencia, según mi criterio, a un enfoque que se debe poner junto a la definición basada en distancias y no en contraposición. El objetivo de esta definición es obtener anomalías que no son triviales y se esconden entre los datos.

La base del razonamiento de este tipo de anomalías surge del hecho de que un objeto puede ser anómalo en un subespacio concreto de los datos, pero no en el espacio total. Vamos a introducir un ejemplo para visualizar un tipo de anomalía que encaje con esta definición.

Veamos la siguiente figura:

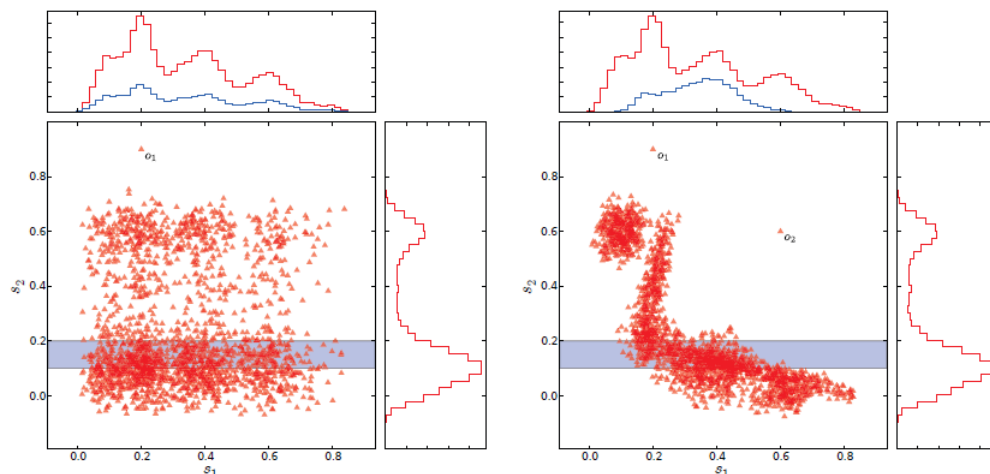


Figura 5.1: Ejemplo de anomalía [4]

Como se puede observar tenemos dos espacios: el izquierdo no presenta datos correlados y el derecho sí presenta correlación. Podemos ver que en ambos casos se comparte una anomalía etiquetada como  $O_1$ . Esta anomalía en el caso del espacio no correlado es perfectamente detectable de forma trivial observando las proyecciones de los datos en una dimensión. En cambio en el segundo caso ninguna de las dos anomalías etiquetadas  $O_1, O_2$  son detectables de esta forma trivial, pues si hacemos las proyecciones uno dimensionales ninguno de los dos datos es discordante en dichas proyecciones. Estas anomalías son las que decimos que son no triviales. En cambio si observamos los datos en una proyección de orden superior como la que estamos viendo de dimensión 2 podemos observar claramente que se salen de la correlación de datos que muestra el resto. Es aquí donde podemos ver que en el conjunto de la derecha ninguno de los puntos es una anomalía en las proyecciones de dimensión uno pero sí lo son en la proyección de dimensión 2.

Vamos por tanto a definir más formalmente este concepto especial de anomalía. Necesitamos introducir en primer lugar un poco de notación.

Partimos de un conjunto de datos  $X = \{x_1, \dots, x_n\}$  de  $n$  objetos cada uno tomando  $d$  valores, es decir,  $x_i = (x_{s_1}, \dots, x_{s_d}) \in \mathbb{R}^d$ . Notamos un subespacio del conjunto de valores como:

$$S = \{s_i | s_i \in \{s_1, \dots, s_d\} \text{ con } i \in \Delta\}$$

Dado un subespacio  $S = \{s_1, \dots, s_p\}$  notamos la proyección de los objetos del conjunto de datos como  $X_S = \{x_{s_1}, \dots, x_{s_p}\}$ .

Esta proyección está distribuida según una distribución conjunta desconocida de  $S$ :

$$p_{s_1, \dots, s_p}(x_{s_1}, \dots, x_{s_p})$$

Notamos la distribución marginal asociada al atributo  $s_i$  como:

$$p_{s_i}(x_{s_i})$$

**Definición 5.1** *Decimos que un subespacio  $S$  es un espacio incorrelado si y sólo si:*

$$p_{s_1, \dots, s_p}(x_{s_1}, \dots, x_{s_p}) = \prod_{i=1}^p p_{s_i}(x_{s_i})$$

Por tanto si estamos bajo la suposición de un espacio incorrelado podemos decir que la densidad esperada es:

$$p_{esp}(x_{s_1}, \dots, x_{s_p}) \equiv \prod_{i=1}^p p_{s_i}(x_{s_i})$$

Recordemos que nuestras anomalías no triviales no están en este tipo de subespacios, si no en los correlados. Por tanto vamos a definirlo de la siguiente forma:

**Definición 5.2** *Decimos que un objeto  $x_S$  es una anomalía no trivial respecto al subespacio  $S$  si:*

$$p_{s_1, \dots, s_p}(x_{s_1}, \dots, x_{s_p}) \ll p_{esp}(x_{s_1}, \dots, x_{s_p})$$

*Es decir, si la probabilidad esperada es significativamente mayor que la probabilidad conjunta.*

Por cómo hemos definido los espacios correlados e incorrelados es claro que no podemos tener anomalías en espacios no correlados como es evidente pues la densidad conjunta y esperada serían iguales.

Este concepto como podemos observar no comparte ninguna relación con nuestra definición de anomalías basadas en distancias por lo que es de esperar que si comparamos ambos tipos de anomalías en un conjunto de datos no obtengamos los mismos objetos.

## Parte III

# Explicación de los modelos y análisis de resultados





## Capítulo 6

# Modelos implementados

En este capítulo vamos a repasar qué modelos he implementado y cómo funcionan cada uno de ellos. Primero se hará una revisión teórica de los modelos y posteriormente un análisis breve del código explicando las particularidades de las implementaciones. El contenido de esta sección se basa en los libros de Aggarwal Outlier Analysis [44] y Outlier Ensembles [43] y en los artículos de HICS [4], LODA [31] y OUTRES [24].

### 6.1. Algoritmos de ensamblaje

Los algoritmos que he implementado pertenecen a una familia concreta de algoritmos de detección de anomalías denominados como algoritmos de ensamblaje o “Ensemble Algorithms” en inglés. Estos algoritmos son lo equivalente a los meta-algoritmos pero destinados a la detección de anomalías. Para dar una mejor definición de qué son los algoritmos de ensamblaje vamos a introducir una clasificación de los mismos para dar las categorías que entran dentro de esta definición.

- Algoritmos de ensamblaje secuenciales: En este tipo de algoritmos tenemos un algoritmo base o un conjunto de algoritmos base que se aplican de forma secuencial, de forma que las primeras ejecuciones se ven usadas o modificadas por ejecuciones futuras de algoritmos. Finalmente el resultado puede ser una combinación ponderada de las

valoraciones de los algoritmos o el resultado del último de ellos.

**Ensamblaje secuencial:**

**Entrada:** Conjunto de datos  $\mathcal{D}$ , Algoritmos base  $\mathcal{A}_1, \dots, \mathcal{A}_r$   
 $j=1$   
**repetir**  
    Tomamos el algoritmo  $\mathcal{A}_j$  según los resultados anteriores  
    Tomamos el conjunto de datos modificado  $f_j(\mathcal{D})$  de anteriores ejecuciones  
    Ejecutamos el algoritmo  $\mathcal{A}_j$  sobre  $f_j(\mathcal{D})$   
     $j=j+1$   
**hasta que** *fin*;  
**Resultado:** Combinación de los resultados

- Algoritmos de ensamblaje independientes: En este caso se emplean o bien diferentes instancias del mismo algoritmo o bien diferentes porciones de los datos que se emplearán de forma distinta. Se puede variar la instanciación por ejemplo dependiendo del subespacio sobre el que queramos ejecutarlo o dependiendo de las características de una porción concreta de los datos.

**Ensamblaje independiente:**

**Entrada:** Conjunto de datos  $\mathcal{D}$ , Algoritmos base  $\mathcal{A}_1, \dots, \mathcal{A}_r$   
 $j=1$   
**repetir**  
    Tomamos el algoritmo  $\mathcal{A}_j$   
    Creamos el conjunto de datos modificado  $f_j(\mathcal{D})$   
    Ejecutamos el algoritmo  $\mathcal{A}_j$  sobre  $f_j(\mathcal{D})$   
     $j=j+1$   
**hasta que** *fin*;  
**Resultado:** Combinación de los resultados

## 6.2. Mahalanobis Kernel

Este algoritmo está englobado dentro de la categoría de algoritmos basados en dependencia. Esta clase de algoritmos intenta estudiar las dependencias que existen entre atributos para así poder detectar las instancias u objetos que no tienen estas dependencias y marcarlos como anomalías.

Si intentamos visualizar esta dependencia entre atributos de forma gráfica lo que observaríamos es que los datos están alineados o posicionados en hiperplanos lineales o no lineales de la siguiente forma:



Figura 6.1: Hiperplano

Esta figura es un ejemplo clásico de estudio de algoritmos como por ejemplo PCA (algoritmo que quedaría dentro de esta categoría).

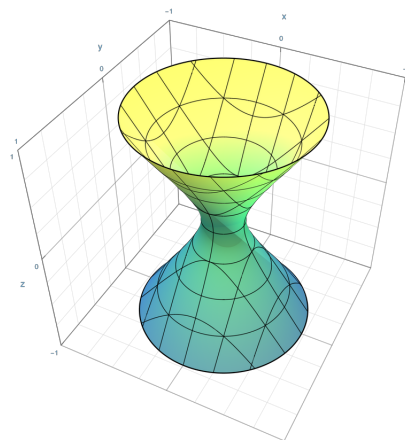


Figura 6.2: Hiperboloide Wikimedia

En este caso tenemos el ejemplo de un hiperboloide que no tiene una dependencia lineal, si no que presenta una dependencia de tipo cuadrático.

El método de Mahalanobis Kernel puede ser visto como una modificación de PCA. PCA básicamente dispone de dos pasos:

1. Determinar un sistema ortogonal de direcciones principales y proyectar los datos sobre este sistema.

2. Calcular la distancia entre el punto original y la proyección como su puntuación de anomalía.

El método Mahalanobis Kernel intenta tener este mismo comportamiento en dos pasos y que ahora veremos. El algoritmo PCA es muy útil cuando los datos tienen atributos relacionados en un hiperplano, mientras que Mahalanobis Kernel funciona mejor cuando los datos están relacionados en formas más complejas como el hiperboloide que hemos enseñado. La elección de este algoritmo en vez de PCA recae en el hecho de que PCA es un algoritmo clásico y el escenario en el que mejor funciona (hiperplano) es más restrictivo que el que nos ofrece Mahalanobis Kernel con un abanico de figuras más amplio.

Vamos a describir el funcionamiento del algoritmo, pero primero vamos a introducir notación. Vamos a llamar  $D$  a la matriz de datos que está centrada en la media y que tiene dimensiones  $n \times d$ , es decir, tenemos  $n$  instancias u objetos de dimensionalidad  $d$ .

#### Mahalanobis Kernel

**Entrada:**  $D$

$$S = DD^T.$$

$$S = Q\Delta^2Q^T.$$

Almacenamos los vectores propios columna no negativos de  $Q\Delta$  en una matriz  $D'$

Normalizamos  $D'$  para que tenga media 0 y varianza 1.

$$\text{vector\_media} = \text{media}(D')$$

$$\text{puntuaciones} = []$$

**para cada fila en  $D'$  hacer**

$$\begin{array}{|l} \text{score} = \text{distancia}(\text{vector\_media}, \text{fila}) \\ \text{puntuaciones} = [\text{puntuaciones}, \text{score}] \end{array}$$

**fin**

**Salida:** puntuaciones

#### Algoritmo 1: Mahalanobis Kernel

El algoritmo comienza con la matriz de datos  $D$ . Se obtiene la matriz simétrica  $S$  y se hace la descomposición en valores singulares.

Con este modelo tenemos las dos fases que teníamos en PCA. Primero obtenemos una matriz  $D'$  de los datos proyectados y transformados para posteriormente reportar la puntuación de anomalía como una distancia.

Veamos ahora la implementación en Python.

```
1 def runMethod(self):
2     ...
```

```

3      @brief Function that executes the Kernel Mahalanobis
        method. The results are
4      stored on the variable self.scores
5      @param self
6      '''
7      ''' Compute the S matrix of the algorithm'''
8      S = np.dot(self.dataset, self.dataset.T)
9      ''' Now we diagonalize it'''
10     Q,delta_sq,Qt = np.linalg.svd(S)
11     del S
12     del Qt
13     ''' Obtain delta as matrix'''
14     delta = np.matrix(np.diag(np.sqrt(delta_sq)))
15     del delta_sq
16     Q = np.matrix(Q)
17     ''' Compute de D' matrix and normalize it'''
18     Dprime = np.dot(Q,delta)
19     del Q
20     del delta
21     Dp_std = scale(Dprime, axis=1)
22     del Dprime
23     ''' We compute its mean on the rows to compute the
        deviation as the score'''
24     mean = Dp_std.mean(axis=0)
25     self.outlier_score=[]
26     ''' The score is the euclidean distance to the mean'''
27     for i in range(len(Dp_std)):
28         self.outlier_score.append(np.linalg.norm(mean-
            Dp_std[i])**2)
29     self.outlier_score = np.array(self.outlier_score)
30     self.calculations_done=True

```

La implementación del algoritmo se ha realizado en Python como el resto del proyecto y posteriormente se explicará en detalle cómo se ha organizado.

El algoritmo basa su implementación en la librería NumPy.

### 6.3. TRINITY

Este algoritmo es del segundo tipo que vimos al principio cuando hicimos una categorización de los algoritmos de ensamblaje, en concreto el algoritmo hace una combinación de tres componentes distintos. La intención de hacer esta composición de modelos es intentar obtener todos los tipos de anomalías que se puedan del conjunto y que reciban una puntuación acorde. La teoría nos dice que esta combinación de modelos nos va a proveer de un resultado más robusto que el uso de modelos aislados como discutiremos en la sección

de resultados.

En concreto este algoritmo consta de tres componentes distintos:

- **Componente basado en distancias:** este componente consta de un algoritmo que base su comportamiento en técnicas de agrupamiento o valoración por distancias como por ejemplo es el método clásico KNN. Este método lo que hace es tomar los  $k$  vecinos más cercanos y colocar como puntaje de anomalía para esa instancia como la suma de estas distancias. De esta forma los puntos que más alejados estén del resto sumarán una mayor distancia y por tanto serán más anómalos. En concreto este modelo se ha utilizado con el valor  $k = 5$  y con una técnica de subsampling. La técnica de subsampling consiste en no utilizar todo el conjunto de datos en el algoritmo, si no partitionarlo y utilizar una pequeña muestra repitiendo este proceso y haciendo la media de las ejecuciones. De esta forma conseguimos una reducción de la varianza. Esto conlleva algunas ventajas como discutimos en la sección de sesgo y varianza anteriormente. En concreto la técnica toma 1000 particiones, ejecuta el algoritmo sobre ellas y hace la media.
- **Componente basado en dependencia:** este componente toma un algoritmo como el que hemos implementado (Mahalanobis Kernel). En este componente vamos a intentar detectar las anomalías que corresponden a datos que no siguen las relaciones entre atributos que sí tienen el resto de los objetos. Para ello he utilizado en este componente el algoritmo Mahalanobis Kernel que ya hemos explicado anteriormente incorporando la técnica de subsampling.
- **Componente basado en densidad en subespacios:** en este componente vamos a incorporar un modelo que intente buscar anomalías que lo sean en base a la densidad que tienen en alguno de los subespacios de los datos. Este hecho no nos debe ser ajeno pues es la segunda de las definiciones que hemos visto de anomalía y que hacía referencia a la función de densidad y los subespacios incorrelados y correlados. En concreto para este componente he utilizado el algoritmo IForest o Isolation Forest. Este algoritmo lo que hace es tomar de forma aleatoria un atributo y se van partitionando los valores del mismo en una estructura de árbol, es decir, dividimos los datos en aquellos con un valor superior al marcado para el atributo y con un valor menor. De esta forma podemos medir cuántos pasos o lo que es lo mismo qué profundidad ha alcanzado nuestro árbol hasta llegar a dividir un objeto del resto de los datos. Este algoritmo también incorpora la técnica de subsampling.

Por último con esto hemos obtenido tres vectores o listas con la puntuación que cada componente nos ha arrojado para cada instancia. Para hacerlos comparables lo que debemos hacer es estandarizar los datos a media cero y varianza unitaria. Finalmente se realiza la media de los tres vectores de puntaje siendo esta la puntuación final devuelta por TRINITY.

Veamos la implementación de este algoritmo:

```

1 def distanceBased(self):
2     '''
3     @brief Function that implements the distance based
4         component
5     @param self
6     @return It returns the vector with the scores of the
7         instances
8     '''
9     ''' Initialize the scores'''
10    scores = np.array([0]*len(self.dataset)).astype(float)
11    for i in range(self.num_iter):
12        knn = KNN(n_neighbors=5, contamination=self.
13            contamination)
14        ''' Number in the interval [50, 1000]'''
15        subsample_size = np.random.randint(50, 1001)
16        sample = []
17        if subsample_size>=len(self.dataset):
18            sample = list(range(len(self.dataset)))
19        else:
20            ''' Take the sample and train the model'''
21            sample = np.random.choice(len(self.dataset),
22                size=subsample_size, replace=False)
23            knn.fit(self.dataset[sample])
24            ''' Update the score to compute the mean'''
25            scores[sample]+=knn.decision_scores_
26        ''' Return the mean'''
27    scores = scores/self.num_iter
28    scores = scale(scores)
29    return scores
30
31 def dependencyBased(self):
32     '''
33     @brief Function that implements the dependency based
34         component
35     @param self
36     @return It returns the vector with the scores of the
37         instances
38     '''
39     ''' Initialize the scores'''
40    scores = np.array([0]*len(self.dataset)).astype(float)
41    for i in range(self.num_iter):

```

```

36         kernel_mahalanobis = KernelMahalanobis(
37             contamination=self.contamination)
38         subsample_size = np.random.randint(50, 1001)
39         sample = []
40         if subsample_size >= len(self.dataset):
41             sample = list(range(len(self.dataset)))
42         else:
43             ''' Take the sample and train the model'''
44             sample = np.random.choice(len(self.dataset),
45                                     size=subsample_size, replace=False)
46             kernel_mahalanobis.fit(self.dataset[sample])
47             ''' Update the score to compute the mean'''
48             scores[sample] += kernel_mahalanobis.outlier_score
49         ''' Return the mean'''
50         scores = scores/self.num_iter
51         scores = scale(scores)
52         return scores
53     def densityBased(self):
54         '''
55         @brief Function that implements the dependency based
56             component
57         @param self
58         @return It returns the vector with the scores of the
59             instances
60         '''
61         ''' Initialize the scores'''
62         scores = np.array([0]*len(self.dataset)).astype(float)
63         for i in range(self.num_iter):
64             iforest = IForest(contamination=self.contamination
65                             , behaviour="new")
66             ''' Number in the interval [50, 1000]'''
67             subsample_size = np.random.randint(50, 1001)
68             sample = []
69             if subsample_size >= len(self.dataset):
70                 sample = list(range(len(self.dataset)))
71             else:
72                 ''' Take the sample and train the model'''
73                 sample = np.random.choice(len(self.dataset),
74                                         size=subsample_size, replace=False)
75                 iforest.fit(self.dataset[sample])
76                 ''' Update the score to compute the mean'''
77                 scores[sample] += iforest.decision_scores_
78             ''' Return the mean'''
79             scores = scores/self.num_iter
80             scores = scale(scores)
81         return scores

```



```
79 def runMethod(self):
80     '''
81     @brief This function is the actual implementation of
82           TRINITY
83     @param self
84     '''
85     ''' Distance module'''
86     if self.verbose:
87         print("Obtaining scores with the distance module")
88     distance_based = self.distanceBased()
89     ''' dependency module'''
90     if self.verbose:
91         print("Obtaining scores with the dependency module")
92     dependency_based = self.dependencyBased()
93     ''' Density module'''
94     if self.verbose:
95         print("Obtaining scores with the density module")
96     density_based = self.densityBased()
97     ''' Compute the mean of the three modules'''
98     self.outlier_score=(distance_based + dependency_based
99                        + density_based)/3
100     self.calculations_done=True
```

Todos los módulos tienen una función parecida. En primer lugar se inicializan las puntuaciones y se repite el mismo proceso de cálculo 100 veces. Se inicializa el modelo y se ajusta con una muestra de tamaño en el intervalo [50, 1000]. Por último se hace la media de todos los cálculos y se estandarizan con la librería Sklearn.

En la función principal “runMethod” se ejecutan los tres módulos y se hace la media de las puntuaciones.

## 6.4. OUTRES

Este método entra dentro del segundo de los tipos que hemos visto en la clasificación inicial pues el objetivo es analizar los datos por subespacios. Una de las cosas que podremos ver al final cuando hagamos el estudio de los resultados es lo costoso de estos métodos, siendo este el primero que nos va a servir de ejemplo para visualizar este problema.

En primer lugar cabe decir que en el resto de algoritmos las puntuaciones reflejan el factor de anomalía en orden creciente, es decir, a mayor puntaje más anómalo es el dato y a menor puntaje menos anómalo se dice que es.

En este caso los puntajes van a estar en el intervalo  $[0, 1]$  siendo 0 un puntaje para un dato lo más anómalo posible y 1 un puntaje para un dato lo más normal posible. Daremos razones para que esto sea así cuando veamos el algoritmo.

### OUTRES

**Entrada:**  $o$ : instancia,  $S$ : subespacio

**para cada**  $i \in (D \setminus S)$  **hacer**

$S' = S \cup \{i\}$

**si**  $S'$  *es relevante* **entonces**

$den(o, S') = \frac{1}{n} \sum_{p \in AN(o, S')} K_e\left(\frac{dist_{S'}(o, p)}{\epsilon(|S'|)}\right)$

$dev(o, S') = \frac{\mu - den(o, S')}{2\sigma}$

**si**  $dev(o, S') \geq 1$  **entonces**

$r(o) = r(o) \cdot \frac{den(o, S')}{dev(o, S')}$

**fin**

$OUTRES(o, S')$

**fin**

**en otro caso**

| Para recursividad

**fin**

**fin**

**Salida:**  $r$ : puntajes

### Algoritmo 2: OUTRES

En primer lugar tenemos que definir qué son los espacios relevantes. Decimos que un subespacio  $S$  es relevante si la proyección sobre ese subespacio no está distribuida de uniformemente. No podemos hacer un test de que toda la proyección esté distribuida uniformemente por lo que nos vamos a valer del siguiente teorema:

**Teorema 6.1** *Sea  $S$  un subespacio del conjunto de datos. Si  $S$  está distribuido uniformemente entonces  $\forall s_i \in S$  tenemos que la proyección uno-dimensional del conjunto de datos sobre  $s_i$  está distribuida uniformemente.*

Este teorema nos da la siguiente herramienta: si comprobamos que ninguna proyección uno-dimensional está distribuida uniformemente entonces podemos afirmar que  $S$  está distribuido uniformemente. Para hacer estas comprobaciones uno-dimensionales lo hemos hecho mediante el test de Kolmogorov-Smirnov.

Además el algoritmo incorpora un nuevo concepto. Los datos tienen mayor relevancia cuando los consideramos en subespacios y cuando los metemos dentro de lo que los autores llaman vecindarios adaptativos. La definición

de un vecindario adaptativo es la siguiente:

**Definición 6.1** *Definimos para la instancia u objeto  $o$  en el subespacio  $S$  su vecindario adaptativo como:*

$$AN(o, S) = \{p | dist_S(o, p) \leq \epsilon(|S|)\}$$

Donde  $dist_S$  es la función distancia sobre los atributos  $S$ . Aquí tenemos una distancia máxima definida en función del cardinal del subespacio que viene dada de la siguiente forma:

$$\epsilon(|S|) = 0.5 \cdot \frac{h_{optimal}(|S|)}{h_{optimal}(2)}$$

Donde:

$$h_{optimal}(d) = \left( \frac{8\Gamma(\frac{d}{2} + 1)}{\pi^{\frac{d}{2}}} (d + 4) (2\sqrt{\pi})^d \right) n^{\frac{-1}{d+4}}$$

Donde  $\Gamma$  denota la función gamma y  $n$  es el tamaño del conjunto de datos, es decir, el número de objetos o instancias.

