

Apuntes tema 2

Principios de los sistemas de aprendizaje automático

El **aprendizaje automático (Machine Learning)** comparte límites con la estadística o la matemática aplicada.

Permite **crear sistemas** capaces de mejorar su rendimiento de **manera autónoma** a medida que adquieren experiencia (procesar más datos).

Gracias al aprendizaje automático, los sistemas de IA se vuelven **adaptativos** (aprende de los datos y ajusta su comportamiento).

Dentro del aprendizaje automático se encuentra el **aprendizaje profundo (Deep Learning)** una subdisciplina basada en **redes neuronales artificiales** con múltiples capas.

Bases del aprendizaje automático

- **Capacidad de aprender a partir de la experiencia:** Los sistemas aprenden de los **datos** (ejemplos del mundo real).
- **El algoritmo como mecanismo de aprendizaje:** Los datos se **introducen** en un algoritmo matemático, que **analiza** la información, **detecta** patrones y **construye** un modelo.
- **Predictión y mejora continua:** Una vez entrenado el modelo puede **aplicarse a nuevos datos**, si este no da resultados satisfactorios puede **reentrenarse** para mejorar su rendimiento.

Enfoque tradicional

Un analista realizaba un análisis manual del problema, para ello **recogía correos** identificados como spam y **buscaba** patrones. A partir de estas observaciones el analista elaboraba un **conjunto de reglas** que definía las condiciones para definir si un correo es spam o no.

El **motor de reglas** se compone de un **conjunto de condiciones** programadas manualmente que permiten distinguir entre un correo electrónico legítimo y uno de spam.

Una vez definido el conjunto de reglas **se prueban** utilizando correos nuevos para comprobar la capacidad de clasificación. Si lo hace de forma **correcta** el sistema puede ser **implementado en producción**, si no se inicia una **fase de**

análisis de errores, donde se revisan que reglas **no están funcionando** correctamente, cuales son **irrelevantes** y que **nuevas** condiciones podrían añadirse.

El enfoque tradicional **depende del analista** ya que es él el que realiza todo el trabajo. Además este sistema se basa en **reglas estáticas** por lo que deben ser revisadas y actualizadas de forma periódica ya que puede quedar obsoleto si los patrones cambian.

Aprendizaje automático

Aquí el **sistema aprende de los datos** es capaz de adaptarse de forma autónoma a los nuevos patrones.

El analista se encarga de **reunir los datos** representativos del problema y de **seleccionar el algoritmo** matemático que considere más adecuado para resolverlo.

Una vez elegido el algoritmo empieza la **fase de entrenamiento** donde **proporciona los datos** al sistema de aprendizaje automático, en este proceso el algoritmo ajusta sus parámetros hasta que construye un modelo capaz de reconoceces patrones.

Una vez entrenado el modelo se somete a una **fase de evaluación** en la que se verifica si el modelo **realiza su trabajo correctamente**, si la solución es satisfactoria se implementan en producción.

En caso de que las predicciones del modelo no sean correctas se vuelve a la **fase de análisis de errores** y se evalúa la calidad de los datos utilizados o si el algoritmo seleccionado es el correcto.

¿Cuándo utilizar Machine Learning?

El Machine Learning se utiliza en los siguientes casos:

- Cuando las soluciones se basan en un **conjunto extenso de reglas** cuya gestión manual resulta compleja o ineficiente.
- En problemas complejos donde un analista no puede **definir fácilmente una solución** a partir de la información disponible, debido a la cantidad, variabilidad o ambigüedad de los datos.
- En entornos que **cambian** con frecuencia o presentan comportamientos **impredecibles**, donde las reglas fijas dejan de ser efectivas con el tiempo.
- Como **apoyo** a los métodos tradicionales de análisis

Clasificación de los sistemas de Machine Learning

El criterio más común para clasificar los sistemas y técnicas de aprendizaje automático se basa en **como** el modelo se entrena y se **ajusta** a lo largo del tiempo

Los métodos de Machine Learning pueden agruparse en varias categorías:

- Según en la forma que se entrenan:
 - **Aprendizaje supervisado:** El modelo aprende a partir de **datos etiquetados**.
 - **Aprendizaje no supervisado:** El modelo trabaja con **datos sin etiquetar**.
 - **Aprendizaje semi-supervisado:** **Combina** datos etiquetados y no etiquetados para mejorar la precisión del modelo.
 - **Aprendizaje por refuerzo:** El sistema aprende mediante la **interacción** con un **entorno**. Recibiendo recompensas o penalizaciones.
- Según la forma en que aprenden con el tiempo:
 - **Aprendizaje online:** El modelo se **actualiza de manera continua** conforme recibe nuevos datos.
 - **Aprendizaje batch (por lotes):** El modelo se entrena de **una sola vez** con un conjunto completo de datos y no se actualiza hasta que se entrena nuevamente.
- Según la forma en que realizan las predicciones:
 - **Aprendizaje basado en instancias:** Las predicciones se realizan comparando **nuevos datos** con **ejemplos almacenados** en el conjunto de entrenamiento.
 - **Aprendizaje basado en modelos:** El sistema construye una **representación general del problema** a partir de los datos y utiliza esa abstracción para realizar predicciones

Técnicas y herramientas de aprendizaje automático

Existen diferentes técnicas de aprendizaje automático, las más utilizadas son:

- **Regresión lineal y regresión logística:** Empleadas para **predecir valores numéricos** continuos o **clasificar datos** en categorías simples.