Con esto ya tenemos la definición del vecindario adaptativo y el objeto de tenerlo es poder comprobar que el la instancia  $o$  es relevante en el subespacio  $S$  dentro de su vecindario adaptativo.

En cuanto a la definición de densidad tenemos la función  $K_\epsilon$  que es el llamado Kernel de Epachenikov. Esta función está definida como:

$$K_\epsilon(x) = (1 - x^2) \forall x < 1$$

En cuanto al  $\mu$  y  $\sigma$  que aparecen en el cálculo de la desviación son la media y la desviación típica de las densidades en el vecindario adaptativo de  $o$  en el subespacio  $S$ . Por tanto con la desviación estamos midiendo cómo de alejada está la instancia  $o$  en densidad respecto del resto de las instancias de su vecindario adaptativo. Si esta densidad es mayor a dos desviaciones típicas entonces  $dev(o, S')$  será mayor que 1 y por tanto estaremos ante un dato anómalo.

Si este es el caso, al estar los puntajes de anomalías inicializados a 1 podemos actualizarlo multiplicando por un valor menor estricto que 1. En

este caso este valor es  $\frac{den(o, S')}{dev(o, S')}$ . Como este valor es menor que 1 reducirá el puntaje y lo acercará más a una anomalía. De esta forma cuantas más veces se actualice su puntaje y cuanto menor puntaje obtenga con  $\frac{den(o, S')}{dev(o, S')}$  más anómalo consideraremos el dato.

Finalmente si el subespacio era relevante significa que aún podemos aumentar más la dimensionalidad pues puede que nos queden subespacios de mayor orden que sigan sin estar distribuidos según una uniforme.

Como dato cabe decir que el algoritmo empieza en dimensión 2 y no en dimensión 1 pues en una única dimensión no tiene sentido estudiar la densidad ya que no vamos a sacar información de calidad.

Veamos la implementación

```

1 def isRelevantSubspace(self, subspace, neighborhood):
2     '''
3     @brief Function that tells if a subspace is relevant,
4     this is that the projection
5     of the dataset over the subspace is not distributed
6     uniformly in the neighborhood
7     @param self
8     @param subspace Subspace to check
9     @param neighborhood neighborhood in which to check the
10    projection
11    @return It returns True if the subspace is relevant,
12    False in other case.
13    '''
14    ''' We check first if we have already considered this
15    subspace. If so, it is not relevant anymore.'''
16    for sub in self.checked_subspaces:
17        if len(np.intersect1d(sub, subspace))==len(
18            subspace):
19            return False
20
21    ''' Make the projection'''
22    projection = self.dataset[:,subspace][neighborhood]
23    if len(projection)==0:
24        return False
25    ''' We check for each subspace if the 1-dimensional
26    data is uniformly distributed'''
27    for i in range(len(subspace)):
28        min = np.amin(projection[:,i].reshape(-1))
29        max = np.amax(projection[:,i].reshape(-1))
30        ''' We do it using the Kolmogorov-Smirnov test'''
31        d,p = kstest(projection[:,i], "uniform", args=(min
32            , max-min))
33        ''' If the null hypothesis is not rejected, this

```

```

        means the data follow a uniform distribution
        '''
26         if p<=self.alpha:
27             return False
28         return True
29
30     def computeHOptimal(self, d):
31         '''
32         @brief Function that calculates the Hoptimal
33         @param self
34         @param d Parameter, usually the dimensionality of the
35             subspace
36         @return It returns a numerical value.
37         '''
38         f1 = (8*gamma(d/2 + 1))/(np.power(np.pi, d/2))
39         f2 = d+4
40         f3 = np.power(2*np.sqrt(np.pi),d)
41         n = len(self.dataset)
42         f4 = np.power(n, -1/(d+4))
43         return f1*f2*f3*f4
44
45     def computeEpsilon(self, subspace):
46         '''
47         @brief Function to compute the epsilon of the
48             adaptative neighborhood
49         @param self
50         @params subspace Subspace considered to compute the
51             epsilon
52         @return It returns a numerical value
53         '''
54         return 0.5*(self.computeHOptimal(len(subspace))/self.
55             computeHOptimal(2))
56
57     def computeNeighborhood(self, subspace, instance):
58         '''
59         @brief This function computes the adaptative
60             neighborhood
61         @param subspace Subspace in which to compute the
62             neighborhood
63         @param instance Instance considered as the centroid of
64             the neighborhood (index of the element)
65         @return It returns a numpy array containing the
66             indexes of the neighborhood
67         '''
68         # First we compute the projection
69         projection = self.dataset[:,subspace]
70         # We compute a numpy array of the distances of all the
71         # elements to the instance
72         tile = np.tile(projection[instance], len(self.dataset)

```

```

        ).reshape((len(self.dataset),len(projection[
        instance])))
64     distances = np.linalg.norm(projection-tile, axis=1)
65     # We keep only the ones that are close enough (epsilon
        distance as max)
66     neighborhood = np.where(distances<self.epsilons[len(
        subspace))][0]
67     # We exclude the instance itself
68     return neighborhood[neighborhood!=instance]
69
70 def computeKernel(self, x):
71     '''
72     @brief Function that computes the Epanechnikov kernel
        with scalar factor 1
73     @param self
74     @param x Number between 0 and 1.
75     @return It returns a numerical value
76     '''
77     return 1-np.power(x,2)
78
79 def computeDensity(self, subspace, neighborhood, instance)
    :
80     '''
81     @brief This is the function that computes the density
82     @param self
83     @param subspace Subspace in which to compute the
        density
84     @param neighborhood Adaptative neighborhood for the
        instance in the subspace
85     @param instance Index of the instance considered at
        the moment
86     @return It return a numerical value.
87     '''
88     # Compute the projection
89     projection = self.dataset[:,subspace]
90     # Compute the density
91     tile = np.tile(projection[instance], len(self.dataset)
        ).reshape((len(self.dataset),len(projection[
        instance])))
92     return np.sum(self.computeKernel(np.linalg.norm(
        projection-tile, axis=1))/self.computeEpsilon(
        subspace))/len(self.dataset)
93
94 def computeDeviation(self, subspace, neighborhood,
    instance, density):
95     '''
96     @brief Function that computes the deviation
97     @param self
98     @param subspace Subspace considered to compute the

```

```

    deviation
99     @param neighborhood Adaptative neighborhood for the
        instance in the subspace
100     @param instance Instance to compute the deviation
101     @param density Density value of the instance
102     @return It returns a numerical value
103     '''
104     ''' First we need to compute the density for all the
        neighbors'''
105     densities = np.array([])
106     for neig in neighborhood:
107         local_neighborhood = self.computeNeighborhood(
            subspace, neig)
108         densities = np.append(densities, self.
            computeDensity(subspace, local_neighborhood,
            neig))
109     ''' We compute the mean and the standard deviation'''
110     mean = np.mean(densities)
111     stdv = np.std(densities)
112     ''' Return the deviation'''
113     return (mean-density)/(2*stdv)
114
115 def outres(self, instance, subspace):
116     '''
117     @brief Main loop of the outres algorithm
118     @param self
119     @param instance Instance to compute the outres score
120     @param subspace Initial subspace of dimension 1
121     '''
122     ''' First we compute the indexes of the features that
        are not used in the actual subspace'''
123     available_indexes = list(set(list(range(len(self.
        dataset[0])))).difference(set(list(subspace))))
124     ''' For each available index we are going to check'''
125     for index in available_indexes:
126         ''' We make the new subspace adding the index'''
127         new_subspace = np.append(subspace, int(index)).
            astype(int)
128         ''' We compute the adaptative neighborhood'''
129         neighborhood = self.computeNeighborhood(
            new_subspace, instance)
130         ''' If the subspace is relevant'''
131         if self.isRelevantSubspace(new_subspace,
            neighborhood):
132             ''' Compute the density and deviation'''
133             density = self.computeDensity(new_subspace,
                neighborhood, instance)
134             deviation = self.computeDeviation(new_subspace
                , neighborhood, instance, density)

```

```

135         ''' If it is a high deviating instance in the
136         subspace then we update the score'''
137         if deviation>=1:
138             if self.verbose:
139                 print("The instance " + str(instance
140                     +1) + " is outlying in the
141                     subspace " + str(new_subspace))
142                 ''' The scores are equal to 1 at first and
143                 1 means no outlieriness and 0 means
144                 very outlying'''
145                 self.outlier_score[instance]*=density/
146                 deviation
147                 ''' We keep the process if the subspace was
148                 relevant'''
149                 self.outres(instance, new_subspace)
150                 ''' We add the subspace to the considered ones'''
151                 self.checked_subspaces.append(new_subspace)
152
153     def runMethod(self):
154         '''
155         @brief This function is the actual implementation of
156         OUTRES
157         '''
158         ''' First we compute all epsilons so we dont need to
159         make this calculation more than once'''
160         self.epsilons = [self.computeEpsilon(list(range(n)))
161             for n in range(len(self.dataset[0])+1)]
162
163         ''' We initialize the scores to one'''
164         self.outlier_score = np.ones(len(self.dataset))
165         ''' For each instance we run outres'''
166         for i in range(len(self.dataset)):
167             ''' Erase checked_subspaces'''
168             self.checked_subspaces = []
169             if self.verbose and i%25==0:
170                 print("Computing the instance " + str(i+1) +
171                     "/" + str(len(self.dataset)))
172             ''' We run for each instance each index'''
173             for j in range(len(self.dataset[0])):
174                 self.outres(i,np.array([j]))
175         ''' At the end, score 1 means no outlieriness and 0
176         100% outlier. We make 1-score
177         so we can keep the ascending order and now this will
178         mean that 0 is no outlieriness
179         and 1 is very outlying.'''
180         self.outlier_score = np.ones(len(self.dataset))-self.
181             outlier_score
182         self.calculations_done=True

```



## 6.5. HICS

HICS es otra aproximación distinta al estudio por subespacios como ha sido el algoritmo OUTRES. OUTRES intenta encontrar un subespacio interesante en el vecindario de una instancia, es decir, para cada instancia se busca el subespacio interesante para dicha instancia y no tiene por qué ser interesante para ninguna más. Esta aproximación es la opuesta pues la intención es buscar subespacios que sean interesantes en general y hacer una valoración de los datos sobre dichos subespacios.

Este algoritmo además pretende encontrar anomalías basándose en el concepto de densidad como introdujimos en la segunda definición de anomalía. Veamos primero el algoritmo en pseudocódigo para poder ir desgranándolo y explicarlo.

### HICS

**Entrada:** D: dataset

$scores = [ ]$

$sub$  = subespacios de alto contraste

**para cada**  $S \in sub$  **hacer**

Ajustamos un modelo con el algoritmo LOF con la proyección sobre  $S$   
 $scores = scores + \text{puntaje LOF}$

**fin**

$scores = \frac{scores}{|sub|}$

**Salida:** scores: puntajes

### Algoritmo 3: HICS

Como podemos ver el objetivo de HICS es en primer lugar obtener una serie de subespacios que sean relevantes y que hemos llamado subespacios de alto contraste. Para cada uno de estos subespacios vamos a estudiar la proyección de los datos sobre estos subespacios y vamos a obtener una puntuación de las instancias con el modelo LOF. Finalmente hacemos la media de todos estos puntajes para obtener la puntuación final.

El modelo original está pensado para funcionar con LOF pero la teoría nos dice que podría funcionar con cualquier modelo basado en proximidad. Por tanto en la implementación desarrollada he incluido los modelos LOF, COF, CBLOF, LOCI, HBOS y SOD como alternativas entre las que elegir para la elección del modelo simple con el que obtener el puntaje.

Veamos ahora el pseudocódigo con el que obtenemos el contraste de un

subespacio.

#### CalcularConstraste

**Entrada:** subespacio: subespacio, M: número de iteraciones del subsampling,  $\alpha$ : valor para obtener el tamaño de la muestra,  $D$ : conjunto de datos

$$size = n \cdot \sqrt[|subespacio|]{\alpha}$$

$$dev = 0$$

**para cada**  $i \in [1, M]$  **hacer**

$comp\_atr = \text{aleatorio de subespacio}$

$sel\_obj = \text{muestra aleatoria de } D \text{ de tamaño } size$

$dev = dev + \text{CalcularDev}(comp\_atr, sel\_obj, subespacio, D)$

**fin**

$$dev = \frac{dev}{M}$$

**Salida:**  $dev$ : contraste

#### Algoritmo 4: CalcularConstraste

En resumen lo que vamos a ir haciendo es aplicar una técnica de subsampling en el algoritmo. Vamos a hacer  $M$  ejecuciones para obtener el contraste tomando diferentes muestras de un tamaño fijado de antemano. Con estas muestras vamos a calcular la desviación del atributo de comparación  $comp\_atr$  entre las instancias como vamos a ver ahora. Finalmente acumulamos toda esta desviación y obtenemos la media para ese subespacio. Con esto tenemos una medida de cuánto se desvían entre sí las instancias dentro de dicho subespacio.

#### CalcularDev

**Entrada:**  $comp\_atr$ : atributo con el que comparar,  $sel\_obj$ : muestra seleccionada aleatoriamente,  $subespacio$ : subespacio sobre el que calcular la desviación,  $D$ : conjunto de datos

$$max = 0$$

**para cada**  $d \in D$  **hacer**

$cum_1 = \sum_{o \in D} o[comp\_atr]$  si  $o[comp\_atr] < d[comp\_atr]$

$cum_2 = \sum_{o \in sel\_obj} o[comp\_atr]$  si  $o[comp\_atr] < d[comp\_atr]$

$$f_a = \frac{cum_1}{|D|}$$

$$f_b = \frac{cum_2}{|D|}$$

$$subs = |f_a - f_b|$$

**si**  $subs > max$  **entonces**

$max = subs$

**fin**

**fin**

**Salida:**  $max$ : máxima desviación

#### Algoritmo 5: CalcularDev

Con este test lo que estamos haciendo es ver cómo se diferencia el atributo escogido para la comparación con cada instancia del resto del conjunto de datos. La idea es similar a la que expusimos cuando comentamos brevemente los Isolated Forests de ir dividiendo los datos con un valor de corte.

Ahora ya tenemos las herramientas con las que podemos medir el contraste de un subespacio. Para ver cuáles son aquellos con mayor contraste los autores probaron dos formas quedándose finalmente con la que yo he añadido a la implementación. En primer lugar podemos pensar en algún tipo de cota que se vaya adaptando al número de subespacios o al contraste que estos vayan presentando. Esta idea finalmente fue descartada primero por no funcionar de forma satisfactoria y segundo por la dificultad de elección de la cota. La opción escogida finalmente es evaluar para cada dimensión todos los subespacios posibles, se obtiene el contraste de cada uno de ellos y se toma un número fijo de los primeros. De esta forma obtendremos por ejemplo en cada dimensión 500 candidatos. Una vez que hayamos evaluado todas las dimensiones volvemos a ordenar los subespacios por contraste (ya sin tener en cuenta la dimensionalidad) y nos quedamos con los 1000 primeros. Con esta metodología vamos a tener la certeza de que vamos a quedarnos con los 1000 subespacios con mayor contraste de entre todos los posibles.

Veamos la implementación del algoritmo.

```
1 def computeContrast(self, subspace):
2     '''
3     @brief Function that computes the contrast for a given
4         subspace
5     @param subspace Numpy array with the indexes of the
6         features that define the subspace
7     @return It returns a float representing the contrast
8         of the subspace
9     '''
10    ''' We set the adaptative size of the test'''
11    size = int(len(self.dataset)*np.power(self.alpha, len(
12        subspace)))
13    ''' Number of instances in the dataset'''
14    N = len(self.dataset)
15    deviation = 0
16    ''' We repeat the process M times'''
17    for i in range(1, self.M+1):
18        ''' This is the comparison attribute for the test,
19            so it will stay untouched'''
20        comparison_attr=np.random.randint(low=0, high=len(
21            subspace))
22        ''' List of booleans that masks the instances of
23            the dataset selected'''
```

```

17         selected_objects = np.array([True]*N)
18         ''' Select random indexes'''
19         selected_objects[reduce(np.union1d,np.array([np.
20             random.choice(N,size=size,replace=False) for _
21             in range(len(subspace)-1)])]=False
22         ''' With the sample given by the mask
23             selected_objects we compute the deviation'''
24         deviation+=self.computeDeviation(subspace[
25             comparison_attr], selected_objects, subspace)
26         ''' Finally the contrast is the average of all
27             deviations'''
28         return deviation/self.M
29
30 def computeDeviation(self, comparison_attr,
31     selected_objects, subspace):
32     '''
33     @brief Function that computes the deviation of the
34             marginal distribution
35             given a fixed attribute, a sample and the condition
36             given as a subspace
37     @param comparison_attr This is the comparison
38             attribute
39     @param selected_objects Mask that sets a sample of the
40             dataset
41     @param subspace Subspace or condition to calculate the
42             deviation
43     @return It returns a float giving the deviation
44     '''
45     max = 0
46     ''' For each instance of the dataset'''
47     for d in self.dataset:
48         ''' This is the cumulative value for all elements
49             in the dataset'''
50         cumul1 = np.sum(self.dataset[:,comparison_attr][
51             self.dataset[:,comparison_attr]<d[
52                 comparison_attr]])
53         ''' This is the cumulative value for the
54             selected_objects aka the sample'''
55         sel = self.dataset[:,comparison_attr][
56             selected_objects]
57         cumul2 = np.sum(sel[sel<d[comparison_attr]])
58         ''' Finally we compute the average in both cases
59             '''
60         fa = cumul1/len(self.dataset)
61         fb = cumul2/len(self.dataset)
62         ''' The difference in absolute value is the
63             deviation'''
64         subs = np.absolute(fa-fb)
65         ''' We return the biggest of the deviations

```

```

    obtained'''
48     if subs>max:
49         max = subs
50     return max
51
52 def hicsFramework(self):
53     '''
54     @brief This function computes the high contrast
55           subspaces on which to score the outlier
56     @return It returns a numpy array containing the high
57           contrast subspaces
58     '''
59     ''' Ordered subspaces by dimension type: list of numpy
60           arrays of numpy arrays
61     this means that in each positions there would be the
62           subspaces of the corresponding
63     dimension in the form of a list of subspaces which
64           are numpy arrays'''
65     all_subspaces = []
66     ''' Record of the contrast for each subspace in each
67           dimension, same shape as all_subspaces'''
68     all_contrasts = []
69     ''' For all dimensions starting from dimension 2 (
70           correlation has no sense on dimension 1)'''
71     for dimension in range(2,len(self.dataset[0])):
72         if self.verbose:
73             print("Computing subspaces in dimension " +
74                   str(dimension) + "/" + str(len(self.
75                         dataset[0])))
76         candidates = []
77         contrasts = []
78         ''' This list will keep the indexes of the
79               redundant subspaces, those are d-dimensional
80               subspaces with d+1-dimensional
81               subspaces containing them with higher contrast'''
82         redundant = []
83         ''' For dimension 2 we just obtain all possible
84               indexes and make all combinations'''
85         if dimension==2:
86             ''' Calculate the candidates as all possible
87                   combinations'''
88             indexes = list(range(len(self.dataset[0])))
89             candidates = np.array([np.array(list(comb))
90                                     for comb in list(combinations(indexes,
91                                         dimension))])
92             ''' Compute the contrasts'''
93             cont = 0
94             p = Pool(self.numThreads)
95             while cont+self.numThreads<len(candidates):

```

```

81         contrasts = contrasts + p.map(self.
            computeContrast, candidates[cont:cont+
                self.numThreads])
82         cont+=self.numThreads
83         print("Computed " + str(cont) + "/" + str(
            len(candidates)))
84         p = Pool(len(candidates)-cont)
85         contrasts = contrasts + p.map(self.
            computeContrast, candidates[cont:])
86         print("Computed " + str(len(candidates)) + "/"
            + str(len(candidates)))
87     else:
88         ''' We need to calculate now the indexes
            starting from a previous subspace
89         We record the parent of each subspace to
            check for redundancy'''
90         parents = []
91         ''' For all subspaces with one dimension less
            '''
92         for i in range(len(all_subspaces[-1])):
93             ''' We only consider new indexes, those
            are the ones not uses in the father
            subspace'''
94             indexes = list(set(list(range(len(self.
                dataset[0])))).difference(set(
                all_subspaces[-1][i])))
95             ''' For each new index'''
96             for ind in indexes:
97                 ''' We calculate the new candidate as the
            same subspace appending the index'''
98                 new_can = np.append(all_subspaces[-1][i],
                    ind)
99                 ''' Now we check that the candidate wasn't
            in the list before'''
100                new = True
101                for previous in candidates:
102                    if len(np.intersect1d(previous, new_can
                        ))==len(new_can):
103                        new = False
104                if new:
105                    candidates.append(new_can)
106                    parents.append(i)
107                ''' Compute the contrasts'''
108                cont = 0
109                p = Pool(self.numThreads)
110                while cont+self.numThreads<len(candidates):
111                    contrasts = contrasts + p.map(self.
                        computeContrast, candidates[cont:cont+
                            self.numThreads])

```

```

112         cont+=self.numThreads
113         print("Computed " + str(cont) + "/" + str(
            len(candidates)))
114     p = Pool(len(candidates)-cont)
115     contrasts = contrasts + p.map(self.
        computeContrast, candidates[cont:])
116     print("Computed " + str(len(candidates)) + "/" +
        + str(len(candidates)))
117
118     ''' Check for redundancy'''
119     for i in range(len(parents)):
120         if contrasts[i]>all_contrasts[-1][parents[
            i]]:
121             redundant.append(parents[i])
122
123     candidates = np.array(candidates)
124     contrasts = np.array(contrasts)
125     ''' If there are redundant subspaces'''
126     if redundant!=[]:
127         if self.verbose:
128             print("Now deleting redundant subspaces in
                dimension " + str(dimension) + ", " +
                str(len(redundant)) + " subspaces
                removed.")
129
130     ''' Delete those ones'''
131     non_redundant_sub = np.delete(all_subspaces[-1],
        redundant)
132
133     ''' Update the subspaces'''
134     all_subspaces[-1]=non_redundant_sub
135     ''' Sort from higher contrast to lower and only
        get numCandidates number of subspaces if
        available'''
136     if len(candidates)>self.numCandidates:
137         all_subspaces.append(candidates[contrasts.
            argsort()[-self.numCandidates:][::-1]])
138         all_contrasts.append(contrasts[contrasts.
            argsort()[-self.numCandidates:][::-1]])
139     else:
140         all_subspaces.append(candidates)
141         all_contrasts.append(contrasts)
142
143     ''' We flatten the numpy array to obtain only a list
        of subspaces and contrasts'''
144     subspaces = np.array(all_subspaces).flatten()
145     contrasts = np.array(all_contrasts).flatten()
146
147     ''' We only give the maxOutputSpaces with higher
        contrast if available'''
148     if len(subspaces)>self.maxOutputSpaces:
149         return subspaces[contrasts.argsort()[-self.
            maxOutputSpaces:][::-1]]

```

```

146     return subspaces
147
148 def runMethod(self):
149     '''
150     @brief This function is the actual implementation of
151           HICS
152     '''
153     if self.verbose:
154         print("Calculating the subspaces\n")
155         ''' First we obtain the high contrast subspaces'''
156         subspaces = self.hicsFramework()
157
158     if self.verbose:
159         print("Now calculating the scoring\n")
160         ''' We initialize the scores for each instance as 0'''
161         scores = np.zeros(len(self.dataset))
162         ''' For each subspace'''
163         for sub in subspaces:
164             ''' We place the corresponding scorer according to
165               parameter'''
166             scorer = None
167             if self.outlier_rank=="lof":
168                 scorer = LOF()
169             elif self.outlier_rank=="cof":
170                 scorer = COF()
171             elif self.outlier_rank=="cblof":
172                 scorer = CBLOF()
173             elif self.outlier_rank=="loci":
174                 scorer = LOCI()
175             elif self.outlier_rank=="hbos":
176                 scorer = HBOS()
177             elif self.outlier_rank=="sod":
178                 scorer = SOD()
179             ''' Fits the scorer with the dataset'''
180             scorer.fit(self.dataset[:,sub])
181             ''' Adds the scores obtained to the global ones'''
182             scores = scores+scorer.decision_scores_
183         ''' Compute the average'''
184         self.outlier_score = scores/len(subspaces)
185         ''' Marks the calculations as done'''
186         self.calculations_done=True

```

## 6.6. LODA

LODA es un algoritmo que entra en la categoría de los algoritmos que involucran histogramas. Aún no hemos visto ningún algoritmo de este ti-



po, por lo que no hemos discutido el funcionamiento de estos algoritmos. Cuando hacemos un histograma de los datos estudiamos la distribución de probabilidad de los datos y por tanto podemos ver si éstos están en las colas en algún atributo o proyección o si están en el centro de la distribución. Con esto podemos saber si el dato es o no anómalo. En concreto LODA emplea una serie de proyecciones uno-dimensionales sobre las que se estudia la distribución.

En primer lugar vamos a ver cómo se obtienen los vectores que nos dan las proyecciones uno-dimensionales.

### ProyeccionesAleatorias

**Entrada:**  $d$ : dimension,  $D$ : dataset,  $k$ : número de histogramas y proyecciones

$no\_neg = \lceil \sqrt{d} \rceil$

$proyecciones = []$

**para** cada  $i \in [1, k]$  **hacer**

$ind = no\_neg$  índices aleatorios en  $[0, d]$

$proy =$  vector con ceros en todas las posiciones menos en  $ind$ ,  
    donde hay valores sacados de una normal  $\mathcal{N}(0, 1)$

$proyecciones = [proyecciones, proy]$

**fin**

**Salida:**  $proyecciones$ : proyecciones

**Algoritmo 6:** ProyeccionesAleatorias

En LODA tenemos un parámetro  $k$  que nos indica el número de proyecciones e histogramas que vamos a desarrollar. Esto nos va a dar más o menos muestras como haríamos con una técnica de subsampling tradicional.

Una vez que tenemos estos vectores de proyección vamos a ver cómo generamos los histogramas a partir de ellos.

### ObtenerHistogramas

**Entrada:**  $D$ : dataset,  $\{w_i\}_{i=1}^k$ : vectores de proyecciones,  $k$ : numero de histogramas y vectores de proyección

Inicializamos los histogramas  $\{h_i\}_{i=1}^k$

**para**  $j = 1 \rightarrow |D|$  **hacer**

**para**  $i = 1 \rightarrow k$  **hacer**

$z_i = x_j^T w_i$

        Actualiza el histograma  $h_i$  con  $z_i$

**fin**

**fin**

**Salida:**  $\{h_i\}_{i=1}^k$ : histogramas

**Algoritmo 7:** ObtenerHistogramas

Con esto ya tenemos tanto las proyecciones como los histogramas, por lo que sólo queda ver cómo obtenemos las puntuaciones de anomalías de los datos.

### LODA

**Entrada:**  $x$ : instancia,  $\{h_i\}_{i=1}^k$ : histogramas,  $\{w_i\}_{i=1}^k$ : vectores de proyección

**para**  $i = 1 \rightarrow k$  **hacer**

$z_i = x^T w_i$   
    Obtenemos  $p_i = p_i(z_i)$  del histograma  $h_i$

**fin**

$f = \frac{-1}{k} \sum_{i=1}^k \log(p_i(z_i))$

**Salida:**  $f$ : puntaje de anomalía de  $x$

### Algoritmo 8: LODA

Finalmente ya tenemos el algoritmo LODA completo. Cuando estamos evaluando una instancia obtenemos la probabilidad de que su proyección uno-dimensional ocurra. Con esta probabilidad si hacemos el logaritmo cuanto más cerca esté de 0 más cerca estará el valor de  $-\infty$  y por tanto mayor va a ser nuestro puntaje anómalo de dicha instancia.

Ahora que ya tenemos el algoritmo completo vamos a ver la implementación:

```

1 def getRandomProjections(self, dimension):
2     '''
3     @brief Function that computes and returns the random
4         projections
5     @param self
6     @param dimension Dimensionality of the dataset (int)
7     @return It returns a list with numpy arrays as
8         projections
9     '''
10    ''' Number of non-negative elements in the projection
11    '''
12    non_neg = int(np.ceil(np.sqrt(dimension)))
13    projections = []
14    ''' We are going to compute k projections'''
15    for i in range(self.k):
16        ''' Select non_neg random indexes to make the
17            projection'''
18        ind = np.random.choice(dimension, replace=False,
19                               size=non_neg)
20        ''' Initialize it to zeroes'''
21        proj = np.zeros(dimension)
22        ''' The non-negative elements are drawn from a
23            normal distribution'''

```

```

18         proj[ind]=np.random.normal(size=non_neg)
19         projections.append(proj)
20     return projections
21
22 def getBin(self, hist_limits, value):
23     '''
24     @brief Function that given a value, it returns the bin
25           it belongs to for the histogram
26     @param self
27     @param hist_limits Limits for each bin of the
28           histogram
29     @param value Value to check for the bin
30     @return It returns the index corresponding to the bin
31     '''
32     bin=-1
33     for i in range(len(hist_limits)):
34         if value<hist_limits[i]:
35             bin=i
36             break
37     return bin-1
38
39 def runMethod(self):
40     '''
41     @brief This is the implementation of the LODA
42           algorithm
43     '''
44     ''' We compute first all projections'''
45     random_projections = self.getRandomProjections(len(
46         self.dataset[0]))
47     ''' Initialize the histograms and the projected data
48     '''
49     histograms = [[]]*self.k
50     Z = [[]]*self.k
51     ''' For each instance of the dataset'''
52     for j in range(len(self.dataset)):
53         ''' For each projection'''
54         for i in range(self.k):
55             ''' Compute the 1D projection'''
56             Z[i].append(np.dot(self.dataset[j].T,
57                 random_projections[i]))
58     ''' Compute the k histograms with the data'''
59     for i in range(self.k):
60         histograms[i]=np.histogram(Z[i], bins = self.
61             n_bins)
62
63     ''' Initialize the scores to zero'''
64     self.outlier_score = np.array([0]*len(self.dataset)).
65         astype(float)
66     ''' For each instance'''

```

```

59     for i in range(len(self.dataset)):
60         prob = []
61         ''' For each histogram'''
62         for j in range(self.k):
63             ''' Compute the projection'''
64             z = np.dot(self.dataset[i].T,
65                         random_projections[j])
66             ''' Check the bin for the projection'''
67             bin = self.getBin(histograms[j][1], z)
68             ''' Obtain the probability linked to z in the
69                 histogram'''
70             prob.append(histograms[j][0][bin]/np.sum(
71                         histograms[j][0]))
72         prob = np.array(prob)
73         ''' Compute the score with the probabilities'''
74         if 0. in prob:
75             self.outlier_score[i] = float("inf")
76         else:
77             self.outlier_score[i] = -np.sum(np.log(prob))/
78                 self.k
79     self.calculations_done=True

```

## 6.7. Implementación

Todos los algoritmos están implementados utilizando una clase base llamada EnsembleTemplate:

```

1  class EnsembleTemplate:
2      '''
3      Template class for the ensemble anomaly detectors.
4      '''
5
6  def __init__(self, contamination=0.1):
7      '''
8      Init template
9      '''
10     pass
11
12 def fit(self, dataset):
13     '''
14     Function to set the dataset and execute the algorithm
15     '''
16     self.dataset = dataset
17     self.outlier_score = [0]*len(self.dataset)
18     self.outliers = []
19     self.runMethod()

```

```
20     return self
21
22 def runMethod(self):
23     '''
24     Function to run the method implemented
25     '''
26     pass
27
28 def getRawScores(self):
29     '''
30     Function that gets the raw scores
31     '''
32     return self.outlier_score
33
34 def getOutliersBN(self, noutliers):
35     '''
36     Function that gets the noutliers instances of the most
37         outlying data
38     '''
39     return self.outliers
40
41 def getOutliers(self):
42     pass
```

El esqueleto de todas las clases que implementan los algoritmos de los que hemos hablado es este. En primer lugar todas las clases tienen un constructor en el que se pasan los parámetros de los modelos en caso de haberlos. En segundo lugar tenemos una función fit. El cometido de esta función es inicializar las puntuaciones, pasar el dataset al objeto de la clase para que se guarde y por último ejecutar el método que implementa.

La función principal es la función runMethod que es la que implementa la ejecución del algoritmo en sí. Esta función no está pensada para ser llamada externamente si no desde fit.

Por último tenemos tres funciones más. La primera de ellas nos da el vector que contiene los puntajes de las anomalías. La segunda función nos da los “noutliers” elementos con mayor puntaje y la tercera nos devuelve las instancias anómalas basándose en un parámetro que llamamos contaminación.

El parámetro de contaminación no es más que una estimación del porcentaje de anomalías que pensamos que va a tener el conjunto de datos. Por tanto si el parámetro de contaminación fuera por ejemplo 0.1 entonces esta función devolvería el primer 10 % con mayor valor de puntaje de anomalía.

Toda la implementación del trabajo se encuentra alojada en GitHub en

este repositorio.

## Capítulo 7

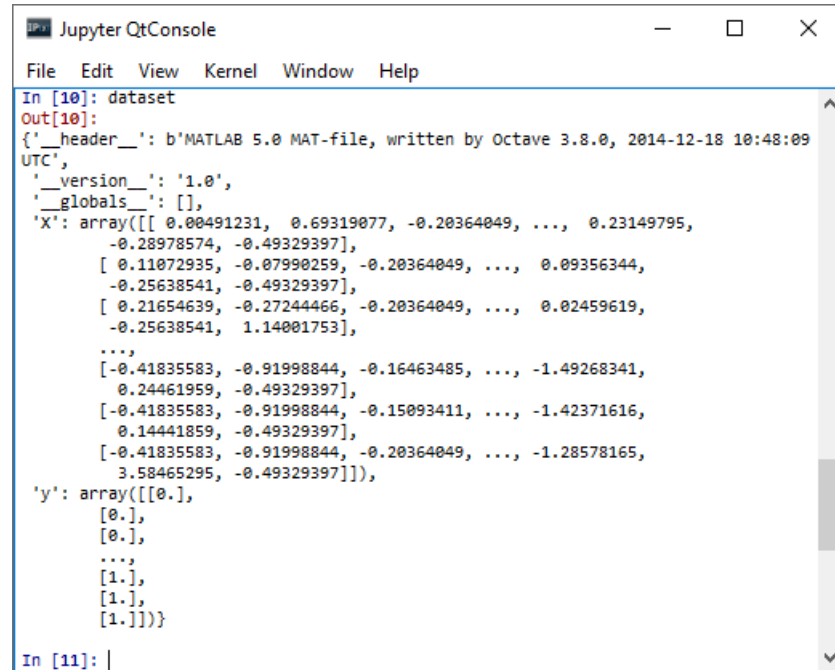
# Experimentación y Resultados

### 7.1. Conjuntos de datos

Para comenzar la experimentación vamos a hacer un repaso de los conjuntos de datos y la técnica seguida para realizar la misma. En primer lugar cabe decir que al ser un problema no supervisado en origen no tendríamos forma de saber nuestro acierto en el problema. En este tipo de casos hay dos aproximaciones: estimar el acierto o utilizar conjuntos que sí están clasificados y obtener de esta forma el acierto. La segunda de las alternativas es la que vamos a seguir en este estudio y es la que se suele denominar como problema semi-supervisado.

Para tomar este camino necesitamos conjuntos en los que tengamos disponible la clasificación de datos anómalos y no anómalos. Estos conjuntos de datos han sido tomados de la web Outlier Detection Datasets [5], librería mantenida por la universidad Stony Brooks.

Estos conjuntos de datos están en formato Matlab, formato que puede ser fácilmente leído por la librería SciPy. Estos conjuntos de datos vienen con información de cabecera, versión e incluso algunos con una breve descripción o resumen si dispusieran de ella. Lo importante es que los datos vienen divididos en dos, primero un vector que contiene una lista con los vectores que componen los datos y en segundo lugar un vector con las etiquetas donde 0 significa que el dato no es anómalo y 1 que sí lo es.



```

Jupyter QtConsole
File Edit View Kernel Window Help

In [10]: dataset
Out[10]:
{'__header__': b'MATLAB 5.0 MAT-file, written by Octave 3.8.0, 2014-12-18 10:48:09
UTC',
 '__version__': '1.0',
 '__globals__': [],
 'X': array([[ 0.00491231,  0.69319077, -0.20364049, ...,  0.23149795,
             -0.28978574, -0.49329397],
            [ 0.11072935, -0.07990259, -0.20364049, ...,  0.09356344,
             -0.25638541, -0.49329397],
            [ 0.21654639, -0.27244466, -0.20364049, ...,  0.02459619,
             -0.25638541,  1.14001753],
            ...,
            [-0.41835583, -0.91998844, -0.16463485, ..., -1.49268341,
              0.24461959, -0.49329397],
            [-0.41835583, -0.91998844, -0.15093411, ..., -1.42371616,
              0.14441859, -0.49329397],
            [-0.41835583, -0.91998844, -0.20364049, ..., -1.28578165,
              3.58465295, -0.49329397]]),
 'y': array([[0.],
            [0.],
            [0.],
            ...,
            [1.],
            [1.],
            [1.]])
In [11]:

```

Figura 7.1: Contenido de los conjuntos de datos

Como podemos ver “X” contiene el conjunto de datos y el campo “y” contiene las etiquetas para los mismos.

En algunos de estos conjuntos de datos podemos encontrar lo que conocemos como valores perdidos o en inglés “missing values”. Estos valores vienen reflejados con “NAN” en los conjuntos. Estos valores no sólo no nos son de interés si no que además nuestros modelos no están preparados para poder trabajar con ellos por lo que tenemos que decidir que transformación aplicamos para poder emplear los conjuntos de datos. La decisión tomada para estos valores ha sido la de eliminar las instancias que presenten valores perdidos. Esta decisión se basa en que, si estas instancias son anómalas no tenemos forma alguna de tratar con ellas porque no disponen de valores numéricos en sus campos y por tanto nuestros modelos no son aptos para resolver el conflicto. Esto no excluye el hecho de que estas instancias puedan ser anomalías reales. Por ejemplo pensemos en un sistema de frenos que sufre una rotura de alguno de sus sistemas. Si estos sistemas poseen sensores que recopilan datos es muy probable que estos sensores no tomen valores y por tanto dispongamos de valores perdidos precisamente porque la instancia es anómala. Esto se discutirá un poco más en profundidad cuando hablemos del trabajo futuro, de momento la decisión ha sido suprimir estas instancias.

Dentro de todos los conjuntos de datos que contiene la librería nosotros



vamos a utilizar los siguientes:

Nombre	Dimensionalidad	Número de instancias
annthyroid	6	7200
arrhythmia	274	452
breastw	9	683
cardio	21	1831
glass	9	214
ionosphere	33	351
letter	32	1600
lympho	18	148
mammography	6	11183
mnist	100	7603
musk	166	3062
optdigits	64	5216
pendigits	16	6870
pima	8	768
satellite	36	6435
satimage-2	36	5803
speech	400	3686
thyroid	6	3772
vertebral	6	240
vowels	12	1456
wbc	30	378
wine	13	129

Cuadro 7.1: Tabla con información de los conjuntos de datos

Como podemos ver hay algunos conjuntos con un tamaño razonablemente grande tanto en dimensionalidad como en número de instancias. Esto será discutido modelo por modelo pues los algoritmos basados en subespacios tienen una complejidad dependiente del factorial de la dimensionalidad, es decir, a partir de una cierta dimensionalidad el tiempo que consumen estos algoritmos es demasiado alto.

## 7.2. Experimentación

Sobre estos conjuntos de datos hemos ejecutado nuestros cinco modelos implementados: HICS, OUTRES, Mahalanobis Kernel, Trinity y LODA. Sobre estas ejecuciones se ha recopilado el porcentaje de acierto sobre ellos, el tiempo consumido en la ejecución y las propias puntuaciones dadas sobre

estos conjuntos de datos por los modelos.

Para poder hacer la comparativa con los datos de nuestros modelos he tomado modelos clásicos. Estos modelos se han cogido de la librería PyOD [6]. De esta librería se han tomado 10 modelos: Angle-Based Outlier Detection (ABOD), Connectivity-Based Outlier Factor (COF), Histogram-Based Outlier Score (HBOS), K Nearest Neighbors (KNN), Local Outlier Factor (LOF), Minimum Covariance Determinant (MCD), One-Class Support Vector Machines (OCSVM), Principal Component Analysis (PCA), Subspace Outlier Detection (SOD) y Stochastic Outlier Selection (SOS). Sobre estos modelos se ha recopilado exactamente la misma información que sobre los nuestros, es decir, el acierto, el tiempo consumido y las puntuaciones de las instancias.

En cuanto a OUTRES podemos estudiar cuándo un subespacio es importante para una instancia completa. Por tanto hemos lanzado otro experimento para intentar analizar los subespacios que son más relevantes para una determinada instancia.

### 7.3. Resultados

En primer lugar vamos a ver los resultados que obtenemos de todos los modelos sobre todos los conjuntos de datos. Se muestra un gráfico de barras por cada conjunto de datos con el desempeño de cada modelo. Cabe decir que tanto OUTRES como HICS son algoritmos como hemos comentado con una eficiencia muy mala en tiempo. Al ser su complejidad en tiempo dependiente del factorial de la dimensionalidad sólo hemos ejecutado el algoritmo en conjuntos de datos de baja dimensionalidad para poder completar dicha ejecución en un tiempo razonable, aunque como veremos hay algunos conjuntos de datos cuya ejecución ha llevado varias horas.

Veamos primero todos los gráficos con los resultados para poder analizarlos y particularizar posteriormente.