- **Árboles de decisión y bosques aleatorios (Random Forest):** Útiles en tareas de **clasificación** y **toma de decisiones** (múltiples variables)
- **K-Means:** técnica de aprendizaje no supervisado que permite **agrupar datos** en clústeres o grupos según su similitud.
- **Redes neuronales artificiales:** Modelos inspirados en el funcionamiento del cerebro humano, ampliamente utilizados en **reconocimiento de imágenes**, **procesamiento de voz** y **texto**.

Para implementar estas técnicas existen herramientas y bibliotecas como:

- **Scikit-learn:** Biblioteca de Python ampliamente utilizada para el **aprendizaje automático clásico**.
- **Weka y Orange:** Entornos gráficos interactivos que permiten experimentar con diferentes algoritmos sin necesidad de programar.
- **TensorFlow y Keras:** Bibliotecas de alto rendimiento diseñadas para el desarrollo de **modelos avanzados** y de **aprendizaje profundo**.

Técnicas

La **elección** de la técnica y la herramienta más adecuada **depende del tipo de problema** a resolver, la cantidad y calidad de los datos disponibles y el nivel de complejidad que se desee alcanzar, el objetivo es seleccionar la que **mejor** se adapte a la naturaleza de los datos y que proporcione resultados precisos, interpretables y eficientes.

Aprendizaje supervisado

En este sistema el modelo aprende a partir de **ejemplos etiquetados**.

Se parte de un conjunto de **datos de entrenamiento** que contiene pares de entrada y salida conocidos. Estos se **añaden** al algoritmo de aprendizaje el cual ajusta sus parámetros internos para encontrar una función que relacione correctamente las entradas con las salidas. El resultado es el modelo (**función hipótesis**) que posteriormente se utiliza para realizar predicciones.

La principal característica es que se necesitan ejemplos etiquetados (**conjunto de datos etiquetados**) para poder aprender la relación entre las entradas y las salidas (**función hipótesis**).

Una vez entrenado el modelo puede aplicarse a **nuevos datos** no etiquetados.

Dentro del aprendizaje supervisado encontramos dos subcategorías principales:

- **Regresión:** Se utiliza cuando el objetivo es **predecir valores continuos** (estimar el precio de una vivienda, predecir el coste económico de un incidente de seguridad, seguridad informática).
- **Clasificación:** Se utiliza cuando el objetivo es **predecir valores discretos**, es decir, resultados que pertenecen a un conjunto limitado y definido de categorías. El modelo asigna cada ejemplo a una clase concreta.

Aprendizaje no supervisado

El aprendizaje no supervisado consiste en **crear una función** que describa la estructura interna de un conjunto de datos sin etiquetar.

Características del aprendizaje no supervisado

- **Crea una función** que les permite descubrir relaciones o patrones ocultos dentro de los datos.
- El **objetivo** es **escribir y organizar** los datos que se le proporcionan.
- Los datos de entrada **no están etiquetados**.

Estos algoritmos trabajan a partir de un **conjunto de datos sin etiquetar**, que se proporciona a un **algoritmo de aprendizaje automático**. El algoritmo, a partir de esos datos, **crea una función hipótesis**, que describe las relaciones o patrones existentes entre los elementos del conjunto.

Asociación entre técnicas, herramientas y tipos de sistemas

Cada tipo de aprendizaje automático se vincula con técnicas y herramientas específicas, adaptadas a la naturaleza del problema y al tipo de datos con los que se trabaja:

- **Aprendizaje supervisado:** Utiliza técnicas como la **regresión lineal**, los **árboles de decisión**, las **máquinas de vectores de soporte (SVM)** o las **redes neuronales**. Estas técnicas se implementan con bibliotecas como **Scikit-learn** o **TensorFlow**, que permiten entrenar modelos a partir de datos etiquetados.

- **Aprendizaje no supervisado:** Emplea métodos como K-Means, PCA (Análisis de Componentes Principales) o **algoritmos de agrupamiento jerárquico**, cuyo objetivo es descubrir patrones y estructuras ocultas en los datos. Se utilizan herramientas como Weka, Orange y Scikit-learn.
- **Aprendizaje semi-supervisado:** Combina datos etiquetados y no etiquetados para mejorar la precisión del modelo. Se apoya en modelos híbridos y se implementa con Scikit-learn o TensorFlow.
- **Aprendizaje por refuerzo:** Se basa en técnicas como Q-Learning o Deep Q-Networks (DQN), en las que el agente aprende mediante prueba y error, recibiendo recompensas o penalizaciones según sus acciones. Este tipo de aprendizaje se desarrolla principalmente con TensorFlow y Keras.

La elección de la técnica y herramienta depende directamente del tipo de aprendizaje automático y de los objetivos del problema a resolver. Mientras que los enfoques supervisados se orientan a la predicción y clasificación, los no supervisados buscan descubrir patrones y estructuras ocultas en los datos. Los modelos semi-supervisados combinan ambos enfoques para aprovechar la información disponible de manera más eficiente, y los algoritmos de refuerzo se aplican cuando el sistema debe aprender mediante la interacción con un entorno cambiante.