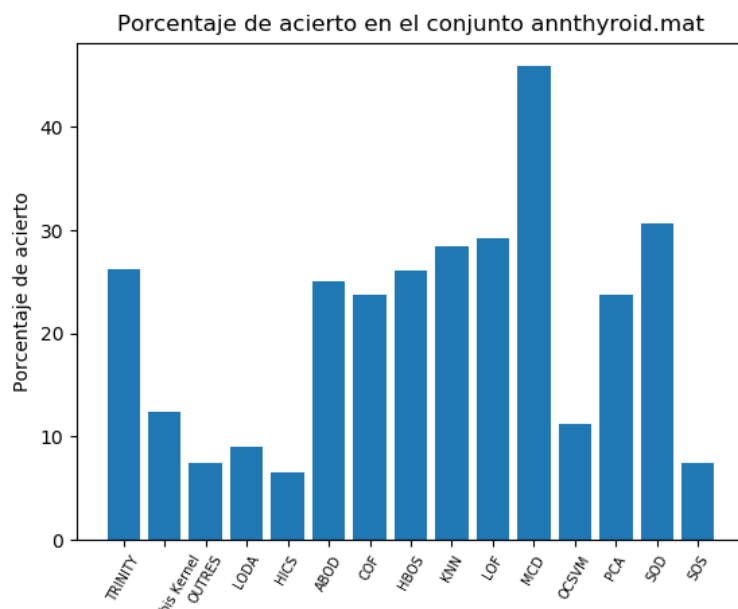


Figura 7.2: Porcentaje de acierto sobre el conjunto de datos annthyroid

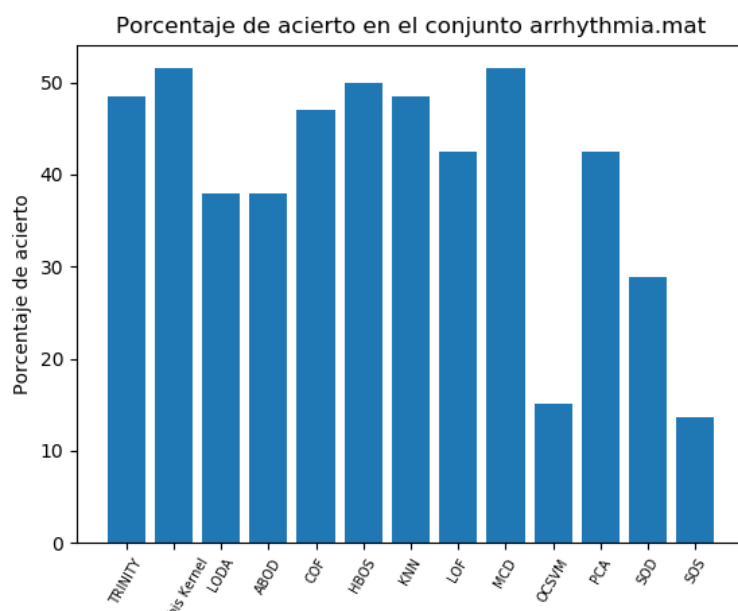


Figura 7.3: Porcentaje de acierto sobre el conjunto de datos arrhythmia

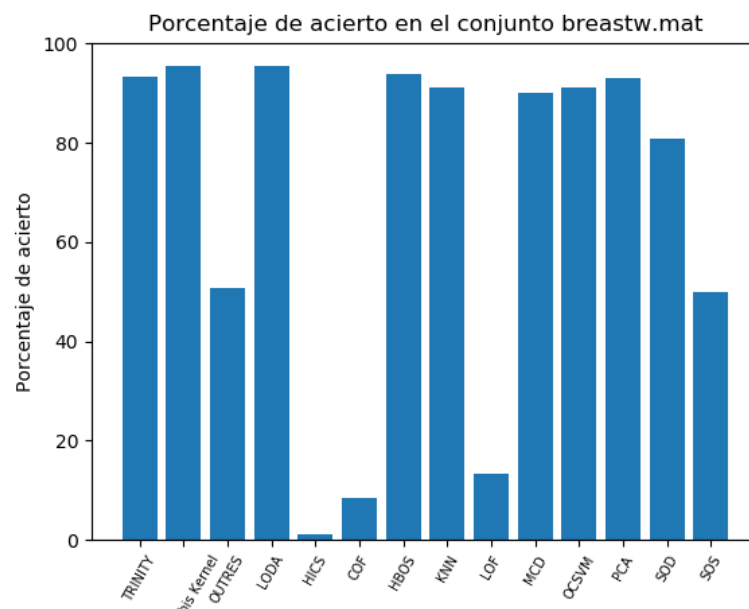


Figura 7.4: Porcentaje de acierto sobre el conjunto de datos breastw

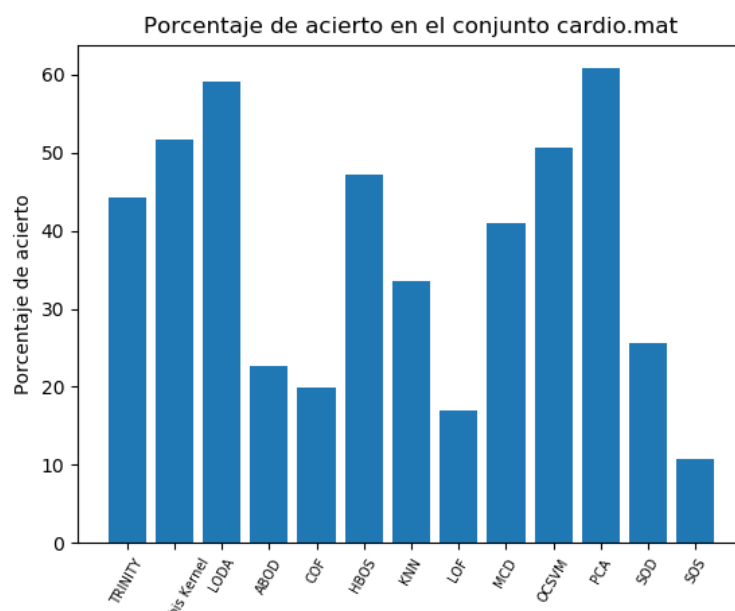


Figura 7.5: Porcentaje de acierto sobre el conjunto de datos cardio

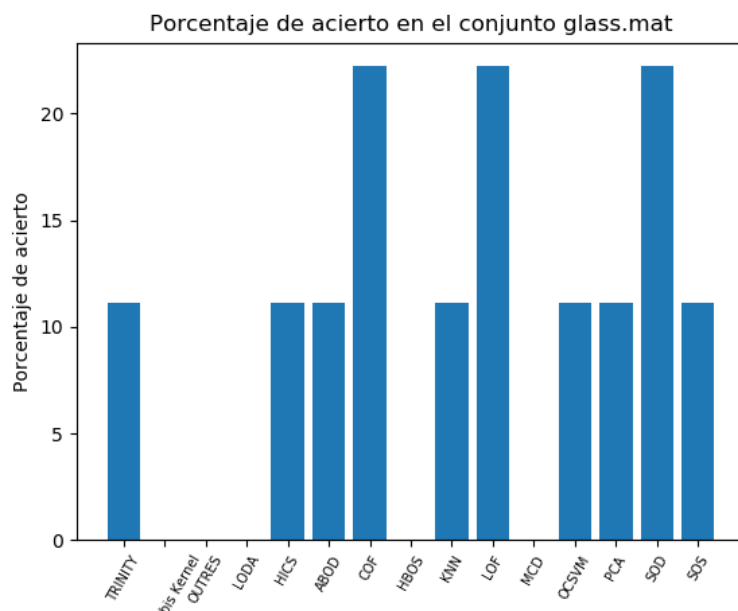


Figura 7.6: Porcentaje de acierto sobre el conjunto de datos glass

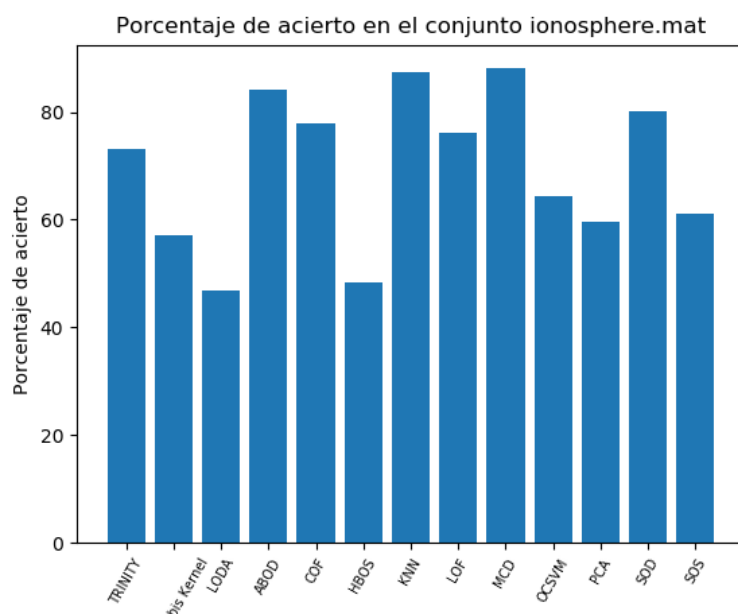


Figura 7.7: Porcentaje de acierto sobre el conjunto de datos ionosphere

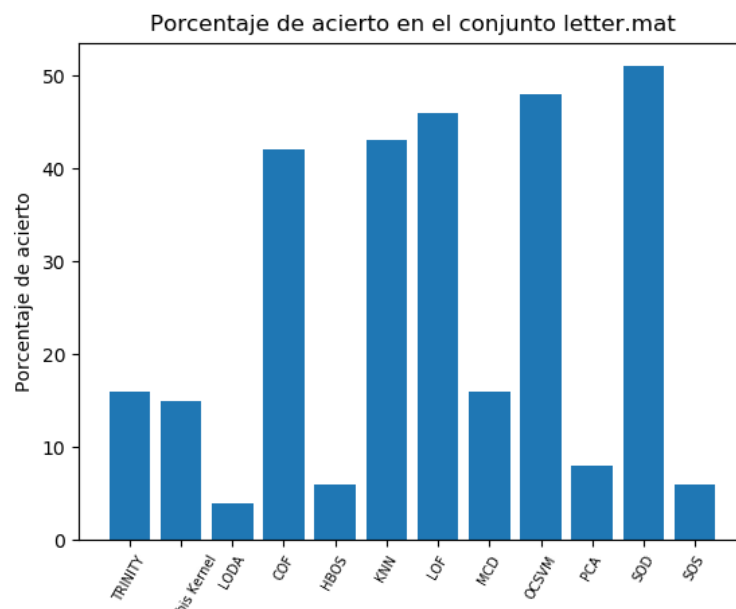


Figura 7.8: Porcentaje de acierto sobre el conjunto de datos letter

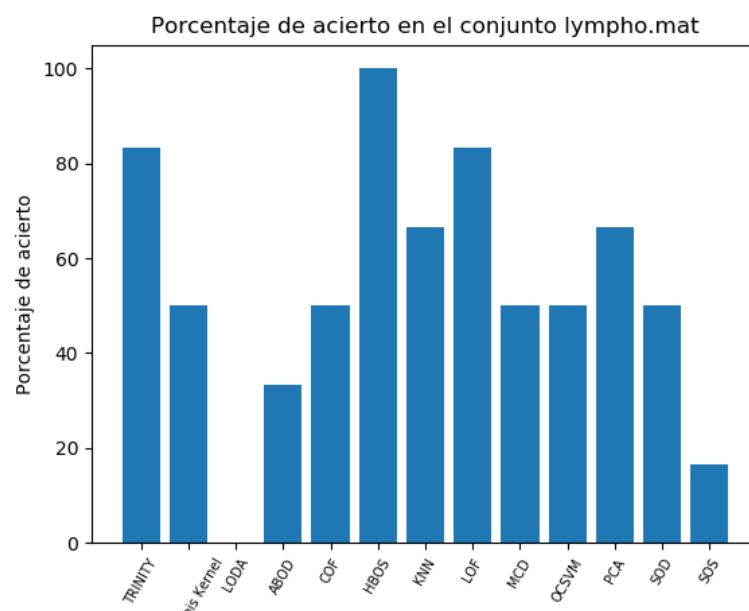


Figura 7.9: Porcentaje de acierto sobre el conjunto de datos lympho

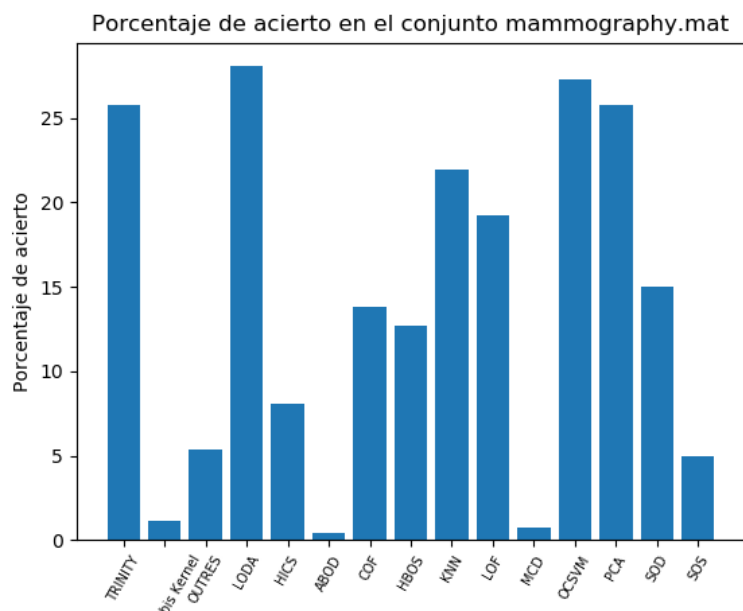


Figura 7.10: Porcentaje de acierto sobre el conjunto de datos mammography

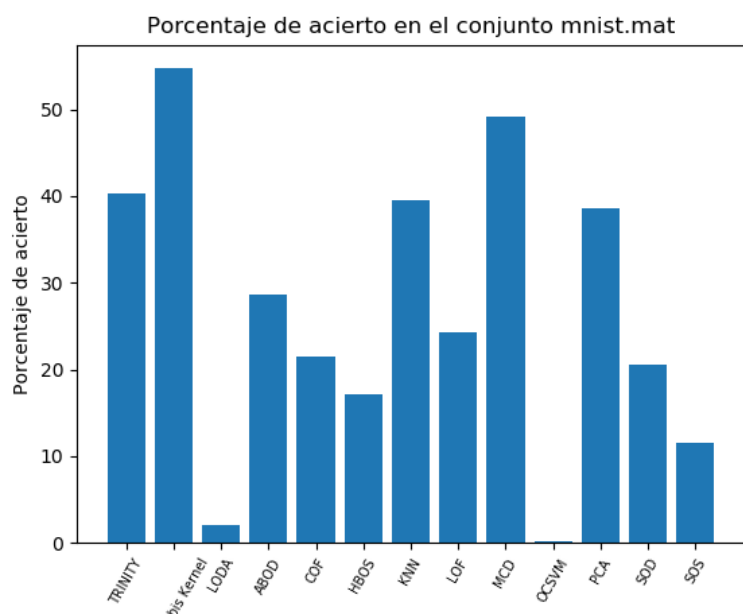


Figura 7.11: Porcentaje de acierto sobre el conjunto de datos mnist

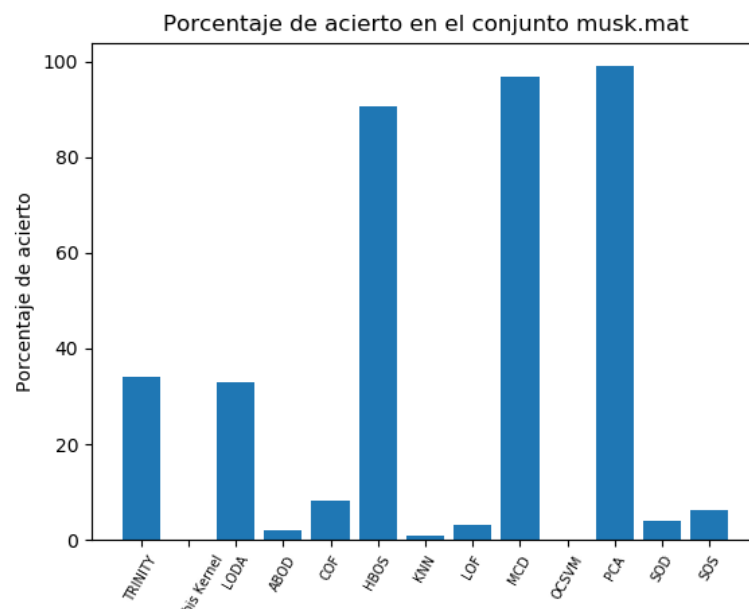


Figura 7.12: Porcentaje de acierto sobre el conjunto de datos musk

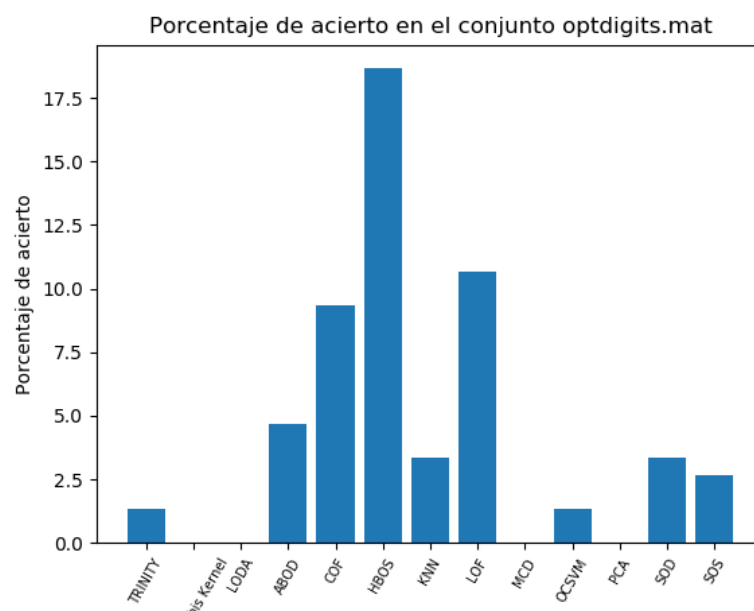


Figura 7.13: Porcentaje de acierto sobre el conjunto de datos optdigits



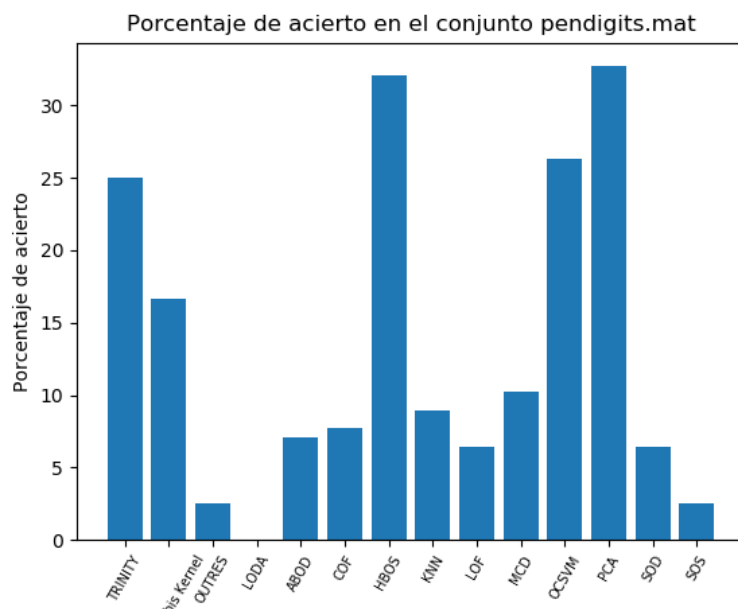


Figura 7.14: Porcentaje de acierto sobre el conjunto de datos pendigits

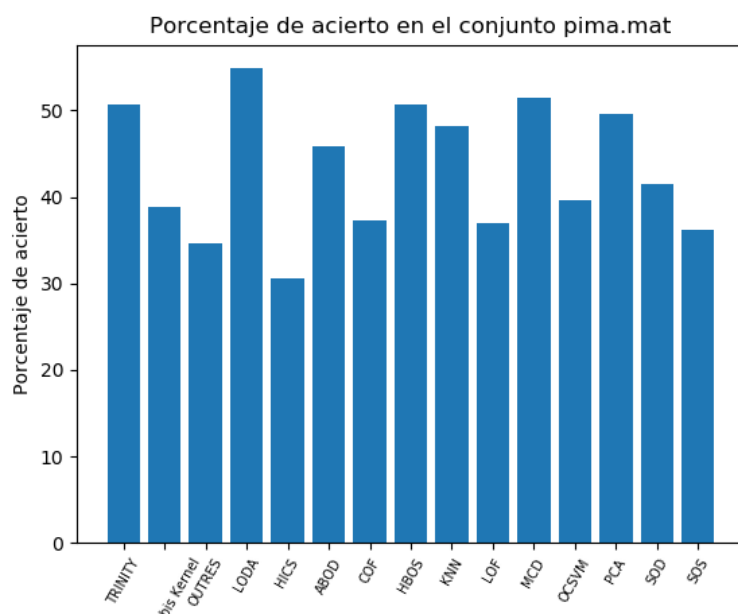


Figura 7.15: Porcentaje de acierto sobre el conjunto de datos pima

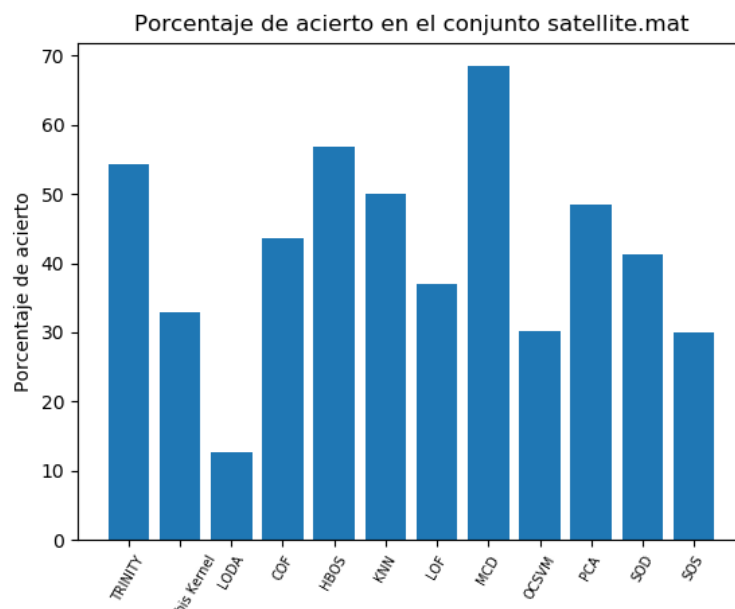


Figura 7.16: Porcentaje de acierto sobre el conjunto de datos satellite

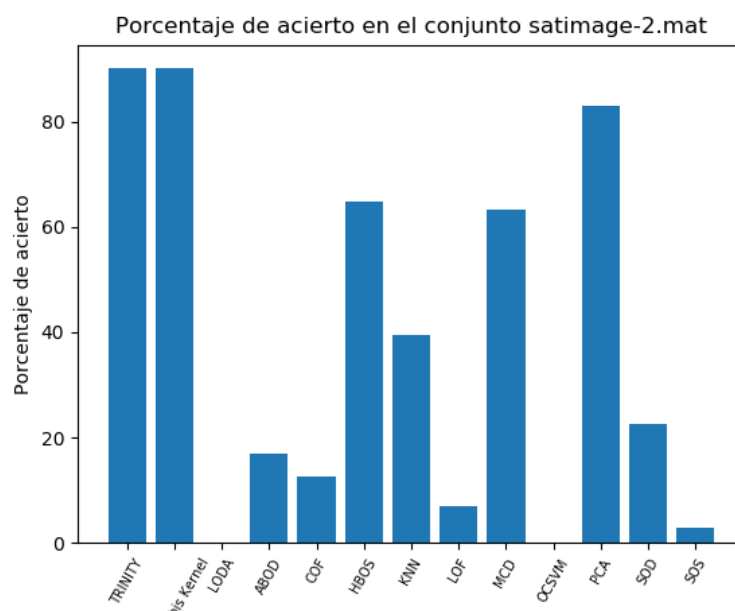


Figura 7.17: Porcentaje de acierto sobre el conjunto de datos satimage-2

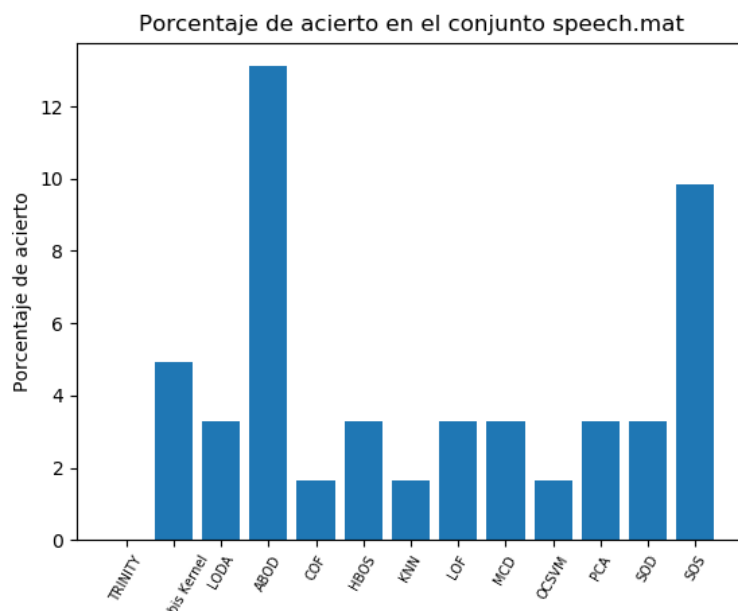


Figura 7.18: Porcentaje de acierto sobre el conjunto de datos speech

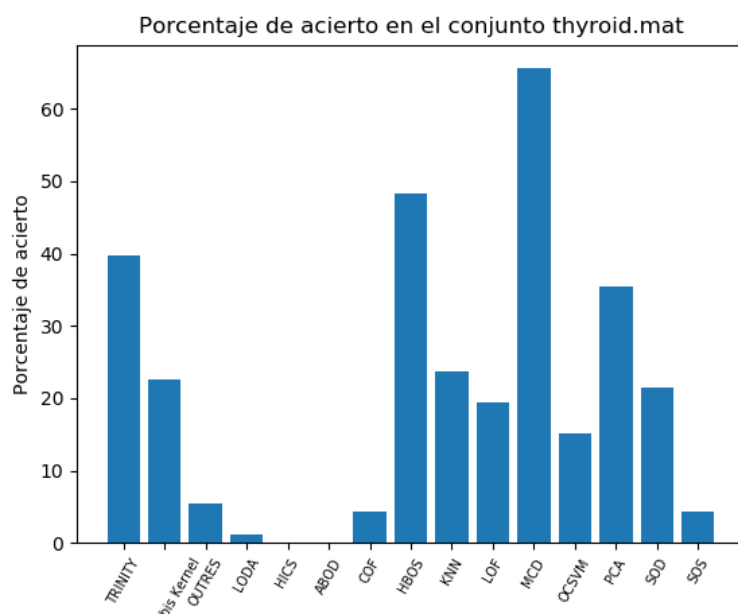


Figura 7.19: Porcentaje de acierto sobre el conjunto de datos thyroid

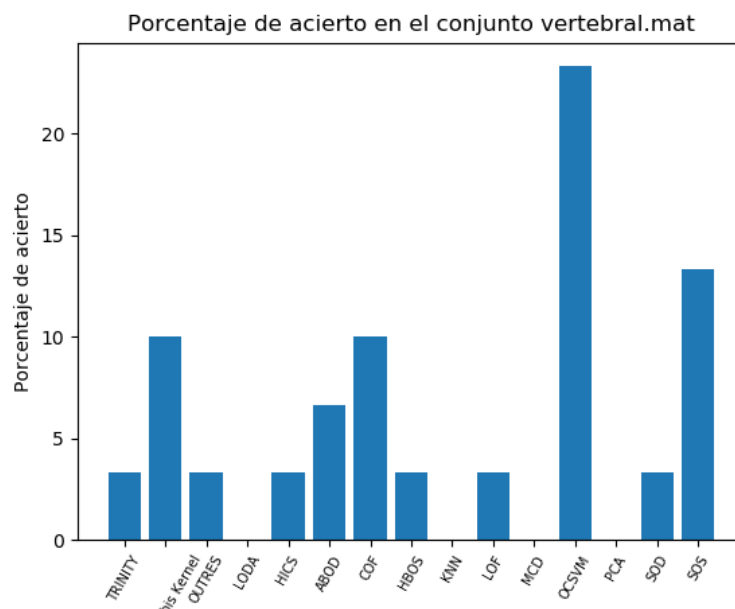


Figura 7.20: Porcentaje de acierto sobre el conjunto de datos vertebral

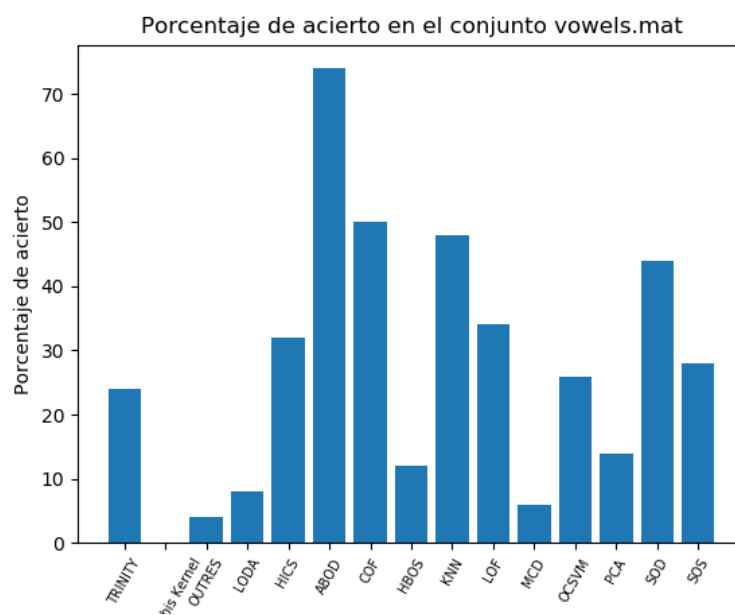


Figura 7.21: Porcentaje de acierto sobre el conjunto de datos vowels

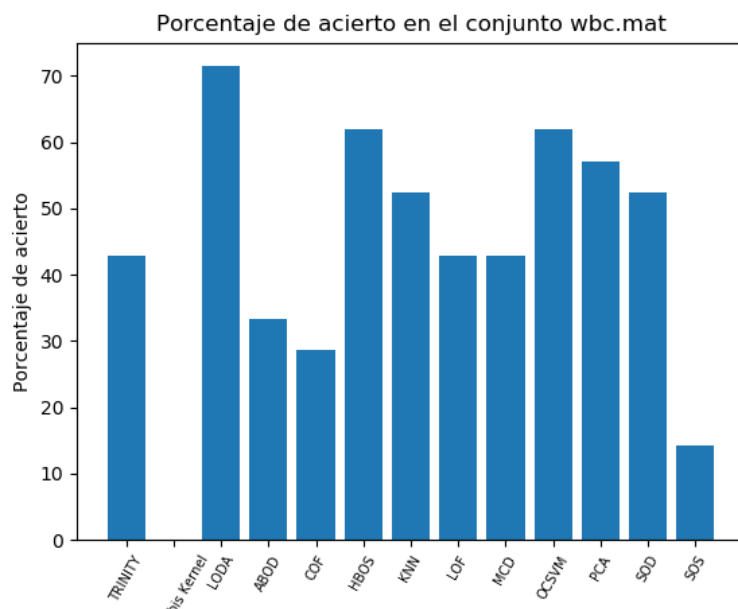


Figura 7.22: Porcentaje de acierto sobre el conjunto de datos wbc

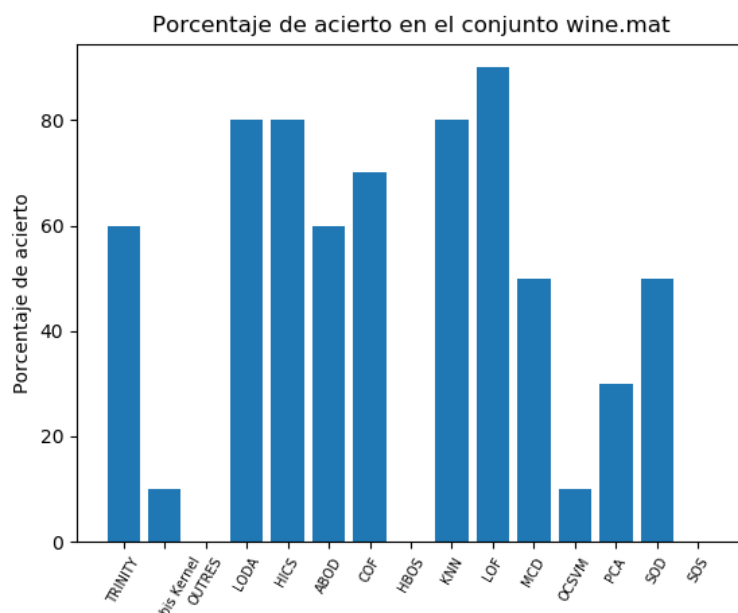


Figura 7.23: Porcentaje de acierto sobre el conjunto de datos wine

Como podemos observar los resultados que hemos obtenido han sido

variados. En primer lugar cabe justificar algunos valores en función de la dificultad de la tarea. Como hemos comentado en la parte teórica el concepto de anomalía es algo difícil de enmarcar por lo que también es algo complejo de detectar y por tanto en función de cada conjunto de datos puede que detectemos mejor o peor sus anomalías. Por eso por ejemplo tenemos conjuntos de datos como 7.6 en los que el mejor de los resultados apenas es poco más de un 20 % o 7.13 en el que ni siquiera llegamos a dicho 20 %. Esto no es más que el reflejo de la dificultad del problema. Lo interesante de este estudio es si conseguimos mejorar en algún caso con respecto a los modelos tradicionales y la respuesta es que alguno de los modelos que hemos implementado superan en ciertos conjuntos de datos a los clásicos.

Hemos conseguido con nuestros modelos conseguir la mejor puntuación en 8 de 22 conjuntos de datos. Este resultado puede no parecer significativo pero debemos considerar que tenemos el doble de modelos clásicos que de modelos de ensamblaje y que ni mucho menos todos los algoritmos clásicos están al mismo nivel. Además tenemos algoritmos clásicos de todos los tipos por lo que como podemos ver en algunos conjuntos de datos no funcionan todos bien pero alguno destaca y viceversa.

Como podemos ver en los 22 conjuntos de datos que hemos probado los dos modelos que peores resultados nos han arrojado de los 5 implementados son HICS y OUTRES, es decir, los dos modelos basados en subespacios que hemos implementado. Esto no quiere decir que los dos modelos sean de poca relevancia. La idea del estudio por subespacio es algo razonable y que puede arrojar buenos resultados, pero quizás no hemos utilizado para estos dos algoritmos ningún conjunto de datos conveniente. Además, los algoritmos de subespacios presentados son un poco rígidos en esta concepción sin querer salirse de la misma. Por ejemplo HICS obtiene sobre todo según hemos visto anomalías que no son triviales o claramente basadas en la definición de distancias. Es por esto que, aunque lo hayamos probado como un modelo sólo, pienso que es un algoritmo más idóneo para aplicarlo en conjunción con otro tipo de algoritmos. Por ejemplo sería interesante aplicar un algoritmo basado en subespacios después de aplicar Mahalanobis Kernel puesto que este modelo y Trinity son los más fiables de los 5 que hemos estudiado. Por ejemplo podemos ver que en 7.3, 7.4, 7.11 o 7.17 tanto Trinity como Mahalanobis Kernel funcionan muy bien.

Hay un dato bastante interesante en la comparativa entre Mahalanobis Kernel y Trinity. Como hemos visto en la explicación de los modelos Trinity tiene a Mahalanobis Kernel en el primer componente. Esto en los resultados se refleja en que Trinity en general obtiene mejores resultados que Mahalanobis Kernel. El segundo componente vimos que era KNN, comparando con este modelo vemos que los resultados que obtiene Trinity son al me-

nos iguales aunque en varios conjuntos son mejores los de Trinity que los de KNN. Por último el tercer componente de Trinity es IForest que no ha entrado dentro de esta comparativa por ser un modelo de ensamblaje también y por tanto carece de sentido contraponerlo con nuestros modelos. Esto nos está mostrando que efectivamente la combinación de modelos hace que los resultados sean más robustos obteniendo mejores resultados en general o en el peor caso manteniendo aproximadamente los resultados del modelo individual.

Por último podemos ver que LODA en general no tiene unos resultados muy espectaculares. Aún así consigue ponerse en cabeza en 7.4, 7.5, 7.10, 7.15 y 7.22. En el resto de conjuntos de datos no obtiene unos buenos resultados, lo que nos está diciendo que funciona muy bien en conjuntos de datos adecuados.

Vamos a ver ambos conjuntos de datos para comprobar la razón de este comportamiento.

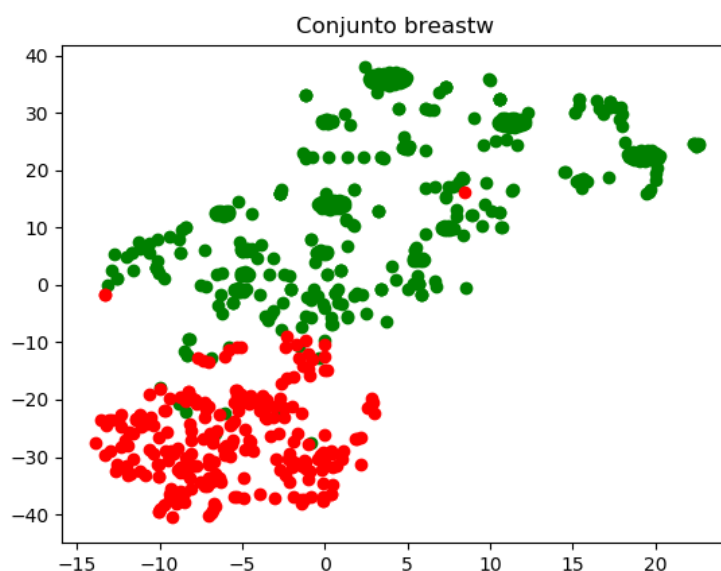


Figura 7.24: Proyección de breastw

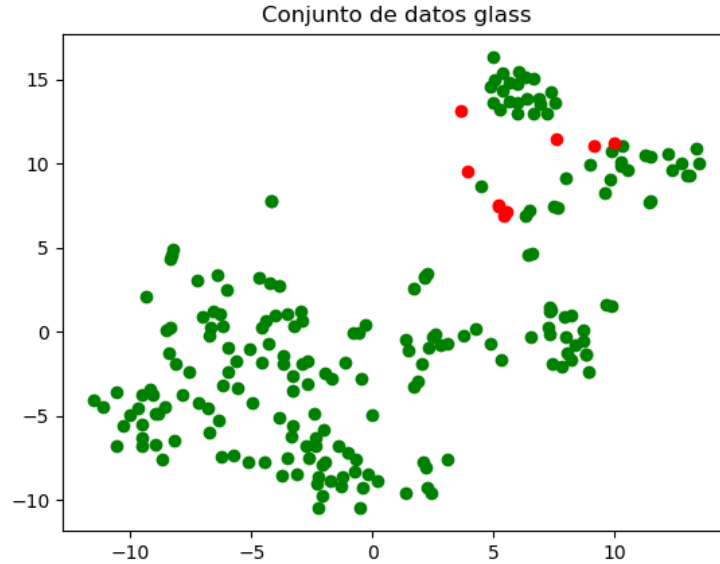


Figura 7.25: Proyección de glass

Como podemos ver en las figuras primeras LODA funciona muy bien sobre el conjunto de datos breastw y muy mal sobre el conjunto de datos glass. Para comprobar la forma de estos dos conjuntos de datos hemos dibujado la proyección en dos dimensiones utilizando la técnica TSNE. Como podemos observar en el conjunto de datos breastw tenemos las anomalías muy separadas del resto de los datos (siendo las anomalías los datos en rojo) mientras que en glass están dentro de los datos que consideraríamos normales. Esto nos está diciendo que cuanto mayor sea la aparición de anomalías del tipo basadas en distancias mejor es el desempeño de LODA.

Como podemos ver casi todos los modelos fallan en conjuntos de datos como optdigits. Veamos su proyección para intentar entenderlo.



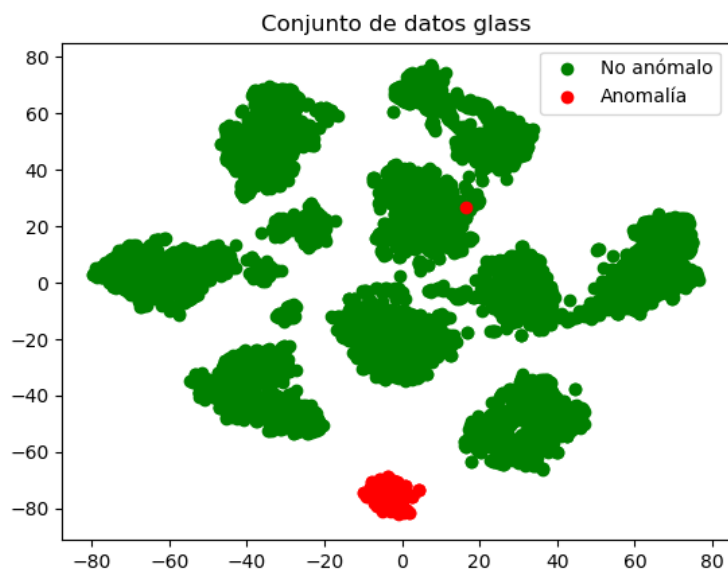


Figura 7.26: Proyección de optdigits

Podría parecer que el mal desempeño de los algoritmos sea completamente ilógico al ver que las anomalías están completamente diferenciadas de los datos. Como podemos ver no sólo están separadas del resto de los datos, si no que además están muy apiñadas entre sí. Esto es un inconveniente tremendo en la detección de anomalías. Como vimos en la primera de las definiciones las anomalías deben ser datos cuya distancia al centroide sea alta cosa que no pasa en este conjuntos de datos. Si nos fijamos en la segunda definición estamos intentando estudiar la densidad de datos para ver la anomalía pero este clúster tiene una alta densidad con lo que los datos no entrarían en la definición. Este conjunto de datos refleja perfectamente la complejidad del problema. Tenemos empíricamente determinadas las anomalías pero no entran claramente en las definiciones que podemos proveer de las mismas con lo que nos es difícil clasificarlas.

HICS tiene un desempeño razonablemente bueno en el conjunto de datos wine con lo que vamos a ver su proyección e intentar sacar conclusiones.

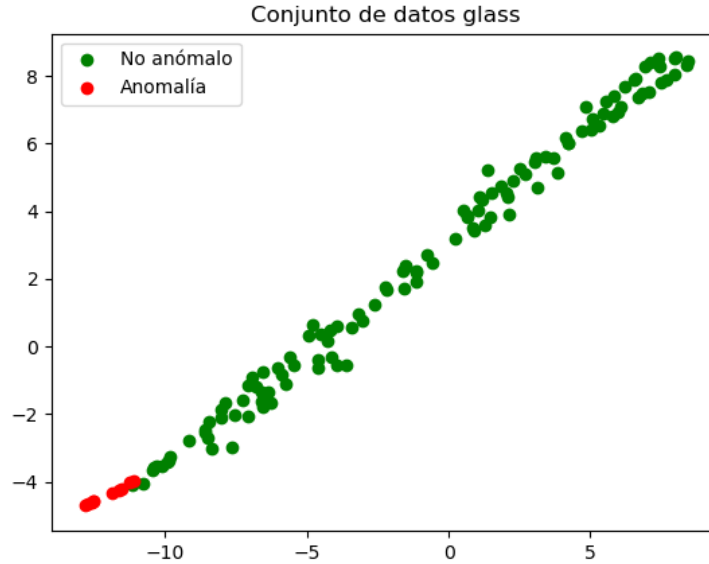


Figura 7.27: Proyección de wine

La proyección nos está mostrando que los datos están esparcidos a lo largo de un eje con lo que podemos explicar perfectamente también el buen desempeño de Mahalanobis Kernel. En concreto podemos deducir que HICS entiende que estos datos son anómalos o al menos más anómalos que el resto de los datos porque tienen una menor densidad en su entorno. Claramente es el punto en el que menos datos hay alrededor por lo que podemos ver razonable el comportamiento satisfactorio de HICS.

Para comprender el comportamiento de OUTRES es buena idea comprobar no sólo cuándo tenemos buenos resultados, si no que además por el propio algoritmo podemos ver el subespacio de los datos en el que cada dato es anómalo.

OUTRES no obtiene demasiados resultados satisfactorios pero donde mejor funciona es en breastw y en pima. Ya hemos visto cómo es la proyección de breastw, veamos la de pima.

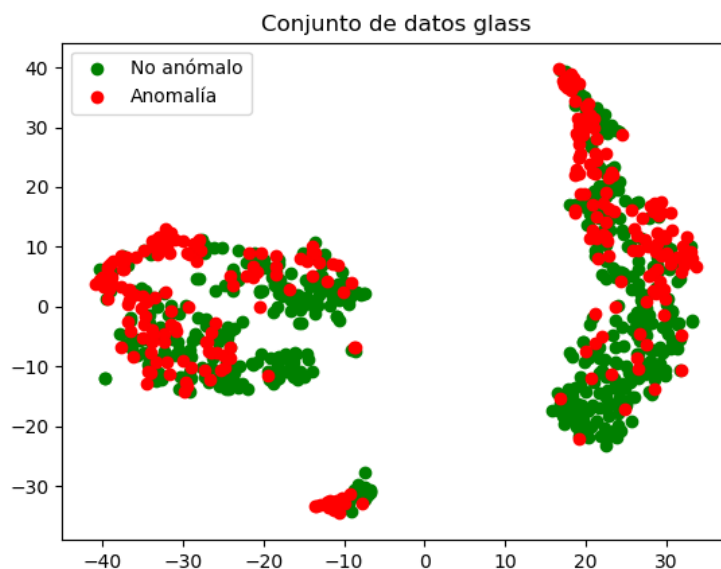


Figura 7.28: Proyección de pima

En un primer vistazo este conjunto de datos parece bastante complejo para obtener buenos resultados, por lo que merece la pena que veamos algunos de los subespacios en los que las instancias son anómalas para así poder entender un poco mejor el resultado. Estas imágenes son de todos los subespacios posibles obtenidos por OUTRES para cada instancia (en rojo) junto con el vecindario (en azul). Si tiene dimensión 2 se pintan directamente, si tienen una dimensionalidad mayor se hace primero la reducción de dimensionalidad mediante la técnica TSNE. Veamos algunos ejemplos:

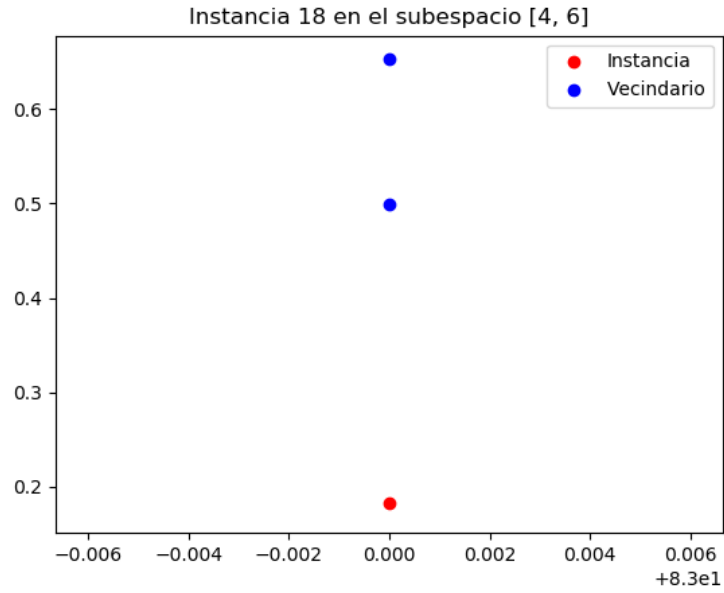


Figura 7.29: Instancia 18 sobre el subespacio [4, 6]

Como podemos ver en dos dimensiones se comprueba rápidamente que la instancia es anómala, pero estos subespacios no son los más interesantes. Cuanto mayor es el vecindario y mayor es la dimensionalidad más conclusiones podemos obtener. Veamos uno de estos ejemplos de mayor dimensionalidad.

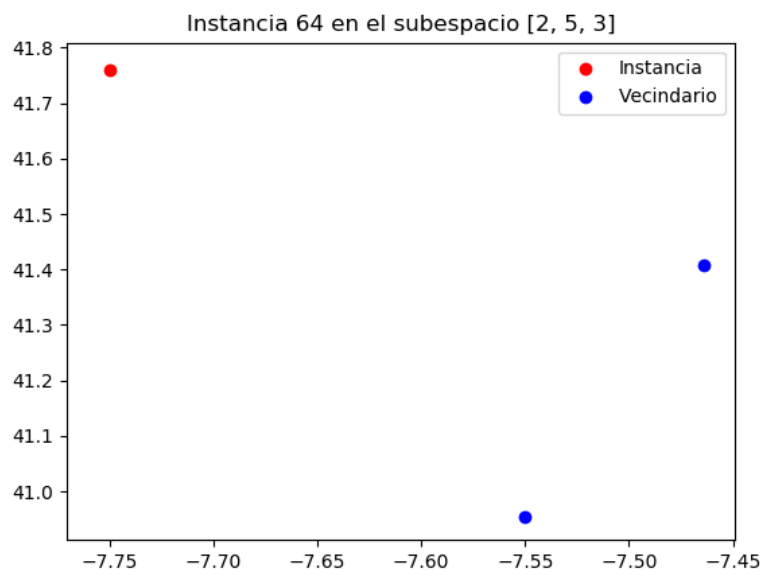


Figura 7.30: Instancia 64 sobre el subespacio  $[2, 5, 3]$

Como podemos ver en este caso tenemos un subespacio de dimensión 3. Las instancias azules están más próximas entre sí que con respecto a la roja por lo que es normal que esta sea considerada anómala en este subespacio pues está aislada.

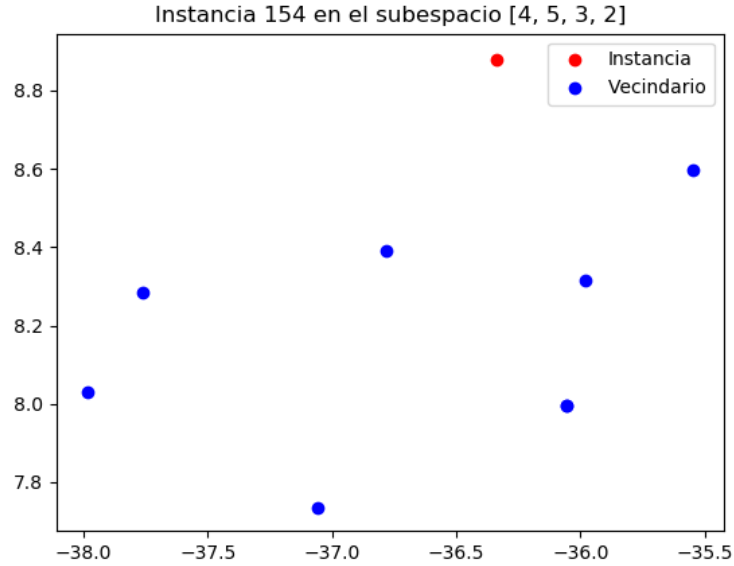
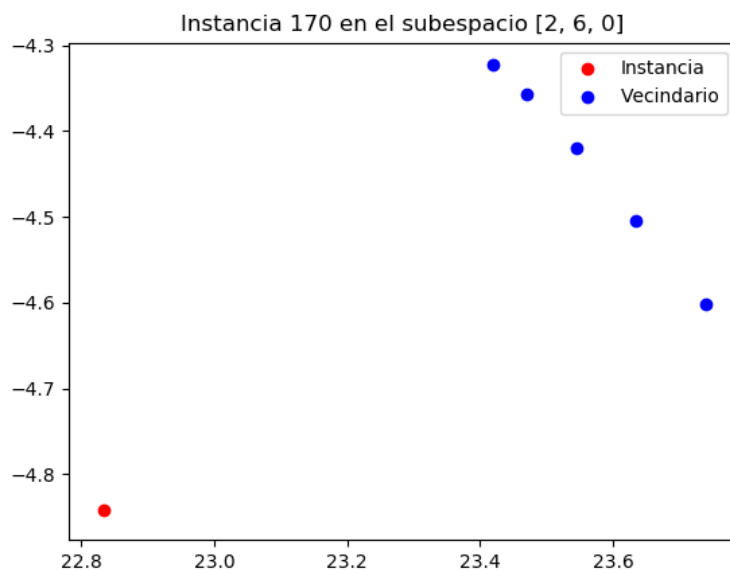


Figura 7.31: Instancia 154 sobre el subespacio [4, 5, 3, 2]

Este ejemplo es de un subespacio de dimensionalidad 4. Aquí podemos ver claramente que de nuevo la instancia no sólo se encuentra algo aislada, si no que se encuentra en lo que podemos calificar como una zona poco densa con respecto a sus vecinos. Por ejemplo el dato central de esta figura no podría ser nunca considerado una anomalía en este subespacio concreto, pues al menos el vecindario sería como mínimo el que estamos observando y por tanto vemos que no es un dato raro, de hecho es el centroide de este vecindario.

Figura 7.32: Instancia 170 sobre el subespacio  $[2, 6, 0]$ 

Este ejemplo es aún más esclarecedor pues como podemos ver los datos normales están no sólo muy concentrados, si no además alineados. Esta idea de encontrar alineamiento en subespacios podría ser una buena característica a buscar en subespacios para poder emplear en ellos técnicas como Mahalanobis Kernel.

Para que sea más fácil ver los datos de acierto, vamos a ponerlos en una tabla.

Data / Mod	Trinity	MK	OUTRES	LODA	HICS	ABOD	COF	HBOS	KNN	LOF	MCD	OCSVM	PCA	SOD	SOS
anathyroid	26.2172 %	12.3595 %	7.4906 %	8.9887 %	6.5543 %	25.0936 %	23.0936 %	26.0299 %	28.4614 %	29.2134 %	<b>45.8801 %</b>	11.2359 %	23.7827 %	30.7116 %	7.4906 %
arrhythmia	48.4848 %	<b>51.5151 %</b>	NAN	37.8787 %	NAN	37.8787 %	46.9696 %	50 %	48.4848 %	42.4242 %	<b>51.5151 %</b>	15.1515 %	42.4242 %	28.7878 %	13.6363 %
breastw	93.3054 %	<b>95.3974 %</b>	50.6276 %	<b>95.3974 %</b>	1.2552 %	NAN	8.3682 %	93.7238 %	91.2133 %	13.3891 %	89.9581 %	91.2133 %	92.8870 %	80.7531 %	49.7907 %
cardio	44.3181 %	51.7045 %	NAN	59.0909 %	NAN	22.7272 %	19.8863 %	47.1590 %	33.5227 %	17.0454 %	40.9090 %	50.5681 %	<b>60.7954 %</b>	<b>25.5681 %</b>	10.7954 %
glass	11.1111 %	0 %	0 %	0 %	11.1111 %	11.1111 %	<b>22.2222 %</b>	0 %	11.1111 %	<b>22.2222 %</b>	0 %	11.1111 %	11.1111 %	<b>22.2222 %</b>	11.1111 %
ionosphere	73.0158 %	57.1428 %	NAN	46.8233 %	NAN	84.1269 %	77.7777 %	48.4126 %	87.3015 %	76.1904 %	<b>88.0952 %</b>	64.2857 %	59.5238 %	80.1587 %	61.1111 %
letter	16 %	15 %	NAN	4 %	NAN	NAN	42 %	6 %	43 %	46 %	16 %	48 %	8 %	<b>51 %</b>	6 %
lympho	83.3333 %	50 %	NAN	0 %	NAN	33.3333 %	50 %	<b>100 %</b>	66.6666 %	83.3333 %	50 %	50 %	66.6666 %	50 %	16.6666 %
mammography	25.7692 %	1.1538 %	5.3846 %	<b>28.0769 %</b>	8.0769 %	0.3846 %	13.8461 %	12.6923 %	21.9230 %	19.2307 %	0.7692 %	27.3076 %	25.7692 %	15 %	5 %
mus1	40.2857 %	<b>54.7142 %</b>	NAN	2 %	NAN	28.5714 %	21.4285 %	17.1428 %	39.5714 %	24.2857 %	49.1428 %	0.1428 %	38.5714 %	20.5714 %	11.5714 %
mus2	34.0206 %	0 %	NAN	32.9896 %	NAN	2.0618 %	8.2474 %	90.7216 %	1.0309 %	3.0927 %	96.9072 %	0 %	<b>98.9690 %</b>	4.1237 %	6.1855 %
optdigits	1.3333 %	0 %	NAN	0 %	NAN	4.6666 %	9.3333 %	<b>18.6666 %</b>	3.3333 %	10.6666 %	0 %	1.3333 %	0 %	3.3333 %	2.6666 %
pendigits	25 %	16.6666 %	2.5641 %	0 %	NAN	7.0512 %	7.6923 %	32.0512 %	8.9743 %	6.4102 %	10.2564 %	26.2820 %	<b>32.0923 %</b>	6.4102 %	2.5641 %
pinna	50.7462 %	38.8059 %	34.7014 %	<b>54.8507 %</b>	30.5970 %	45.8955 %	37.3134 %	50.7462 %	48.1343 %	36.9402 %	51.4925 %	39.5522 %	49.6268 %	41.4179 %	36.1940 %
satellite	54.3713 %	32.8585 %	NAN	12.6227 %	NAN	NAN	43.5166 %	56.8271 %	50.0982 %	37.0825 %	<b>68.4675 %</b>	30.1571 %	48.3791 %	41.3064 %	29.9115 %
satimage-2	<b>90.1408 %</b>	<b>90.1408 %</b>	NAN	0 %	NAN	16.9014 %	12.6760 %	64.7887 %	39.4306 %	7.0422 %	63.3802 %	0 %	83.0985 %	22.5382 %	2.8169 %
speech	0 %	4.9180 %	NAN	3.2786 %	NAN	<b>13.1147 %</b>	1.6393 %	3.2786 %	1.6393 %	3.2786 %	<b>65.5913 %</b>	15.0537 %	3.2786 %	21.5053 %	9.8360 %
thyroid	39.7849 %	22.5806 %	5.3763 %	1.0752 %	0 %	0 %	4.3010 %	48.3870 %	23.0559 %	19.3548 %	0 %	<b>23.3333 %</b>	0 %	3.3333 %	4.3010 %
vertebral	3.3333 %	3.3333 %	3.3333 %	0 %	3.3333 %	6.6666 %	10 %	3.3333 %	0 %	3.3333 %	0 %	26 %	0 %	3.3333 %	13.3333 %
vowels	24 %	0 %	4 %	8 %	32 %	<b>74 %</b>	50 %	12 %	48 %	34 %	6 %	26 %	14 %	44 %	28 %
wbc	42.8571 %	0 %	NAN	<b>71.4285 %</b>	NAN	33.3333 %	28.5714 %	61.9047 %	52.3809 %	42.8571 %	42.8571 %	61.9047 %	57.1428 %	52.3809 %	14.2857 %
wine	60 %	10 %	0 %	80 %	80 %	60 %	70 %	0 %	80 %	<b>90 %</b>	50 %	10 %	30 %	50 %	0 %



Para poder completar el estudio, al estar en un caso de clasificación binaria, podemos incluir los valores AUC y algunas de las curvas ROC asociadas. Para ello en primer lugar vamos a ver la tabla de valores AUC.

Data / Model	Tinity	MK	OUTRES	LODA	HICS	ABOD	COF	HBOS	KNN	LOF	MCD	OCSVM	PCA	SOD	SOS
amthyroid	0.6015	0.5266	0.5003	0.5084	0.4953	0.5954	0.5833	0.6005	0.6136	0.6177	<b>0.7077</b>	0.5206	0.5883	0.6258	0.5003
arhythmia	0.6983	<b>0.7161</b>	NAN	0.6362	NAN	0.6362	0.6895	0.7072	0.6983	0.6628	0.7161	0.5032	0.6628	0.5830	0.4943
breastw	0.9485	<b>0.9646</b>	0.6202	<b>0.9646</b>	0.2405	NAN	0.2952	0.9517	0.9324	0.3338	0.9227	0.9324	0.9452	0.8519	0.6138
cardio	0.6919	0.7328	NAN	0.7737	NAN	0.5725	0.5568	0.7076	0.6322	0.5411	0.6731	0.7265	<b>0.7831</b>	0.5882	0.5065
glass	0.5360	0.4780	0.4780	0.4780	0.5360	0.5360	<b>0.5940</b>	0.4780	0.5360	<b>0.5940</b>	0.4780	0.5360	0.5360	<b>0.5940</b>	0.5360
ionosphere	0.7895	0.6657	NAN	0.5852	NAN	0.8761	0.8266	0.5976	0.9009	0.8142	<b>0.9071</b>	0.7214	0.6842	0.8452	0.6966
letter	0.5519	0.5466	NAN	0.488	NAN	NAN	0.6906	0.4986	0.696	0.712	0.5519	0.7226	0.5093	<b>0.7386</b>	0.4986
lympho	<b>0.9131</b>	0.7394	NAN	0.4788	NAN	0.6525	0.7394	1.0	0.8262	<b>0.9131</b>	0.7394	0.7394	0.8262	0.7394	0.5657
mammography	0.6200	0.4940	0.5156	<b>0.6318</b>	0.5294	0.4900	0.5589	0.5530	0.6003	0.5865	0.4920	0.6278	0.6200	0.5648	0.5136
mnist	0.6711	<b>0.7506</b>	NAN	0.4603	NAN	0.6066	0.5673	0.5437	0.6672	0.5830	0.7199	0.4500	0.6617	0.5625	0.5130
musk	0.6593	0.4836	NAN	0.6539	NAN	0.4942	0.5262	0.9520	0.4889	0.4996	0.9840	0.4836	<b>0.9946</b>	0.5049	0.5155
optdigits	0.4920	0.4851	NAN	0.4851	NAN	0.5092	0.5332	<b>0.5812</b>	0.5023	0.5401	0.4851	0.4920	0.4851	0.5023	0.4989
pendigits	0.6162	0.5736	0.5015	0.4883	NAN	0.5244	0.5277	0.6523	0.5342	0.5211	0.5408	0.6228	<b>0.6556</b>	0.5211	0.5015
pinna	0.6217	0.5300	0.4985	<b>0.6532</b>	0.4669	0.5844	0.5185	0.6217	0.6016	0.5157	0.6274	0.5357	0.6131	0.5500	0.5099
satellite	0.6662	0.5089	NAN	0.3609	NAN	NAN	0.5868	0.6842	0.6350	0.5398	<b>0.7693</b>	0.4891	0.6224	0.5707	0.4873
satimage-2	<b>0.9500</b>	<b>0.9500</b>	NAN	0.4938	NAN	0.5793	0.5579	0.8217	0.6934	0.5294	0.8146	0.4938	0.9144	0.6078	0.5080
speech	0.4915	0.5165	NAN	0.5082	NAN	<b>0.5582</b>	0.4992	0.5082	0.4992	0.5082	0.5082	0.4999	0.5082	0.5082	0.5415
thyroid	0.6913	0.6031	0.5149	0.4928	0.4873	0.4873	0.5094	0.7354	0.6086	0.5865	<b>0.8236</b>	0.5645	0.6692	0.5976	0.5094
vertebral	0.4476	0.4857	0.4476	0.4285	0.4476	0.4666	0.4857	0.4476	0.4285	0.4476	0.4285	<b>0.5619</b>	0.4285	0.4476	0.5047
vowels	0.6064	0.4822	0.5029	0.5236	0.6479	<b>0.8653</b>	0.7411	0.5443	0.7307	0.6582	0.5132	0.6168	0.5547	0.7100	0.6271
wbc	0.6974	0.4705	NAN	<b>0.8487</b>	NAN	0.6470	0.6218	0.7983	0.7478	0.6974	0.6974	0.7983	0.7731	0.7478	0.5462
wine	0.7831	0.5121	0.4579	0.8915	0.8915	0.7831	0.8373	0.4579	0.8915	<b>0.9457</b>	0.7289	0.5121	0.6205	0.7289	0.4579

En este caso podemos ver que el mejor de los valores de AUC para todos los datasets vuelve a ser superior al resto en 8 conjuntos de datos con nuestros modelos de ensamblaje.

Hagamos un breve repaso del valor AUC para poder entender los valores que hemos obtenido. El valor AUC o área bajo la curva ROC viene dado por el área que engloba la curva ROC, que es aquella que mide la tasa de verdaderos positivos frente a la tasa de falsos positivos, es decir:

$$TPR = \frac{VP}{VP + FN}, \quad FPR = \frac{FP}{VN + FP}.$$

Donde  $VP$  es el número de verdaderos positivos,  $FP$  el número de falsos positivos,  $VN$  el número de verdaderos negativos y  $FN$  el número de falsos negativos. Es decir en la tasa de verdaderos positivos o  $TPR$  medimos cuántos aciertos tenemos frente al número negativos que fallamos y en la tasa de falsos positivos medimos los falsos positivos que cometemos frente a los verdaderos negativos. De esta forma lo que nos va a interesar es que nuestro modelo obtenga una alta tasa  $TPR$ , es decir, que acertemos muchos positivos y una tasa baja de  $FPR$  o lo que es lo mismo, no cometer muchos falsos positivos.

La curva ROC dibuja la  $TPR$  en el eje  $Y$  y la  $FPR$  en el eje  $X$ . Por tanto el mejor valor que podemos obtener de  $TPR$  frente a  $FPR$  sería un valor de 1, lo que nos dejaría con un valor AUC de 1. El peor de los escenarios sería todo lo contrario, es decir, un valor de 0 de  $TPR$  frente a  $FPR$  y por tanto un valor AUC de 0. Si por contra obtenemos un valor de entorno a 0.5 entonces lo que estamos obteniendo es que tenemos aproximadamente una proporción similar de falsos positivos y de verdaderos positivos con lo que nuestro modelo no sería mucho mejor que un modelo aleatorio.

Una vez que tenemos esta información vamos a estudiar los valores AUC obtenidos para estos conjuntos de datos. Como podemos ver tenemos conjuntos en los que ningún modelo obtiene un rendimiento bueno como por ejemplo el conjunto “speech”. Para este conjunto el mayor de los valores AUC es 0.5582 con lo que ninguno de los modelos obtiene un resultado mejor que un modelo aleatorio o no informado.

Como podemos ver los dos modelos que repuntan en cuanto a los valores AUC vuelven a ser Mahalanobis Kernel y Trinity, siendo LODA el modelo que le sigue en cuanto a mejores valores AUC. Tanto HICS como OUTRES obtienen unos valores peores siendo casi todos valores entorno a 0.5 menos en el conjunto “wine” donde obtienen los mejores resultados de entre nuestros modelos.

Estos valores corroboran nuestras conclusiones sobre Mahalanobis Kernel y Trinity en cuanto a robustez y nos confirman también el desempeño de LODA. En cuanto a los algoritmos HICS y OUTRES volvemos a obtener resultados no satisfactorios.

Veamos ahora para cada modelo la mejor y la peor curva ROC por parejas para poder ver gráficamente estos resultados.

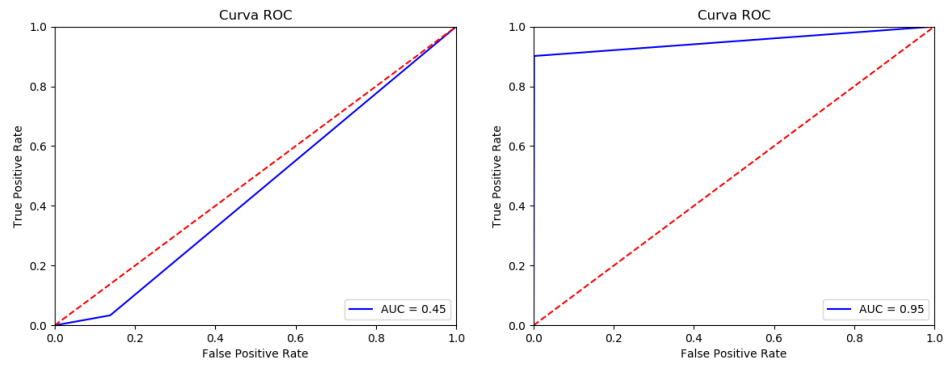


Figura 7.33: Curvas ROC para Trinity

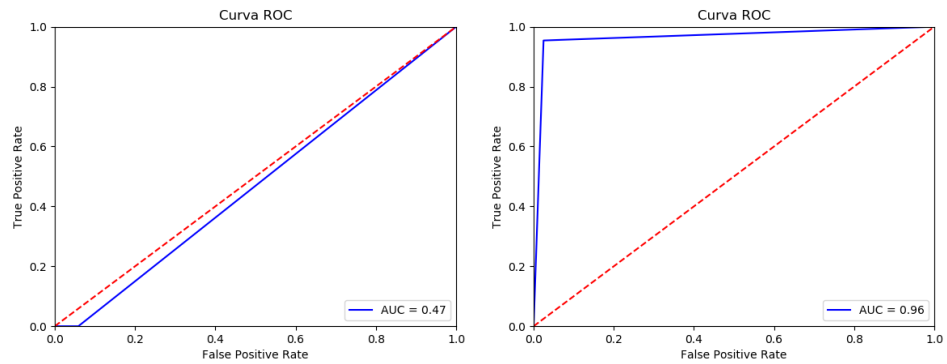


Figura 7.34: Curvas ROC para Mahalanobis Kernel

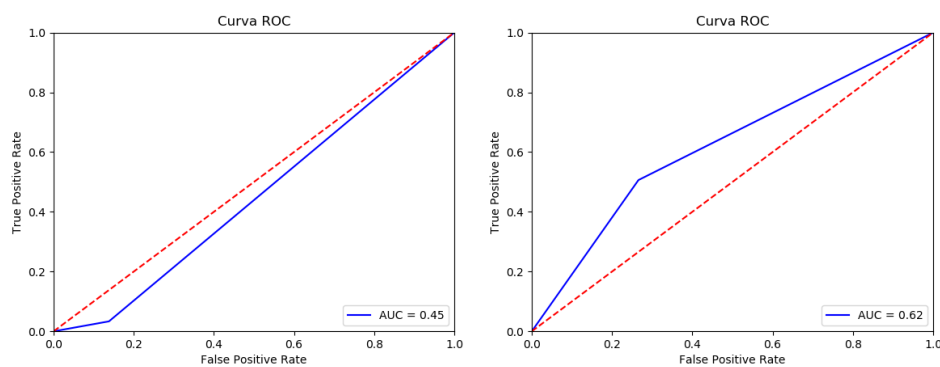


Figura 7.35: Curvas ROC para OUTRES

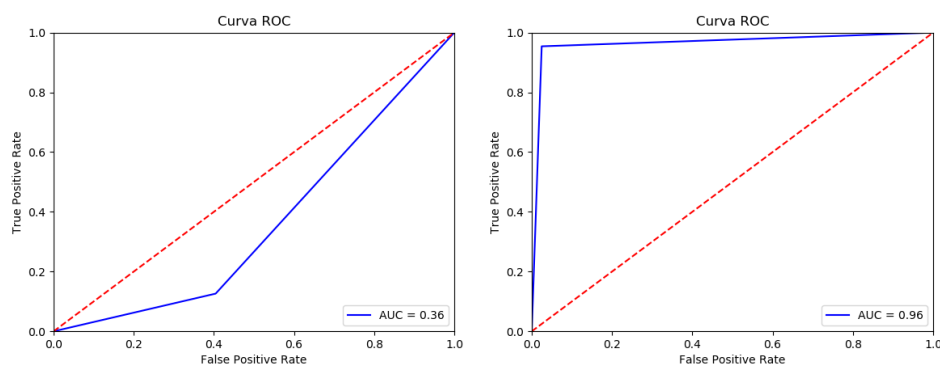


Figura 7.36: Curvas ROC para LODA

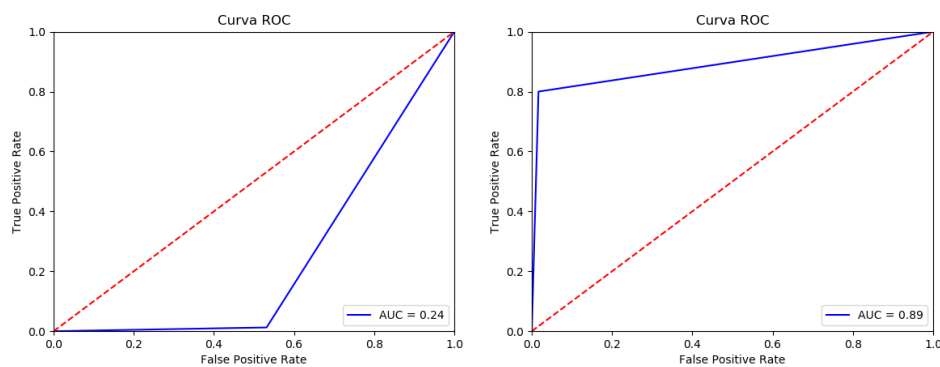


Figura 7.37: Curvas ROC para HICS

Estas gráficas confirman lo descrito por los valores AUC y además nos

dan una idea del rango de valores entre los que se mueve cada algoritmo. Como podemos ver para todos los modelos el peor de los casos es un modelo no informado o aún peor incluso con tasas AUC menores a 0.5. Por contra los tres mejores casos que obtenemos son los de Mahalanobis Kernel, LODA y Trinity. Para HICS obtenemos un buen resultado pero sólo en el conjunto “wine”, en el resto no tenemos buenos resultados de valores AUC.

Ahora para completar vamos a ver las gráficas de los tiempos consumidos por cada algoritmo para cada conjunto de datos junto con la tabla de los mismos.

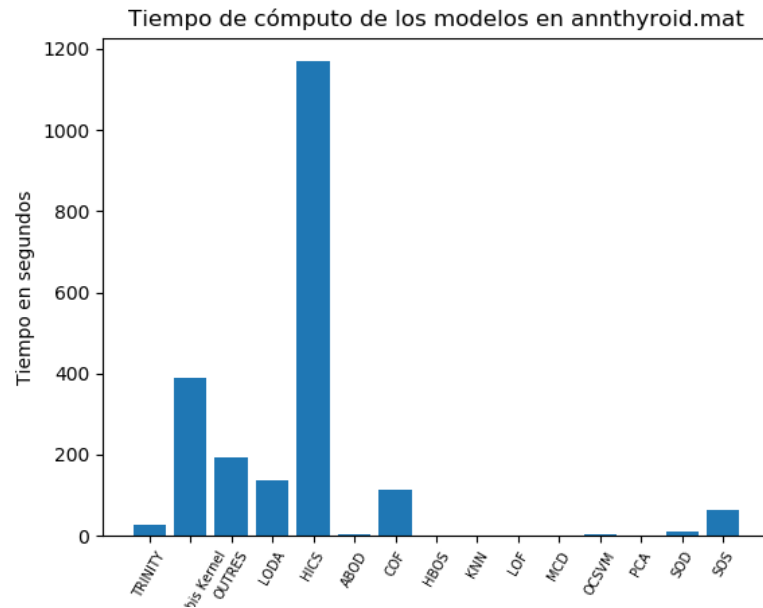


Figura 7.38: Tiempos sobre el conjunto de datos annthyroid

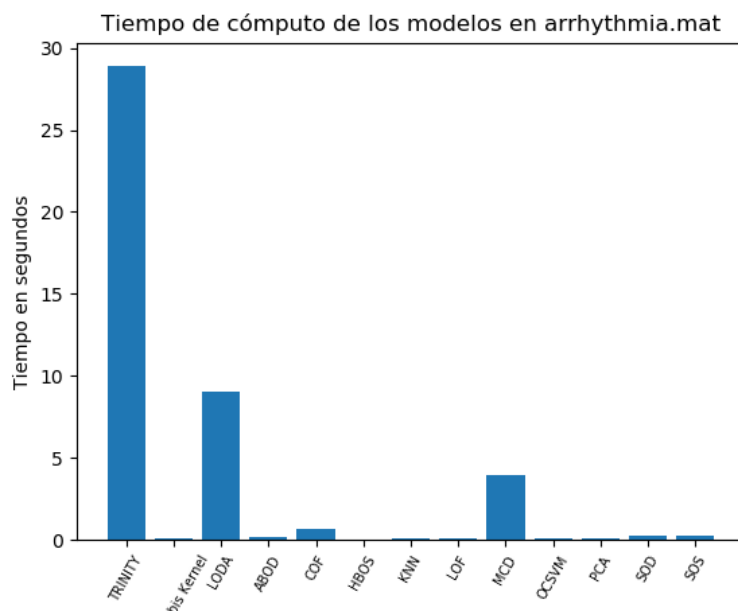


Figura 7.39: Tiempos sobre el conjunto de datos arrhythmia

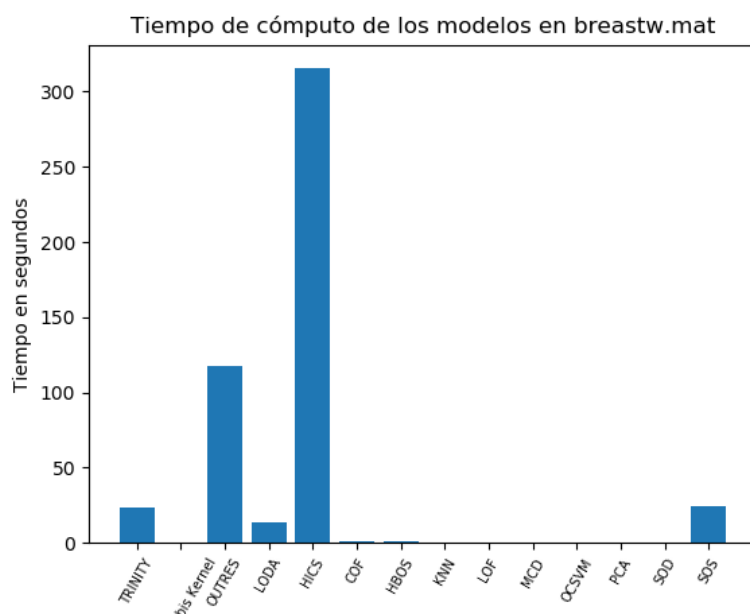


Figura 7.40: Tiempos sobre el conjunto de datos breastw

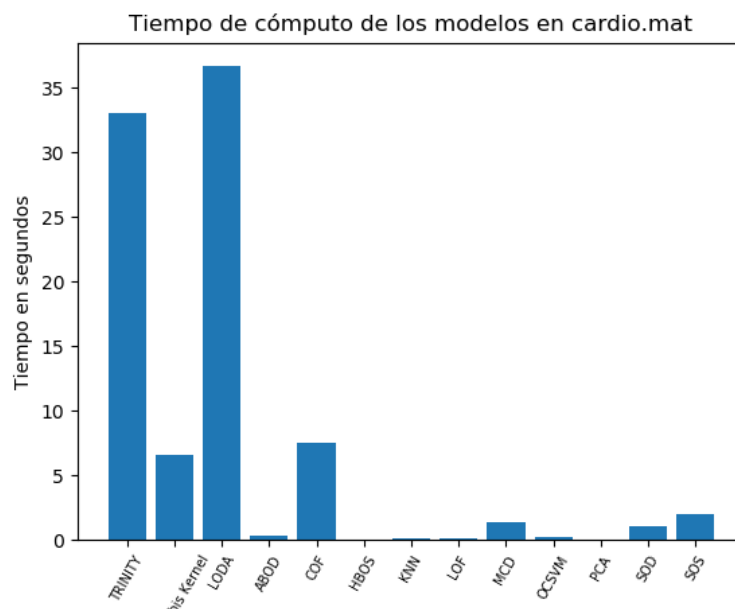


Figura 7.41: Tiempos sobre el conjunto de datos cardio

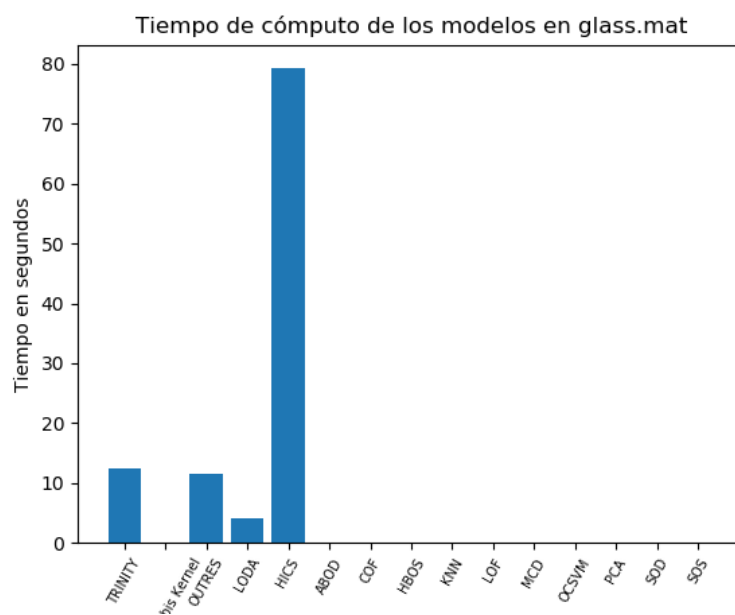


Figura 7.42: Tiempos sobre el conjunto de datos glass



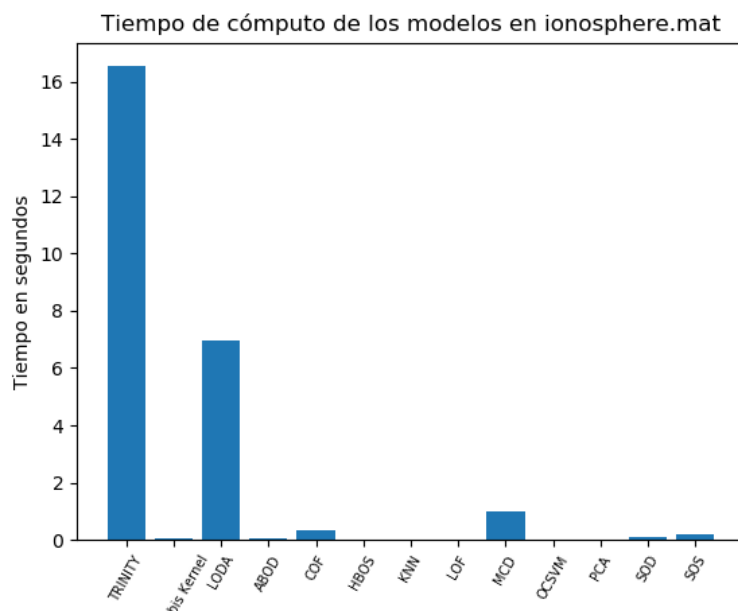


Figura 7.43: Tiempos sobre el conjunto de datos ionosphere

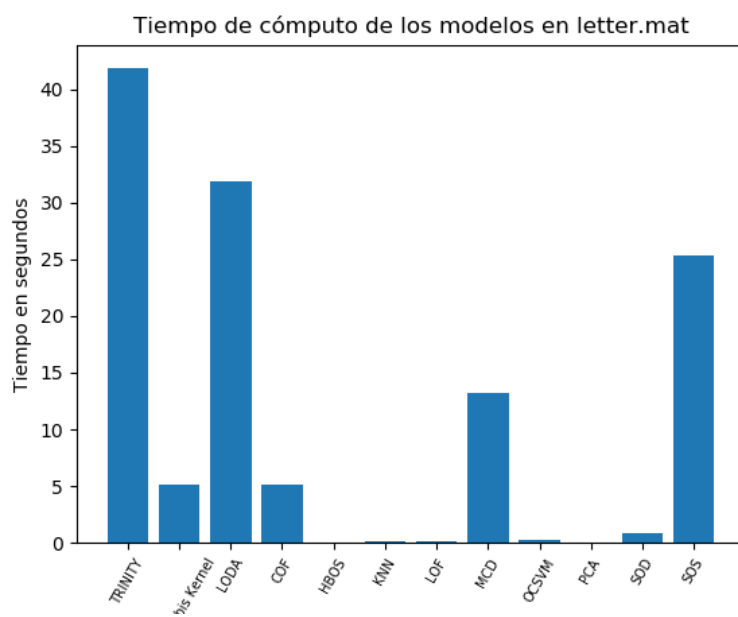


Figura 7.44: Tiempos sobre el conjunto de datos letter

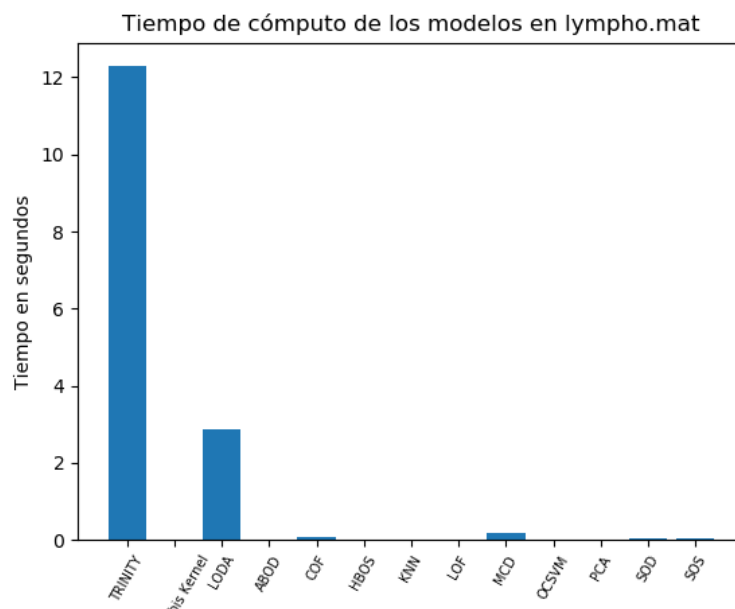


Figura 7.45: Tiempos sobre el conjunto de datos lympho

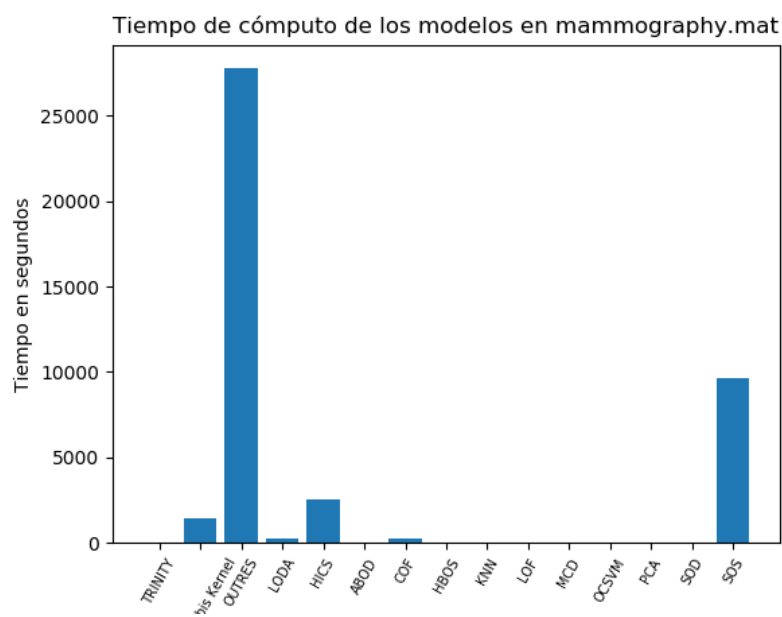


Figura 7.46: Tiempos sobre el conjunto de datos mammography

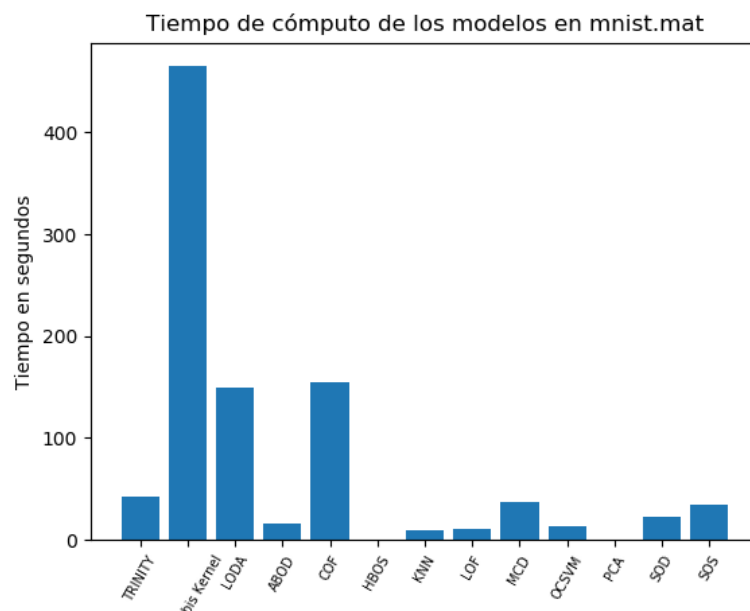


Figura 7.47: Tiempos sobre el conjunto de datos mnist

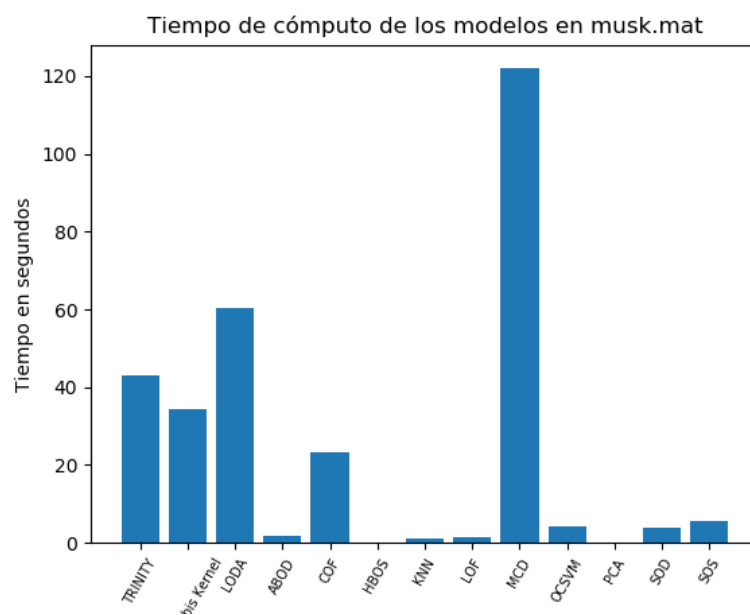


Figura 7.48: Tiempos sobre el conjunto de datos musk

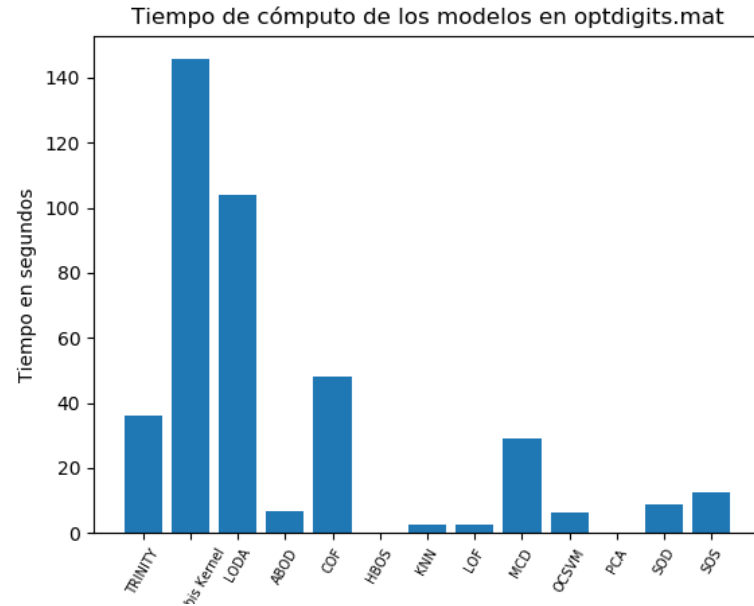


Figura 7.49: Tiempos sobre el conjunto de datos optdigits

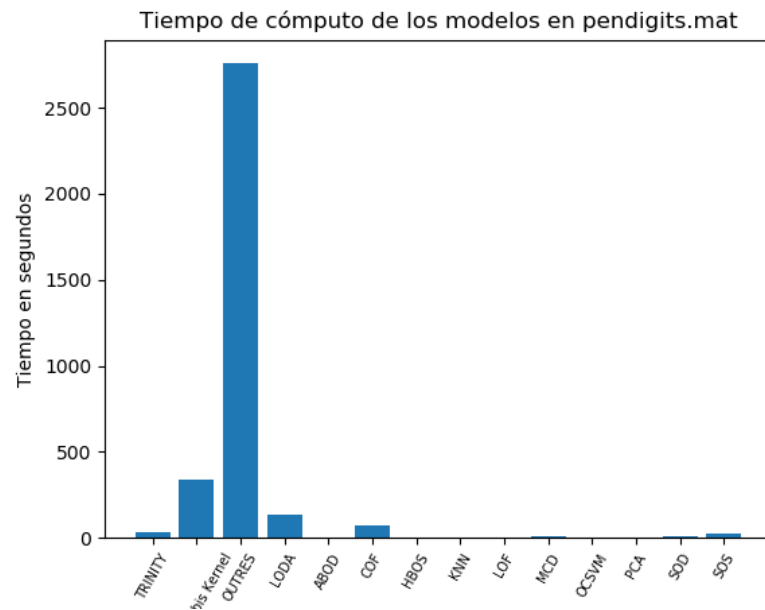


Figura 7.50: Tiempos sobre el conjunto de datos pendigits

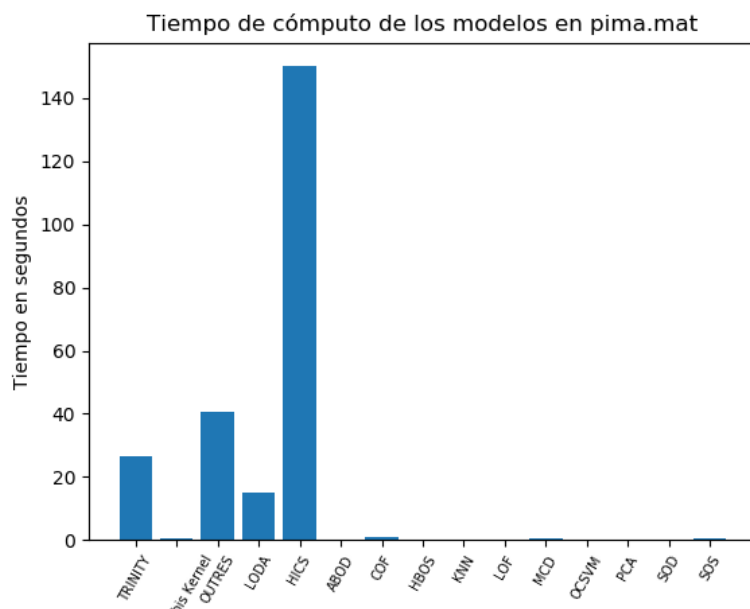


Figura 7.51: Tiempos sobre el conjunto de datos pima

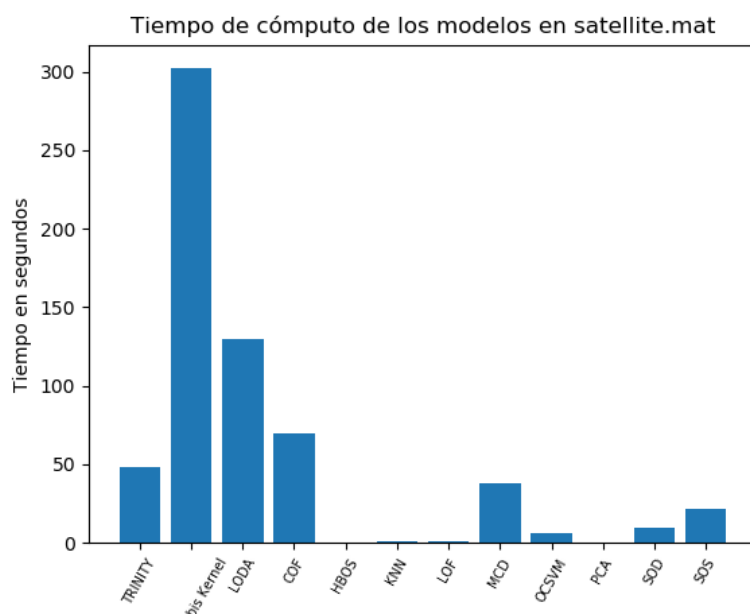


Figura 7.52: Tiempos sobre el conjunto de datos satellite

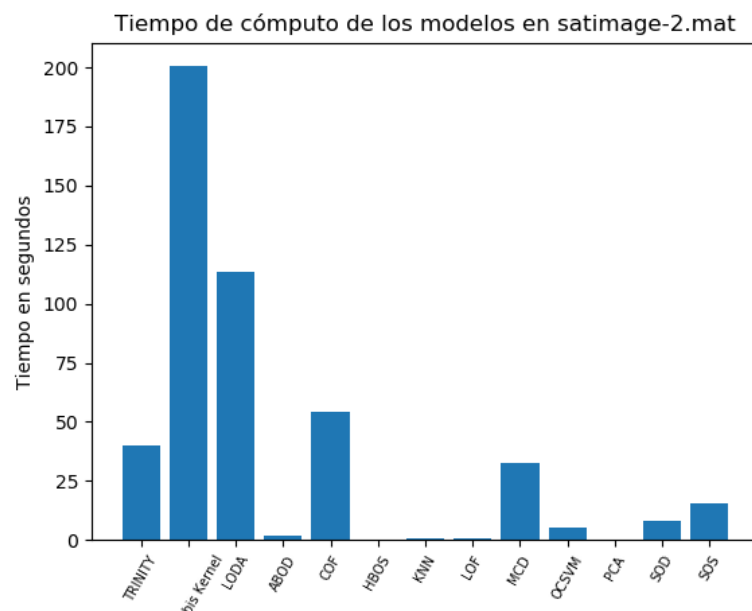


Figura 7.53: Tiempos sobre el conjunto de datos satimage-2

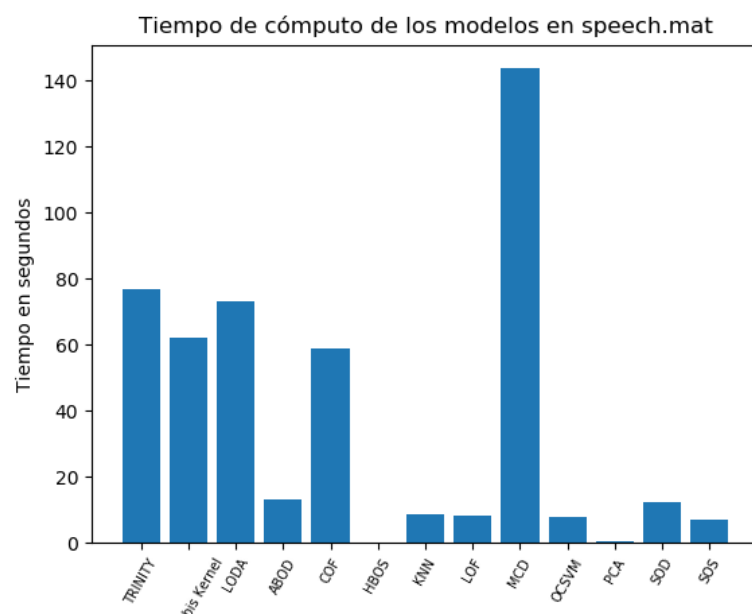


Figura 7.54: Tiempos sobre el conjunto de datos speech

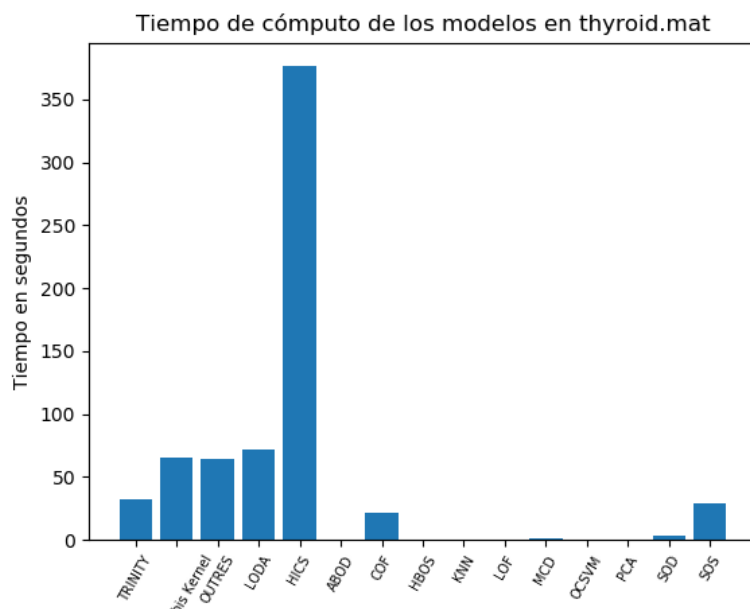


Figura 7.55: Tiempos sobre el conjunto de datos thyroid

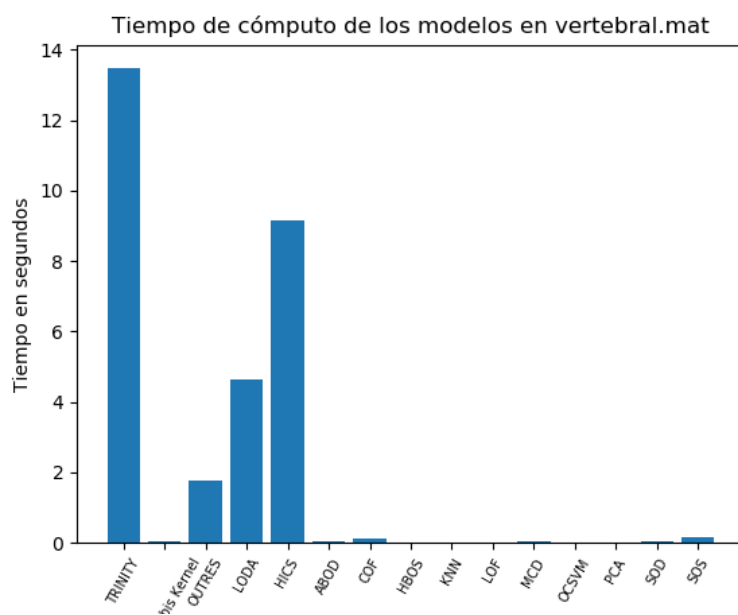


Figura 7.56: Tiempos sobre el conjunto de datos vertebral

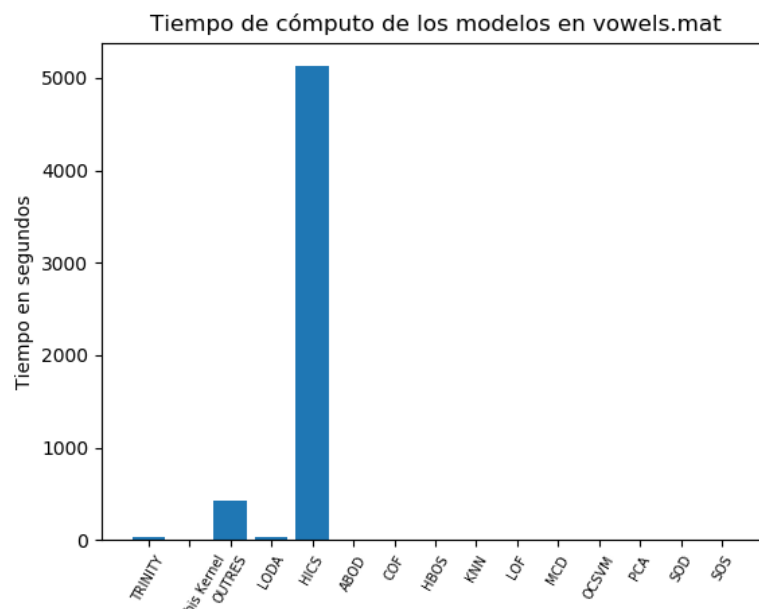


Figura 7.57: Tiempos sobre el conjunto de datos vowels

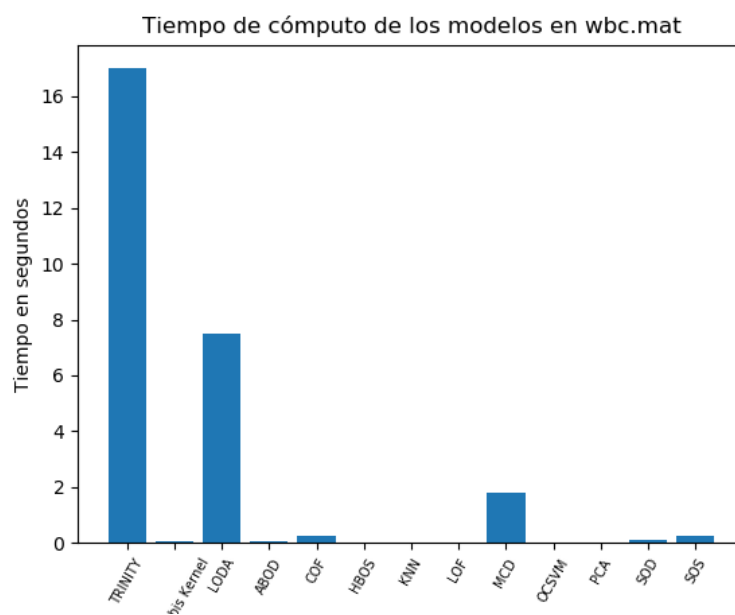


Figura 7.58: Tiempos sobre el conjunto de datos wbc



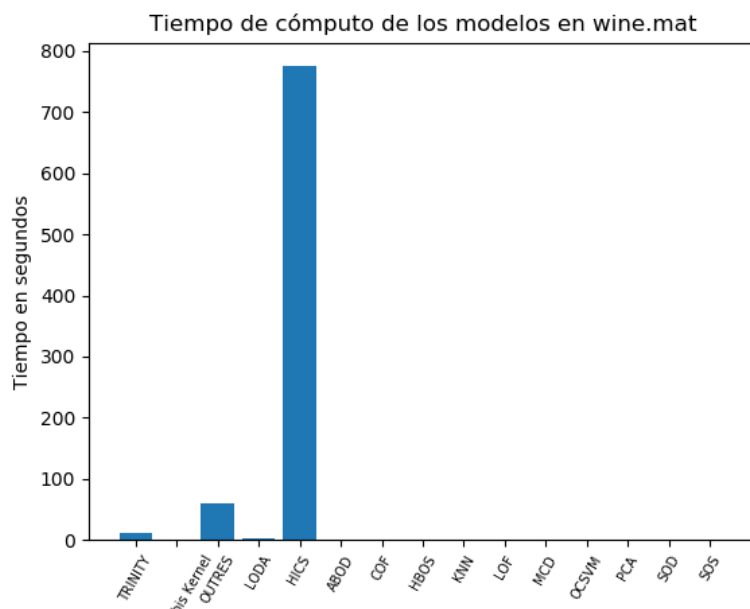


Figura 7.59: Tiempos sobre el conjunto de datos wine

Hay una cosa que podemos ver claramente y es el hecho de que los algoritmos de ensamblaje consumen un tiempo mayor en general que los algoritmos clásicos. De entre los 5 algoritmos implementados que se han propuesto podemos ver que cuando OUTRES y HICS se ejecutan sobre el conjunto son los que consumen un mayor tiempo, siendo no sólo los que más tiempo consumen si no que además obtienen los mayores tiempos de todos los conjuntos de datos superando incluso los mil segundos.

Tanto Trinity como Mahalanobis Kernel y LODA tienen conjuntos de datos en los que son los algoritmos que más tardan por lo que no podemos decir que uno sea más lento que el resto.

Veamos los tiempos en segundos en una tabla de datos.

Data / Mod	Trinity	MK	OUTRES	LODA	HICS	ABOD	COF	HBOS	KNN	LOF	MCD	OCSVM	PCA	SOD	SOS
<b>antithyroid</b>	28.5212	300.5397	193.6110	137.8692	1169.3422	2.5419	114.7065	1.2222	0.2307	0.1145	1.5861	0.0038	0.0038	10.9631	63.2884
<b>arhythmia</b>	28.8828	0.1243	NAN	9.0474	NAN	0.1662	0.6619	0.0508	0.0759	0.0917	3.9257	0.1281	0.0843	0.2299	0.2713
<b>breastw</b>	23.3296	0.3165	117.8225	13.2879	315.4130	NAN	1.0530	0.7055	0.0057	0.0098	0.5311	0.0200	0.0189	0.2007	23.9622
<b>cardio</b>	33.0496	6.5851	NAN	36.6768	NAN	0.3701	7.4887	0.0053	0.0872	0.1170	1.3748	0.2028	0.0051	1.0434	2.0196
<b>glass</b>	12.5272	0.0220	11.5349	4.0798	79.2560	0.0358	0.1341	0.0036	0.0014	0.0021	0.0905	0.0028	0.0021	0.0421	0.1425
<b>ionosphere</b>	16.5319	0.0565	NAN	6.9664	NAN	0.0641	0.3415	0.0062	0.0071	0.0101	0.9893	0.0103	0.0044	0.0897	0.2140
<b>letter</b>	41.8301	5.1648	NAN	31.8875	NAN	NAN	5.1220	0.0075	0.0839	0.1047	13.1818	0.2577	0.0073	0.8809	25.3305
<b>lympho</b>	12.2874	0.0187	NAN	2.8804	NAN	0.0228	0.0693	0.0038	0.0014	0.0017	0.1741	0.0020	0.0029	0.0288	0.0526
<b>mammography</b>	31.5619	1444.1323	27765.1978	224.8207	2502.0258	1.7394	280.7073	0.0037	0.2790	0.3027	2.3683	5.8535	0.0066	25.2311	9653.7372
<b>mnist</b>	42.7623	464.8962	NAN	150.1434	NAN	16.4729	154.4384	0.0502	9.7564	10.2119	37.5253	14.0057	0.1746	22.8423	34.5968
<b>musk</b>	42.8683	34.4336	NAN	60.4207	NAN	1.6461	23.2048	0.0555	1.1578	1.3294	121.9505	4.1720	0.2416	3.8690	5.7815
<b>optdigits</b>	36.2723	145.6876	NAN	103.9115	NAN	6.6622	47.9141	0.0312	2.3891	2.4586	29.2400	6.0881	0.0513	8.8440	12.5010
<b>pendigits</b>	34.0999	340.2855	2757.0345	135.0839	NAN	1.4151	75.1194	0.0076	0.3140	0.4336	6.3704	3.1717	0.0105	10.5999	25.3345
<b>pinna</b>	26.3576	0.3482	40.6379	15.2128	150.1283	0.1230	0.9667	0.0021	0.0053	0.0057	0.5652	0.0567	0.0028	0.2303	0.4855
<b>satellite</b>	48.2618	301.9960	NAN	129.6712	NAN	NAN	70.0058	0.0146	0.7749	0.8185	38.1214	6.5430	0.0305	9.8771	21.9062
<b>satimage-2</b>	39.7535	200.5037	NAN	113.2818	NAN	1.7584	54.0372	0.0139	0.7183	0.7796	32.5359	5.4775	0.0240	8.2761	15.4193
<b>speech</b>	76.6633	62.2470	NAN	73.0844	NAN	13.2967	58.9203	0.1523	8.6546	8.4023	143.7647	7.8068	0.5699	12.2820	7.1908
<b>thyroid</b>	32.6503	65.3469	64.2370	72.1607	376.2697	0.5982	21.8574	0.0022	0.0450	0.0676	1.0717	0.5607	0.0026	3.3138	29.4608
<b>vertebral</b>	13.4726	0.0301	1.7653	4.6250	9.1404	0.0355	0.1153	0.0013	0.0015	0.0019	0.0435	0.0050	0.0011	0.0472	0.1450
<b>vowels</b>	36.2093	3.1876	426.6157	28.2930	5126.5627	0.2367	3.3253	0.0030	0.0247	0.0346	0.8870	0.0890	0.0023	0.6860	1.3831
<b>wbc</b>	17.0011	0.0675	NAN	7.5109	NAN	0.0700	0.2526	0.0061	0.0082	0.0080	1.7926	0.0101	0.0043	0.0864	0.2449
<b>wine</b>	11.2756	0.0165	58.9642	2.4540	774.9212	0.0231	0.0421	0.0025	0.0010	0.0032	0.1075	0.0020	0.0020	0.0226	0.0539

Cuadro 7.2: Tabla de tiempos

## 7.4. Conclusiones y trabajo futuro

Ya hemos visto todos los resultados que hemos obtenido con los modelos y el análisis de cómo funcionan de forma teórica por lo que hemos reunido todos los ingredientes necesarios para sacar algunas conclusiones sobre este estudio.

En primer lugar cabe decir que en general los algoritmos que hemos implementado (salvo los basados en subespacios) están al mismo nivel de rendimiento que los modelos clásicos. En este estudio he comprendido el potencial que podría tener un buen modelo que combine de forma adecuada modelos clásicos o incluso modelos de ensamblaje.

El enfoque de los algoritmos basados en subespacios que se han implementado no parece ser algo que funcione en conjuntos de datos reales aunque los conceptos de densidad puedan resultar interesantes por ofrecer otro punto de vista. Algoritmos como HICS y OUTRES pueden ofrecer un buen aporte extra para un modelo ya implementado, es decir, utilizar estos algoritmos para detectar lo que ellos mismos llaman anomalías no triviales. Como modelos individuales ya hemos visto que no tienen un desempeño demasiado bueno además del alto consumo en tiempo que tienen y que hace que sea difícil su aplicación en conjuntos de datos más grandes.

Un punto de vista interesante y que se debería tener en cuenta es la aplicación de modelos en función del tipo de datos que tengamos. Es decir, un algoritmo que regule su propio comportamiento primero analizando brevemente el conjunto de datos con algunos parámetros y posteriormente ejecutando los métodos que convengan.

Hemos podido ver en los resultados que para todos los modelos existen conjuntos de datos en los que no funcionan bien, incluso algunos llegan a sacar un 0% tanto de los clásicos como de los algoritmos de ensamblaje. Esto nos está reflejando que no es una aproximación inteligente intentar dar un algoritmo que aplique una misma técnica para todos los conjuntos de datos con los que se encuentre.

Creo que los resultados que hemos obtenido dejan margen de mejora, lo cual hace este campo interesante y desafiante para proponer nuevas ideas sobre la mesa. En primer lugar hemos visto que todos los algoritmos tienen problemas en cuanto al manejo de los valores perdidos. Es lógico que estos algoritmos no estén preparados ante vectores que no dispongan de ningún valor numérico, pero creo que sería interesante disponer de alguna técnica que nos permita trabajar con vectores que tengan algunos valores no disponibles. Podríamos pensar por ejemplo en alguna técnica que considere la

proyección del conjunto de datos sobre los atributos disponibles de esa instancia con valores perdido y hacer un estudio sobre esa proyección. Como hemos discutido previamente es fácil que, tras esas instancias con valores perdidos, se escondan anomalías reales.

Los algoritmos como HICS y OUTRES tienen ideas teóricas muy elaboradas pero no piensan en los problemas de eficiencia que llevan tras de sí, con lo que se hacen algoritmos poco prácticos para su uso. Sería de utilidad la inclusión de técnicas inherentes a los algoritmos que mejoren su eficiencia sin reducir en exceso su desempeño. Por ejemplo la aproximación de HICS al obtener los subespacios de alto contraste siempre se queda con los de mayor contraste pero a cambio debemos hacer un cómputo desmesurado de subespacios y contrastes que disminuyen terriblemente su eficiencia.

Por contra hemos visto como Trinity consigue unos resultados robustos en comparación con los modelos que emplea. Este tipo de algoritmos de ensamblaje pueden tener mejores resultados según la experiencia que he desarrollado en este trabajo. Creo que se podrían mezclar diferentes técnicas en un algoritmo como Trinity. Por ejemplo hemos visto que hay subespacios o trozos de los conjuntos de datos en los que el alineamiento de las instancias en hiperplanos u otras formas es clara y evidente. Esto nos hace pensar en la posibilidad de usar en dichas circunstancias algoritmos como Mahalanobis Kernel.

Todo este análisis nos está dejando claro que el futuro de los algoritmos de ensamblaje es prometedor y como línea principal de trabajo futuro para mí mismo destaco la posibilidad de crear un modelo con todo lo aprendido. Empleando las técnicas de análisis de subespacios, algoritmos basados en densidad y relación entre atributos y algoritmos basados en histogramas se podría desarrollar un modelo más completo que supere en desempeño a los estudiados en este trabajo y sobre todo a los algoritmos clásicos.

# Apéndices

Todo el código del proyecto está disponible y libre en GitHub en el repositorio **Ensemble Outlier Analysis**.

Todos los resultados de las ejecuciones son reproducibles con el código del repositorio.

Se puede encontrar una documentación explicando todo el contenido del mismo en el mismo repositorio accesible en formato HTML en el fichero índice: **Documentación**

Para su visualización se recomienda descargar el repositorio y acceder hasta la carpeta HTML y abrir el fichero “index.html”.



# Bibliografía

- [1] Vapnik V. *The Nature of Statistical Learning Theory*. New York: Springer.
- [2] Vladimir Cherkassky and Filip M. Mulier. *Learning from Data: Concepts, Theory, and Methods*. John Wiley & Sons. 02476.
- [3] Hastie T., R. Tibshirani, and J. Friedman. *The elements of Statistical Learning: Data Mining Inference and Prediction*. New York: Springer.
- [4] Fabian Keller, Emmanuel Müller, and Klemens Böhm. HiCS: High contrast subspaces for density-based outlier ranking. page 12.
- [5] Shebuti Ryana. ODDS library.
- [6] Yue Zhao, Zain Nasrullah, and Zheng Li. PyOD: A python toolbox for scalable outlier detection.
- [7] Abu-Mostafa Yaser, Magdon-Ismail Malik, and Lin Hsuan-Tien. *Learning from Data: a short course*.
- [8] Barbora Micenková, Brian McWilliams, and Ira Assent. Learning representations for outlier detection on a budget. 00000.
- [9] L. I. Kuncheva. A theoretical study on six classifier fusion strategies. 24(2):281–286. 00000.
- [10] M. Galar, A. Fernandez, E. Barrenechea, H. Bustince, and F. Herrera. A review on ensembles for the class imbalance problem: Bagging-, boosting-, and hybrid-based approaches. 42(4):463–484. 00000.
- [11] S. Sukhanov, C. Debes, and A. M. Zoubir. Dynamic selection of classifiers for fusing imbalanced heterogeneous data. In *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 5361–5365. 00000.
- [12] Alessio Carrega, Francesca Cipollini, and Luca Oneto. Simple continuous optimal regions of the space of data. 00000.

- [13] Francesca Cipollini, Luca Oneto, Andrea Coraddu, Alan John Murphy, and Davide Anguita. Condition-based maintenance of naval propulsion systems: Data analysis with minimal feedback. 177:12–23. 00005.
- [14] Arthur Zimek, Matthew Gaudet, Ricardo JGB Campello, and Jörg Sander. Subsampling for efficient and effective unsupervised outlier detection ensembles. In *Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 428–436. ACM.
- [15] Charu C. Aggarwal and Saket Sathe. Theoretical foundations and algorithms for outlier ensembles. 17(1):24–47.
- [16] Arthur Zimek, Erich Schubert, and Hans-Peter Kriegel. A survey on unsupervised outlier detection in high-dimensional numerical data. 5(5):363–387.
- [17] Aleksandar Lazarevic and Vipin Kumar. Feature bagging for outlier detection. In *Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining*, pages 157–166. ACM.
- [18] Yue Zhao, Maciej K. Hryniewicki, Zain Nasrullah, and Zheng Li. LSCP: Locally selective combination in parallel outlier ensembles.
- [19] Yue Zhao and Maciej K. Hryniewicki. XGBOD: improving supervised outlier detection with unsupervised representation learning. In *2018 International Joint Conference on Neural Networks (IJCNN)*, pages 1–8. IEEE.
- [20] Yue Zhao and Maciej K. Hryniewicki. DCSO: dynamic combination of detector scores for outlier ensembles. In *ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD), Outlier Detection De-constructed Workshop, London, UK*.
- [21] Zengyou He, Shengchun Deng, and Xiaofei Xu. A unified subspace outlier ensemble framework for outlier detection. In *International Conference on Web-Age Information Management*, pages 632–637. Springer.
- [22] Alexander Strehl and Joydeep Ghosh. Cluster ensembles — a knowledge reuse framework for combining multiple partitions. 3:583–617.
- [23] Charu C. Aggarwal and Philip S. Yu. Outlier detection for high dimensional data. In *Proceedings of the 2001 ACM SIGMOD International Conference on Management of Data, SIGMOD '01*, pages 37–46. ACM. event-place: Santa Barbara, California, USA.



- [24] Emmanuel Müller, Matthias Schiffer, and Thomas Seidl. Statistical selection of relevant subspace projections for outlier ranking. In *Data Engineering (ICDE), 2011 IEEE 27th International Conference on*, pages 434–445. IEEE.
- [25] Fei Tony Liu, Kai Ming Ting, and Zhi-Hua Zhou. On detecting clustered anomalies using SCiForest. In *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*, pages 274–290. Springer.
- [26] Ye Zhu and Kai Ming Ting. Commentary: a decomposition of the outlier detection problem into a set of supervised learning problems. 105(2):301–304.
- [27] Patricia Iglesias Sánchez, Emmanuel Müller, Fabian Laforet, Fabian Keller, and Klemens Böhm. Statistical selection of congruent subspaces for mining attributed graphs. In *2013 IEEE 13th International Conference on Data Mining*, pages 647–656. IEEE.
- [28] Fei Tony Liu, Kai Ming Ting, and Zhi-Hua Zhou. Isolation-based anomaly detection. 6(1):3.
- [29] Fei Tony Liu, Kai Ming Ting, and Zhi-Hua Zhou. Isolation forest. In *2008 Eighth IEEE International Conference on Data Mining*, pages 413–422. IEEE.
- [30] Jing Gao and Pang-Ning Tan. Converting output scores from outlier detection algorithms into probability estimates. In *Sixth International Conference on Data Mining (ICDM'06)*, pages 212–221. IEEE.
- [31] Tomáš Pevný. Loda: Lightweight on-line detector of anomalies. 102(2):275–304.
- [32] Saket Sathe and Charu C. Aggarwal. Subspace outlier detection in linear time with randomized hashing. In *2016 IEEE 16th International Conference on Data Mining (ICDM)*, pages 459–468. IEEE.
- [33] Leo Breiman. Bagging predictors. 24(2):123–140.
- [34] Peter Lukas Bühlmann. Bagging, subbagging and bragging for improving some prediction algorithms. In *Research report/Seminar für Statistik, Eidgenössische Technische Hochschule (ETH)*, volume 113. Seminar für Statistik, Eidgenössische Technische Hochschule (ETH), Zürich.
- [35] Andreas Buja and Werner Stuetzle. Observations on bagging. 16(2):323.
- [36] Peter Bühlmann and Bin Yu. Analyzing bagging. 30(4):927–961.
- [37] Charu C. Aggarwal. Outlier ensembles: Position paper. 14(2):49–58.

- [38] Shebuti Rayana and Leman Akoglu. Less is more: Building selective anomaly ensembles. 10(4):42.
- [39] Swee Chuan Tan, Kai Ming Ting, and Tony Fei Liu. Fast anomaly detection for streaming data. In *Twenty-Second International Joint Conference on Artificial Intelligence*.
- [40] Mahsa Salehi, Christopher A. Leckie, Masud Moshtaghi, and Tharsan Vaithianathan. A relevance weighted ensemble model for anomaly detection in switching data streams. In *Pacific-Asia Conference on Knowledge Discovery and Data Mining*, pages 461–473. Springer.
- [41] Hoang Vu Nguyen, Hock Hee Ang, and Vivekanand Gopalkrishnan. Mining outliers with ensemble of heterogeneous detectors on random subspaces. In *International Conference on Database Systems for Advanced Applications*, pages 368–383. Springer.
- [42] Zhi-Hua Zhou. *Ensemble methods: foundations and algorithms*. Chapman and Hall/CRC.
- [43] Charu C. Aggarwal and Saket Sathe. *Outlier Ensembles: An Introduction*. Springer. Google-Books-ID: UNmfDgAAQBAJ.
- [44] Charu C. Aggarwal. *Outlier Analysis*. Springer-Verlag.
- [45] Obermayer. Proof of the key theorem of statistical learning theory.
- [46] Juanjo Nieto and Antonia Delgado. Apuntes modelos matemáticos 2.
- [47] Jürgen Braun and Michael Griebel. On a constructive proof of kolmogorov’s superposition theorem. page 19.
- [48] Hoang-Vu Nguyen, Emmanuel Müller, and Klemens Böhm. A near-linear time subspace search scheme for unsupervised selection of correlated features. 1:37–51. 00002.
- [49] M. Loève. *Probability Theory*. Springer-Verlag.

